Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

J.192

(11/2005)

SÉRIE J: RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

Câblo-modems

Passerelle résidentielle assurant la remise des services de données par câble

Recommandation UIT-T J.192

Recommandation UIT-T J.192

Passerelle résidentielle assurant la remise des services de données par câble

Résumé

La présente Recommandation décrit une passerelle résidentielle en fournissant un ensemble de caractéristiques fondées sur le protocole IP qui peut être ajouté à un câblo-modem ou être incorporé dans un dispositif autonome. Ces caractéristiques permettront aux câblo-opérateurs d'offrir à leurs clients un ensemble additionnel de services de réseau domestique améliorés, comprenant la prise en charge de la qualité de service (QS), la découverte de dispositifs et de services, une meilleure sécurité, la gestion des pare-feu, des caractéristiques de gestion et de préconfiguration orientées vers le réseau domestique, la conversion d'adresse de réseau géré, l'amélioration de l'adressage et du traitement des paquets et les diagnostics de dispositif de réseau local. La présente Recommandation est fondée sur les cadres architecturaux qui sont définis dans la Rec. UIT-T J.190.

La présente Recommandation représente une amélioration par rapport à la Rec. UIT-T J.191 car elle en conserve l'essentiel de la fonctionnalité en tant que fondation et développe cette base afin d'offrir d'autres caractéristiques évoluées. Un objectif de conception essentiel pour un équipement conforme à la présente Recommandation est son interopérabilité avec l'équipement conforme à la Rec. UIT-T J.191. Par exemple, des bases MIB communes sont utilisées pour la fonctionnalité fondamentale. Il en résulte qu'une tête de réseau conforme à la présente Recommandation peut gérer un déploiement mixte J.191 et J.192.

Source

La Recommandation UIT-T J.192 a été approuvée le 29 novembre 2005 par la Commission d'études 9 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou l'implémentation de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Recommandation UIT-T J.192

Passerelle résidentielle assurant la remise des services de données par câble

1 Domaine d'application

La présente Recommandation décrit une passerelle résidentielle en fournissant un ensemble de caractéristiques fondées sur le protocole IP qui peut être ajouté à un câblo-modem ou être incorporé dans un dispositif autonome. Ces caractéristiques permettront aux câblo-opérateurs d'offrir à leurs clients un ensemble additionnel de services de réseau domestique améliorés, comprenant la prise en charge de la qualité de service (QS), la découverte de dispositifs et de services, une meilleure sécurité, la gestion des pare-feu, des caractéristiques de gestion et de préconfiguration orientées vers le réseau domestique, la conversion d'adresse de réseau géré, l'amélioration de l'adressage et du traitement des paquets et les diagnostics de dispositif de réseau local. La présente Recommandation est fondée sur les cadres architecturaux qui sont définis dans la Rec. UIT-T J.190.

La présente Recommandation représente une amélioration par rapport à la Rec. UIT-T J.191 car elle en conserve l'essentiel de la fonctionnalité en tant que fondation et développe cette base afin d'offrir d'autres caractéristiques évoluées. Un objectif de conception essentiel pour un équipement conforme à la présente Recommandation est son interopérabilité avec l'équipement conforme à la Rec. UIT-T J.191. Par exemple, des bases MIB communes sont utilisées pour la fonctionnalité fondamentale. Il en résulte qu'une tête de réseau conforme à la présente Recommandation peut gérer un déploiement mixte J.191 et J.192.

La fonctionnalité clé que la présente Recommandation définit en plus de celle qui est définie par la Rec. UIT-T J.191 comprend les éléments suivants:

- découverte de dispositifs et de services pour applications et services dans le réseau local;
- prise en charge par conversion NAT de clients de réseau privé virtuel et de serveurs de réseau domestique sous protocole IPSec;
- langage et signalisation normalisés de configuration du pare-feu;
- fonctionnalité normalisée de pare-feu de base;
- simple commande parentale;
- qualité de service pour le réseau local, gérée dans la passerelle résidentielle.

Le texte non normatif qui se rapporte à la fonctionnalité UPnP figure dans la présente Recommandation sous forme d'implémentations exemplaires de la qualité de service et de la gestion d'un réseau domestique: ces exemples ont été mis entre accolades et marqués comme suit: "{texte informatif: …}". Tous les textes mis entre de telles accolades sont non normatifs.

2 Références

2.1 Références (normatives)

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

– Recommandation UIT-T J.112 Annexe B (2004), *Spécifications de l'interface du service de transmission de données par câble: interface radioélectrique*.

– Recommandation UIT-T J.125 (2004), *Confidentialité des liaisons pour les implémentations de câblo-modems*.

– Recommandation UIT-T J.126 (2004), *Spécification de câblo-modem intégré*.

– Recommandation UIT-T J.161 (2001), *Caractéristiques des codecs audio destinés au service audio bidirectionnel sur les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.162 (2005), *Protocole réseau de signalisation d'appel pour la fourniture de services à temps critique sur les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.163 (2005), *Qualité de service dynamique pour la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.164 (2005), *Prescriptions relatives aux messages d'événement pour la prise en charge des services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.167 (2005), *Prescriptions d'installation des adaptateurs MTA utilisés pour la fourniture de services en temps réel sur les réseaux de télévision par câble au moyen de câblo-modems*.

– Recommandation UIT-T J.170 (2005), *Spécification de la sécurité sur IPCablecom*.

– Recommandation UIT-T J.175 (2005), *Protocole de serveur audio*.

– Recommandation UIT-T J.178 (2005), *Signalisation entre serveurs de gestion d'appel IPCablecom*.

– Recommandation UIT-T J.191 (2004), *Paquetage de fonctionnalités IP pour l'amélioration des câblo-modems*.

– Recommandation UIT-T X.509 (2005) | ISO/CEI 9594-8:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

– Recommandation UIT-T X.690 (2002) | ISO/CEI 8825-1:2002, *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives*.

– ANSI/SCTE 22-1-2002, *DOCSIS 1.0, Radio Frequency Interface*.

– ANSI/SCTE 23-3-2005, *DOCSIS 1.1 Part 3*: *Operations Support System Interface (Interface avec le système d'aide à l'exploitation).*

– FIPS 140-2 (2001), *Security Requirements for Cryptographic Modules, (Règles de sécurité pour modules cryptographiques)*, Department of Commerce, NIST, 25 mai 2001.

– FIPS 180-1 (1995), *Secure Hash Algorithm (Algorithme de hachage sécurisé),* Department of Commerce, NIST.

– IANAifType MIB Definitions (Définitions de base MIB de type d'interface IANA), http://www.iana.org/assignments/ianaiftype-mib.

– IEEE 802.11-1999-MIB-D6.2, *IEEE 802.11 Management Information Base* (Base d'informations de gestion IEEE 802.11).

– IEEE 802.11A-1999, *IEEE Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz Band, Annex D.* Spécifications de commande d'accès au support (MAC) et de couche Physique de réseau local (LAN, local area network) sans fil – Couche Physique à grande vitesse dans la bande des 5 GHz), Annexe D, IEEE.

– IEEE 802.11B/Cor1-2001, *Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 2: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band, Corrigendum 1, Annex D.* (Spécifications de commande d'accès au support (MAC) et de couche Physique de réseau local (LAN) sans fil – Amendement 2: Extension de couche Physique à vitesse supérieure dans la bande des 2,4 GHz) – Corrigendum 1, Annexe D.

– IEEE 802.11D, *IEEE Standard for IT. Telecommunications and information exchange between systems – LAN/MAN Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 3: Specification for operation in additional regulatory domains, Annex D.* (Spécifications de commande d'accès au support (MAC) et de couche Physique de réseau local (LAN) sans fil – Amendement 3: Spécification pour l'exploitation dans des domaines administratifs additionnels), Annexe D.

– IEEE 802.11G-2003, *IEEE Standard for IT. Telecommunications and information exchange between systems – LAN/MAN Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, Annex D.* (Spécifications de commande d'accès au support (MAC) et de couche Physique de réseau local (LAN) sans fil – Amendement 4: Nouvelle extension de débit supérieur dans la bande des 2,4 GHz), Annexe D.

– ISO/CEI 8802-2 (ANSI/IEEE Std 802.2):1998, *Technologies de l'information – Télécommunications et échange d'informations entre systèmes – Réseaux locaux et métropolitains – Exigences spécifiques – Partie 2: Contrôle de liaison logique*.

– ISO/CEI 10038 (ANSI/IEEE Std 802.1D):1993, *Technologies de l'information – Télécommunications et échange d'informations entre systèmes – Réseaux locaux – Contrôle d'accès au milieu (MAC) – Ponts*.

– IETF RFC 347 (1972), *Echo Process*. (Traitement de l'écho).

– IETF RFC 768 (1980), *User Datagram Protocol (UDP)* (Protocole des datagrammes d'utilisateur).

– IETF RFC 791 (MIL STD 1777) (1981), *DARPA Internet Program, Protocol Specification. Internet Protocol* (Protocole Internet).

– IETF RFC 792 (1981), *DARPA Internet Program, Protocol Specification. Internet Control Message Protocol (ICMP)* (Protocole des messages de commande de l'Internet).

– IETF RFC 793 (1981), *DARPA Internet Program, Protocol Specification. Transmission Control Protocol* (Protocole de commande de transmission).

– IETF RFC 868 (1983), *Time Protocol* (Protocole temporel).

– IETF RFC 919 (1984), *Broadcasting Internet Datagrams* (Diffusion de datagrammes en protocole Internet).

– IETF RFC 922 (1984) *Broadcasting Internet datagrams in the presence of subnets* (Diffusion de datagrammes du protocole Internet en présence de sous-réseaux).

– IETF RFC 1034 (1987), *Domain Names – Concepts and Facilities* (Noms de domaines – Concepts et services).

– IETF RFC 1035 (1987), *Domain Names – Implementation and Specification* (Noms de domaines – Mise en œuvre et spécification).

– IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication Layers* (Exigences relatives aux serveurs locaux Internet – Couches de communication).

– IETF RFC 1123 (1989), *Requirements for Internet Hosts – Application and Support* (Exigences relatives aux serveurs locaux Internet – Application et prise en charge).

– IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP)* (Un protocole simple de gestion de réseau).

– IETF RFC 1213 (1991), *Management Information Base for Network Management of TCP/IP-based Internets MIB-II* (Base d'informations de gestion afin de gérer les réseaux Internet en protocoles TCP/IP).

– IETF RFC 1350 (1992), *The TFTP Protocol (Revision 2)* (Le protocole TFTP).

– IETF RFC 1510 (1993), *The Kerberos Network Authentication Service (V5)* (Le service d'authentification de réseau Kerberos).

– IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers* (Exigences relatives aux routeurs IP de version 4).

– IETF RFC 1889 (1996), *RTP: A Transport Protocol for Real-Time Applications* (Protocole de transport pour applications en temps réel).

– IETF RFC 1901 (1996), *Introduction to Community-based SNMPv2* (Introduction à la version 2 du protocole SNMP de communauté).

– IETF RFC 2011 (1996), *SNMPv2 Management Information Base for the Internet Protocol using SMIv2* (Base d'informations de gestion SNMPv2 pour le protocole Internet utilisant la version SMIv2).

– IETF RFC 2013 (1996), *SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2* (Base d'informations de gestion SNMPv2 pour le protocole de datagrammes d'utilisateur utilisant la version SMIv2).

– IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication* (HMAC: hachage de clés calculées pour l'authentification des messages).

– IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol* (Protocole de configuration dynamique du serveur local).

– IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions* (Options DHCP et extensions BOOTP de vendeur).

– IETF RFC 2236 (1999), *Internet Group Management Protocol, Version 2* (Protocole de gestion de groupe Internet).

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0* (La version 1.0 du protocole TLS).

– IETF RFC 2315 (1998), PKCS #7, *Cryptographic Message Syntax*, Version 1.5.

– IETF RFC 2349 (1998), *TFTP Timeout Interval and Transfer Size Options* (Options d'intervalle de temporisation et de longueur de transfert en protocole FTP).

– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol* (Architecture pour le protocole Internet).

– IETF RFC 2402 (1998), *IP Authentication Header* (En-tête d'authentification IP).

– IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP)* (Charge utile de sécurité par encapsulage IP).

– IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)* (L'échange de clés Internet).

– IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers* (Définition du champ de services différenciés (champ DS) dans les en-têtes IPv4 et IPv6).

– IETF RFC 2578 (1999), *Structure of Management Information Version 2 (SMIv2)* (Structure de la version 2 des informations de gestion) (SMIv2).

– IETF RFC 2579 (1999), *Textual Conventions for SMIv2* (Conventions textuelles pour la version SMIv2).

– IETF RFC 2580 (1999), *Conformance Statements for SMIv2* (Déclarations de conformité pour la version SMIv2).

– IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1* (Protocole de transfert d'hypertexte – HTTP/1.1).

– IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations* (Terminologie et considérations relatives à la conversion d'adresses IP de réseau (NAT)).

– IETF RFC 2669 (1999), *DOCSIS Cable Device MIB – Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems* (Base MIB de dispositifs par câble DOCSIS – Base d'informations de gestion de dispositif par câble pour câblo-modems et systèmes de terminaison de câblo-modem conformes à DOCSIS).

– IETF RFC 2670 (1999), *Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces* (Base d'informations de gestion d'interface radioélectrique pour interfaces RF conformes aux systèmes MCNS/DOCSIS).

– IETF RFC 2786 (2000), *Diffie-Hellman USM Key Management Information Base and Textual Convention* (Base d'informations de gestion de clés dans le modèle USM à codage Diffie-Helman et convention textuelle).

– IETF RFC 2863 (2000), *The Interfaces Group MIB* (Base d'information de gestion de groupe d'interfaces).

– IETF RFC 3022 (2001), *Traditional IP Network Address Translator (Traditional NAT)* (Convertisseur d'adresse de couche réseau IP traditionnel (conversion NAT traditionnelle)).

– IETF RFC 3046 (2001), *DHCP Relay Agent Information Option* (Option d'information d'agent-relais DHCP).

– IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* (Certificat et profil de liste de révocation de certificat (CRL) de l'infrastructure de clé publique Internet X.509).

– IETF RFC 3291 (2002), *Textual Conventions for Internet Network Addresses* (Conventions textuelles pour les adresses de réseau Internet).

– IETF RFC 3396 (2002), *Encoding Long Options in the Dynamic Host Configuration Protocol* (DHCPv4) (Codage d'options longues dans la version 4 du protocole de configuration dynamique du serveur local) (DHCPv4).

– IETF RFC 3410 (2002), *Introduction and Applicability Statements for Internet-Standard Management Framework* (Déclarations d'introduction et d'applicabilité pour le cadre de gestion par la norme Internet).

– IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol* (Architecture de description des cadres de gestion en protocole SNMP).

– IETF RFC 3412 (2002), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (Traitement et distribution de messages pour le protocole simple de gestion de réseau) (SNMP).

– IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) Applications* (Applications du protocole SNMP).

– IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)* (Modèle de sécurité du point de vue de l'utilisateur pour la version 3 du protocole simple de gestion de réseau).

– IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)* (Modèle de contrôle d'accès fondé sur la vue pour le protocole simple de gestion de réseau).

– IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)* (Version 2 des opérations du protocole simple de gestion de réseau) (SNMPv2).

– IETF RFC 3417 (2002) *Transport Mappings for the Simple Network Management Protocol (SNMP)* (Mappages de transport pour le protocole simple de gestion de réseau) (SNMP), décembre 2002.

– IETF RFC 3418 (2002), *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)* (Base d'informations de gestion (MIB) pour le protocole simple de gestion de réseau (SNMP)).

– IETF RFC 3584 (2003), *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework* (Coexistence entre les versions 1, 2 et 3 du cadre de gestion de réseau par la norme Internet).

– W3C Working Draft, World Wide Web Consortium (W3C), *Simple Object Access Protocol (SOAP) Version 1.2*, 19 décembre 2002, http://www.w3.org/2000/xp/Group/#drafts

– W3C Working Draft, World Wide Web Consortium (W3C) *XML Protocol (XMLP) Requirements*, 26 juin 2002, http://www.w3.org/TR/2002/WD-xmlp-reqs-20020626

2.2 Références (informatives)

– IANA Port Numbers, http://www.iana.org/assignments/port-numbers (Numéros de port de l'autoritéIANA)

– IETF RFC 2644 (1999), *Changing the Default for Directed Broadcasts in Routers* (Modification dans les routeurs de la valeur par défaut des diffusions orientées).

– IETF RFC 3164 (2001), *The BSD Syslog Protocol* (Protocole de journalisation SYSLOG des événements de diagnostic BSD).

– IETF RFC 3235 (2002), *Network Address Translator (NAT)-Friendly Application Design Guidelines* (Convertisseur d'adresses de réseau – Directives de conception d'applications conviviales).

– IETF RFC 3435 (2003), *Media Gateway Control Protocol (MGCP) Version 1.0* (Protocole de commande de passerelle de média).

– [draft-ietf-ipcdn-bpiplus-mib-05]

DOCSIS Baseline Privacy Plus MIB – Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus, IETF Internet Draft, http://www.watersprings.org/pub/id/draft-ietf-ipcdn-bpiplus-mib-05.txt

– Federal Information Processing Standards Publications (FIPS PUB) 186 (1994), *Digital Signature Standard (DSS).*

– Fenner W., *et al., IGMP-based Multicast Forwarding ("IGMP Proxying")*, IETF Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-magma-igmp-proxy-01.txt

– RSA Laboratories (1999), *PKCS #1, v2.0: RSA Cryptography Standard.*

– SCTE 22-3-2002, *DOCSIS 1.0 Part 3: Operations Support System Interface*.

– UDA 1.0 UPnP™ Device Architecture, Version 1.0, 08 juin, 2000 http://www.upnp.org/download/UPnPDA10_20000613.htm

– UQA UPnP™ QoS Architecture 1.0, 10 March, 2005, http://www.upnp.org

– UQD UPnP™ QosDevice 1.0 Service Definition Document, 10 mars, 2005.

– UQM UPnP™ QosManager 1.0 Service Definition Document, 10 mars 2005.

– UQPH UPnP™ QosPolicyHolder 1.0 Service Definition Document, 10 mars 2005.

– UIGD, InternetGatewayDevice:1, Device Template Version 1.01 for Universal Plug and Play Version 1.0, 12 novembre 2001, http://www.upnp.org

– UWIC WANIPConnection:1 Service Template Version 1.01 For UPnP™ Version 1.0, 12 novembre 2001, http://www.upnp.org

3 Définitions

La présente Recommandation définit les termes suivants:

3.1 portail de sécurité IPCable2Home (CSP, *IPCable2Home security portal*): élément fonctionnel qui offre des fonctions de gestion de la sécurité et de conversion entre l'hybride HFC et le réseau domestique.

3.2 dispositif PS intégré: élément de services de portail qui n'utilise pas d'interface autonome afin de se connecter à un câblo-modem.

3.3 dispositif d'accès domestique (HA, *home access*): groupement d'éléments logiques servant à réaliser l'accès par hybride HFC dans des réseaux IPCable2Home. Ce dispositif est désigné par le terme de *passerelle résidentielle* dans la présente Recommandation.

3.4 dispositif de client domestique (HC, *home client*): groupement d'éléments logiques servant à offrir une fonctionnalité à des applications clientes. Ce dispositif est désigné par le terme de *serveur local IPCable2Home* dans la présente Recommandation.

3.5 dispositif IP de réseau local: dispositif IP typique qui est censé résider dans les réseaux domestiques et contenir une pile de protocoles TCP/IP ainsi qu'un client du protocole DHCP.

3.6 service (de) portail (PS, *portal service*): élément fonctionnel qui fournit des fonctions de gestion et de conversion entre l'hybride HFC et le réseau domestique.

3.7 dispositif PS autonome: élément de services de portail qui se connecte au câblo-modem en utilisant seulement une interface autonome.

4 Abréviations et conventions

4.1 Abréviations

La présente Recommandation utilise les abréviations suivantes:

A/V	audio/vidéo
ALG	passerelle de couche Application (*application layer gateway*)
APP	application
ASP	mandataire spécifique de l'application (*application specific proxy*)
BP	point extrême (*boundary point*)
BPSC	configuration globale des services de portail (*bulk portal services configuration*)
CA	autorité de certification (*certificate authority*)
CAP	portail d'adresse IPCable2Home (*IPCable2Home address portal*)
CAT	conversion d'adresse IPCable2Home (*IPCable2Home address translation*)
CDC	client IPCable2Home de protocole DHCP (*IPCable2Home DHCP client*)
CDP	portail DHCP IPCable2Home (*IPCable2Home DHCP portal*)
CDS	serveur distant de protocole DHCP du modèle IPCable2Home (*IPCable2Home DHCP server*)
CH	serveur local IPCable2Home (*IPCable2Home host*)
CM	câblo-modem
CMP	portail de gestion IPCable2Home (*IPCable2Home management portal*)
CMS	serveur de gestion d'appels (*call management server*)
CMTS	système de terminaison de câblo-modem (*cable modem termination system*)
C-NAPT	conversion d'adresse réseau et portail IPCable2Home (*IPCable2Home network address and port translation*)
C-NAT	conversion d'adresse de réseau IPCable2Home (*IPCable2Home network address translation*)
CNP	portail de nommage IPCable2Home (*IPCable2Home name portal*)
CPU	unité centrale (*central processing unit*)
CQoS	qualité de service IPCable2Home (*IPCable2Home quality of service*)
CQP	portail de qualité de service IPCable2Home (*IPCable2Home QoS portal*)
CRG	passerelle résidentielle IPCable2Home (*IPCable2Home residential gateway*)
CRL	liste de révocation de certificat (*certificate revocation list*)
CSP	portail de sécurité IPCable2Home (*IPCable2Home security portal*)
CTL	laboratoire d'essais de certification (*certification testing laboratory*)
CTP	portail d'essais IPCable2Home (*IPCable2Home test portal*)
CVC	certificat de vérification de code

CVS	signature de vérification de code (*code verification signature*)
CxP	sous-fonction des services de portail IPCable2Home (*IPCable2Home portal services sub-function*)
DER	règles de codage distinctives (*distinguished encoding rules*)
DHCP	protocole de configuration de serveur dynamique (*dynamic host configuration protocol*)
DNS	serveur de nom de domaine (*domain name server*)
DOCSIS	spécification d'interface du service de transmission de données par câble (*data-over-cable service interface specification*)
DoS	refus de service (*denial of service*)
DQoS	qualité de service dynamique (PacketCable) (*dynamic quality-of-service*)
E-MTA	adaptateur de terminal multimédia incorporé (*embedded multimedia terminal adapter*)
FTP	protocole de transfert de fichiers (*file transfer protocol*)
FW	pare-feu (*firewall*)
GMT	temps moyen de Greenwich (*Greenwich mean time*)
HA	accès domestique (*home access*)
HE	tête de réseau (*headend*)
HEX	hexadécimal
HFC	hybride optique coaxial (*hybrid fibre coax*)
ICMP	protocole des messages de commande Internet (*Internet control message protocol*)
IETF	groupe de travail d'ingénierie Internet (*Internet engineering task force*)
IGMP	protocole de gestion de groupe Internet (*Internet group management protocol*)
IP	protocole Internet (*Internet protocol*)
IPCDN	réseau de données IP par câble (Groupe de travail de l'IETF) (*IP over cable data network*)
IPF	filtre de paquets entrants (*inbound packet filter*)
IPSec	sécurité du protocole Internet (*Internet protocol security*)
KDC	centre de distribution de clé (*key distribution centre*)
LAN	réseau local (*local area network*)
LAN-Pass	adresse LAN de transfert (*pass-through local area network address*)
LAN-Trans	adresse LAN convertie (*translated local area network address*)
MAC	commande d'accès au support (*media access control*)
MBP	point extrême de gestion (*management boundary point*)
MCF	fonction de client de gestion (*management client function*)
MGCP	protocole de contrôle de passerelle média (*media gateway control protocol*)
MIB	base d'informations de gestion (*management information base*)
MPLS	commutation multiprotocolaire par étiquetage (*multiprotocol label switching*)

MSF	fonction de serveur de gestion (*management server function*)
MTA	adaptateur de terminal multimédia (*multimedia terminal adapter*)
NAPT	conversion d'adresse et de portail de réseau (*network address and portal translation*)
NAT	conversion d'adresse de réseau (*network address translation*)
NCS	signalisation d'appel fournie par le réseau (*network-based call signalling*)
NMS	système de gestion de réseau (*network management system*)
NS	serveur distant de noms documentés (*authoritative name server*)
OID	identificateur d'objet (*object identifier*)
OPF	filtre de paquets sortant (*outbound packet filter*)
OSI	interconnexion des systèmes ouverts (*open systems interconnection*)
OSS	système support d'exploitation (*operations support system*)
PDU	unité de données protocolaire (*protocol data unit*)
PF	filtre de paquets (*packet filter*)
PING	sondeur de paquets entre réseaux (*packet inter-network grouper*)
PKI	infrastructure de clé publique (*public key infrastructure*)
PKINIT	authentification initiale par cryptographie à clé publique (*public-key cryptography for initial authentication*)
PS	services de portail (*portal services*)
PS WAN-Data	interface de données entre un réseau régional et un élément des services de portail IPCable2Home (*IPCable2Home portal services element WAN data interface*)
PS WAN-Man	interface de gestion entre un réseau régional et un élément des services de portail IPCable2Home (*IPCable2Home portal services element WAN management interface*)
QBP	point extrême de qualité de service (*quality of service boundary point*)
QCC	client de politique de qualité de service (*quality of service characteristics client*)
QCS	serveur distant de politique de qualité de service (*quality of service characteristics server*)
QFM	réexpédition et accès au support de la qualité de service (*quality of service forwarding & media access*)
QS	qualité de service
RAM	mémoire à accès aléatoire (*random access memory*)
RDN	nom distinctif relatif (*relative distinguished name*)
RFC	demande de commentaires (*request for comments*)
RG	passerelle résidentielle (*residential gateway*)
ROM	mémoire morte (*read-only memory*)
RSA	Rivest, Shamir, Adleman
RSVP	protocole de réservation de ressource (*resource reservation protocol*)
RTCP	protocole de commande en temps réel (*real-time control protocol*)

RTP protocole de transport en temps réel (*real-time transport protocol*)

SDP protocole de description de session (*session description protocol*)

SHA-1 algorithme de hachage sécurisé 1 (*secure hash algorithm 1*)

S-MTA adaptateur autonome de terminal multimédia (*standalone multimedia terminal adapter*)

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

SoA début de zone administrative (*start of authority*)

SPF filtrage de paquet d'après l'état (*stateful packet filtering*)

SYSLOG journalisation du système (*system log*)

TCP protocole de commande de transmission (*transmission control protocol*)

TFTP protocole trivial de transfert de fichiers (*trivial file transfer protocol*)

TLS sécurité de la couche Transport (*transport layer security*)

TLV type-longueur-valeur

ToD heure locale (*time of day*)

UDP protocole datagramme d'utilisateur (*user datagram protocol*)

URL adresse universelle (*uniform resource locator*)

USFS commutation de réexpédition sélective en amont (*upstream selective forwarding switch*)

USM modèle de sécurité fondé sur l'utilisateur (*user security model*)

UTC temps universel coordonné (*coordinated universal time*)

VACM modèle de commande d'accès fondé sur la vue (*view-based access control model*)

VoIP téléphonie utilisant le protocole Internet (*voice over Internet protocol*)

WAN réseau régional (*wide area network*)

WAN-Data secteur d'adresse de données de réseau régional (*wide area network data address realm*)

WAN-Man secteur d'adresse de gestion de réseau régional (*wide area network management address realm*)

4.2 Conventions

Dans l'ensemble de la présente Recommandation, les mots qui servent à définir la portée d'exigences particulières sont imprimés en majuscules. Ces mots sont les suivants:

"DOIT" Cette forme verbale ou l'adjectif "REQUIS" signifie que le sujet est une exigence absolue de la présente Recommandation.

"NE DOIT PAS" Cette expression signifie que le sujet est une interdiction absolue de la présente Recommandation.

"DEVRAIT" Cette forme verbale ou l'adjectif "RECOMMANDÉ" signifie qu'il peut exister, dans des circonstances particulières, des raisons valides pour ignorer ce sujet; mais il faut en comprendre toutes les implications et peser attentivement le cas avant de choisir une option différente.

"NE DEVRAIT PAS" Cette expression signifie qu'il peut exister, dans des circonstances particulières, des raisons valides pour que le comportement indiqué soit acceptable ou même utile; mais il faut en comprendre toutes les implications et peser attentivement le cas avant de mettre en œuvre un quelconque comportement décrit avec cette mention.

"PEUT" Cette forme verbale ou l'adjectif "FACULTATIF" signifie que le sujet est véritablement facultatif. Un vendeur peut choisir d'inclure le sujet parce qu'un marché particulier le requiert ou, par exemple, parce que le sujet améliore le produit; un autre vendeur peut omettre le même sujet.

5 Architecture de référence

L'objectif du modèle IPCable2Home doit permettre la livraison de nouveaux services par câble à des dispositifs situés à domicile en complément des services offerts par les infrastructures CableModem et IPCablecom. Plus précisément, le modèle IPCable2Home offre une infrastructure spécifiant un environnement de création de réseaux domestiques permettant d'acheminer, de gérer et de prendre en charge des services IPCablecom et d'autres applications connexes.

La présente Recommandation facilite la mise au point d'une passerelle résidentielle (CRG, *residential gateway*) interopérable. L'objectif est la création d'un environnement orienté vers une passerelle résidentielle configurable par le câblo-pérateur, qui va interagir valablement avec les dispositifs résidentiels en protocole IP (dispositifs IP de réseau local). Cet environnement apporte à la passerelle résidentielle une gestion, une préconfiguration, une qualité de service et une sécurité pilotées par le câblo-opérateur. La messagerie de découverte, la qualité de service priorisée et les télédiagnostics simples pour les dispositifs domestiques sont également spécifiés. {texte informatif: la messagerie de qualité de service requise pour la répartition des politiques entre les applications fonctionnant sur des serveurs locaux conformes à l'environnement de qualité de service UPnP est également spécifiée}. Un résumé des capacités offertes par la présente Recommandation est reproduit ci-dessous:

gestion, découverte et préconfiguration

- gestion et configuration à distance du dispositif de passerelle résidentielle;
- mandataire de diagnostics simples de passerelle résidentielle pour les dispositifs domestiques en protocole IP;
- préconfiguration automatique des dispositifs de passerelle résidentielle;
- découverte de dispositifs domestiques en protocole IP et des applications associées;
- gestion de la passerelle résidentielle à partir du réseau local;

adressage et traitement de paquet

- conversion d'adresse multivoque (point à multipoint) pour les dispositifs domestiques;
- conversion d'adresse bi-univoque (point à point) pour les dispositifs domestiques;
- adressage sans conversion pour les dispositifs domestiques (à applications allergiques à la conversion NAT);
- protection du trafic par hybride HFC vis-à-vis des communications internes par les dispositifs domestiques;
- prise en charge de l'adressage domestique au cours d'un délestage d'hybride HFC;
- serveur DNS simple dans la passerelle résidentielle;
- prise en charge de la conversion NAT pour clients VPN sous IPSec;
- prise en charge par conversion d'adresse des serveurs domestiques en protocole IP;
- configuration en client de la conversion NAT.

qualité de service (QS)

- fonction de dérivation transparente dans le dispositif de passerelle résidentielle pour les messages de qualité de service IPCablecom au départ/à destination d'applications conformes au système IPCablecom;
- capacité d'attribuer des priorités de trafic à des applications spécifiques (accès différencié au support);
- capacité d'attribuer des priorités aux files d'attente dans le dispositif de passerelle résidentielle en association avec la fonctionnalité de traitement des paquets;
- {texte informatif: fourniture aux serveurs locaux UPnP des services de gestionnaire de qualité de service et de détenteur de politique UPnP};

sécurité

- authentification du dispositif de passerelle résidentielle;
- messages de gestion sécurisés entre le réseau de transmission de données par câble et la passerelle résidentielle;
- téléchargement sécurisé de fichiers de configuration et de mise à jour logicielle;
- sécurité facultative du fichier de configuration;
- gestion à distance du pare-feu de passerelle résidentielle;
- configuration et signalisation de pare-feu normalisées;
- contrôle parental simple.

Le reste du présent paragraphe considère l'architecture de référence IPCable2Home à partir des six points de vue suivants:

- vue logique (§ 5.1);
- vue fonctionnelle (§ 5.2);
- vue de l'interface de messagerie (§ 5.3);
- vue informationnelle (§ 5.4);
- vue opérationnelle (§ 5.5);
- vue de l'interface physique (§ 5.6).

5.1 Architecture de référence logique

Comme représenté dans la Figure 5-1, le présent paragraphe présente les concepts des éléments logiques IPCable2Home et des dispositifs IPCable2Home.

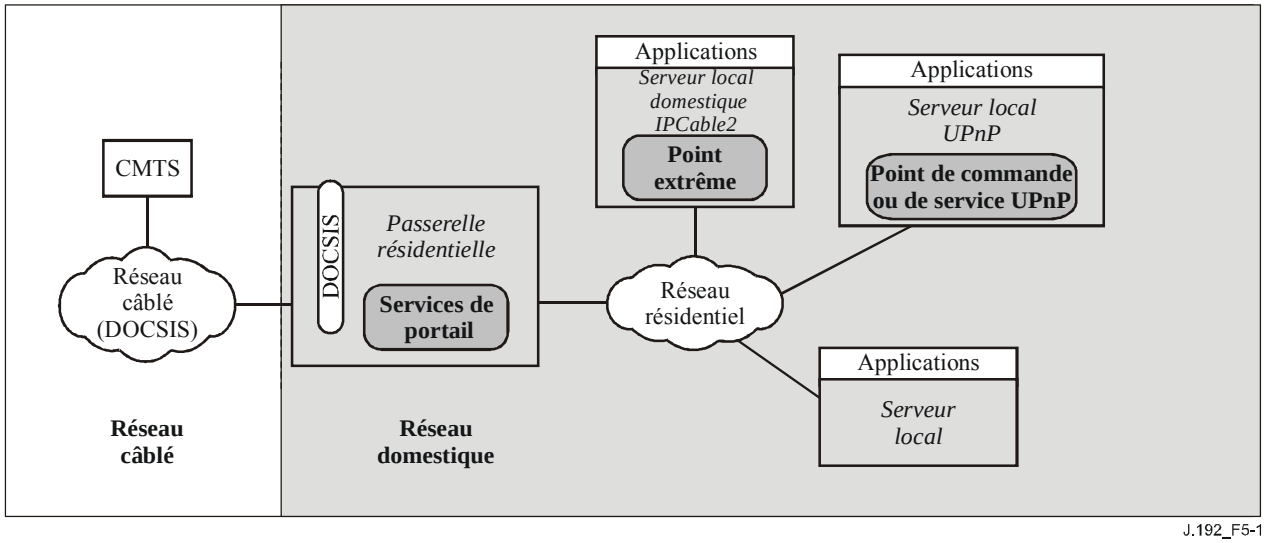


Figure 5-1/J.192 – Principaux concepts logiques IPCable2Home

5.1.1 Dispositifs IPCable2Home

L'architecture IPCable2Home identifie des dispositifs afin d'offrir un contexte tangible aux éléments logiques décrits dans le § 5.1.2. Les définitions de dispositif permettent de donner une description informative de la topologie d'un réseau domestique ainsi que des éléments logiques situés dans le réseau domestique, mais ces définitions ne sont pas considérées comme définitives ou restrictives. Les dispositifs IPCable2Home comprennent la passerelle résidentielle et le serveur local IPCable2Home.

Le dispositif de passerelle résidentielle (HA, *home access*, dans la Rec. UIT-T J.190) représente l'emplacement physique de l'élément logique de services de portail (PS) qui est décrit dans le § 5.1.2.1. La passerelle résidentielle a une seule interface avec un réseau régional, un seul élément logique des services de portail et peut avoir une ou plusieurs interfaces avec un réseau local.

Le terme de "*dispositif IP de réseau local"* sert à désigner tout serveur local de réseau local qui implémente une pile IPv4, y compris un client DHCP. un dispositif IP de réseau local qui met en œuvre une fonctionnalité IPCable2Home est désigné par le terme de *dispositif de serveur local IPCable2Home* ("HC" dans la Rec. UIT-T J.190). {texte informatif: un dispositif IP de réseau local sans fonctionnalité IPCable2Home ni UPnP est désigné par le terme de *serveur local*.}

Le dispositif de serveur local IPCable2Home représente l'emplacement physique du point extrême (BP, *boundary point*), lequel, défini dans le § 5.1.2.3, permet aux serveurs locaux IPCable2Home d'interagir avec des passerelles résidentielles IPCable2Home. Le serveur local IPCable2Home n'a qu'une seule interface avec un réseau local.

{texte informatif: le dispositif de serveur local UPnP représente l'emplacement physique de la fonctionnalité de point de commande ou de services UPnP. Le serveur local UPnP interagit avec la passerelle résidentielle CableHome en utilisant les messages de découverte UPnP et de qualité de service UPnP afin de communiquer ses attributs de dispositif et d'établir la qualité de service dans le réseau local domestique.}

Le modèle IPCable2Home implique une topologie de création de réseau domestique avec un seul câblo-modem DOCSIS et une seule passerelle résidentielle IPCable2Home dans le réseau local domestique. L'on part du principe que le câblo-modem conforme à DOCSIS est la seule connexion directe à l'hybride HFC. Théoriquement, la passerelle résidentielle IPCable2Home sera directement connectée au câblo-modem sans autres dispositifs raccordés entre le câblo-modem et la passerelle résidentielle IPCable2Home afin que celle-ci puisse offrir la protection spécifiée au réseau

domestique. Tous les serveurs locaux de réseau local sont connectés au réseau local derrière la passerelle résidentielle IPCable2Home.

5.1.2 Eléments logiques

Le cadre architectural introduit le concept d'éléments logiques IPCable2Home, qui sont des entités fonctionnelles logiquement associées, pouvant produire des messages spécifiés et y répondre. Les éléments logiques IPCable2Home fonctionnent dans la couche du protocole IP et dans les couches supérieures, ce qui leur permet de rester indépendants de toute technique particulière de réseau physique. Ces éléments possèdent également la capacité de recueillir et de communiquer des informations selon les besoins afin de découvrir, de gérer et de livrer des services sur des réseaux IPCable2Home. Le modèle IPCable2Home définit une entité logique spécifique à chaque dispositif IPCable2Home: l'entité logique de services de portail encapsule une fonctionnalité IPCable2Home définie pour les passerelles résidentielles, tandis que l'entité logique de point extrême encapsule une fonctionnalité définie pour les serveurs locaux IPCable2Home (voir au § 5.1.1 une description des dispositifs IPCable2Home).

5.1.2.1 Services de portail (PS, *portal services*)

Les services de portail forment un élément logique qui fournit dans les bâtiments des services composites de sécurité, de gestion, de préconfiguration, d'adressage et de qualité de service. Le terme de "portail" sert à indiquer des services qui assurent l'interface du réseau régional avec le réseau local. Le présent paragraphe décrit les caractéristiques de l'élément logique de services de portail.

5.1.2.1.1 Dispositif PS autonome et dispositif PS avec câblo-modem intégré

Les deux composants primaires pouvant être intégrés dans une passerelle résidentielle, à savoir le câblo-modem (CM) et l'élément de services de portail (PS), peuvent utiliser des ressources matérielles et logicielles partagées ou indépendantes. C'est ce partage de ressources entre les fonctions de câblo-modem et de services de portail qui distingue le dispositif PS autonome d'un dispositif PS intégré.

Un dispositif PS autonome NE DOIT PAS partager de composants matériels ou logiciels avec un câblo-modem. La séparation entre le câblo-modem et le dispositif PS autonome DOIT apparaître aux services de portail comme une simple déconnexion de son réseau régional – c'est-à-dire que le dispositif PS restera entièrement fonctionnel, comme s'il avait été déconnecté du réseau régional. Sinon, le dispositif PS sera considéré comme intégré. Compte tenu de ces définitions, il est possible qu'un dispositif PS puisse résider dans la même enveloppe physique qu'un câblo-modem tout en restant considéré comme un dispositif PS autonome.

CM et PS sont considérés comme étant des éléments distincts, aussi bien dans le cas de l'autonomie que dans celui de l'intégration. Ils répondent à des adresses de gestion uniques. Dans le cas de l'intégration, CM et PS se partagent des composants matériels ou logiciels mais, du point de vue de la gestion, ce sont des entités distinctes.

La Figure 5-2 décrit les dispositifs PS autonomes et intégrés. Dans ces deux cas, la combinaison d'un CM et d'un PS est considérée comme englobant le concept de dispositif HA.

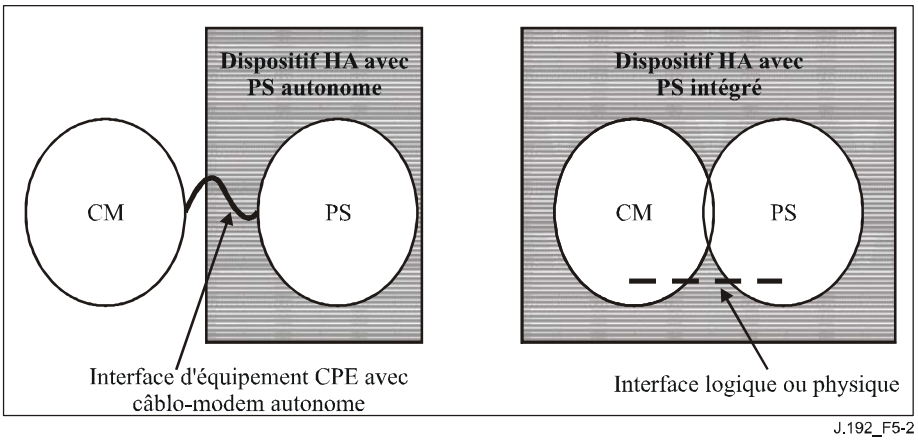


Figure 5-2/J.192 – Dispositif PS autonome et dispositif PS avec câblo-modem intégré

5.1.2.2 {texte informatif: services et points de commande UPnP

Un serveur local UPnP englobe une fonctionnalité UPnP logique, telle que les services ou les points de commande UPnP. Bien qu'il soit une entité logique spécifiée par le modèle CableHome, le dispositif PS interagit avec des éléments logiques du réseau local qui ne sont pas spécifiés par CableHome. Le dispositif PS fournit des services limités à tous les dispositifs IP du réseau local et des services additionnels afin d'interagir avec les services UPnP et les points de commande UPnP. L'architecture CableHome utilise une messagerie conforme au modèle UPnP entre le dispositif PS et les services et points de commande UPnP dans le réseau local. Dans l'architecture UPnP [UDA, 1.01], les messages de commande sont émis par le point de commande UPnP et reçoivent une réponse des services UPnP.}

5.1.2.3 Point extrême (point BP)

Un point extrême (point BP, *boundary point*) est un élément logique qui englobe l'ensemble de la fonctionnalité IPCable2Home définie pour un serveur local IPCable2Home dans le réseau local.

5.1.3 Secteurs d'adresses

Un secteur d'adresses est défini comme "un domaine de réseau dans lequel les adresses de couche Réseau sont attribuées de façon univoque à des entités de telle sorte que les datagrammes puissent leur être acheminés" [RFC 2663]. Dans la présente Recommandation, les secteurs d'adresses entrent dans les deux catégories suivantes: secteurs d'adresses de réseau régional et secteurs d'adresses de réseau local (voir Figure 5-3).

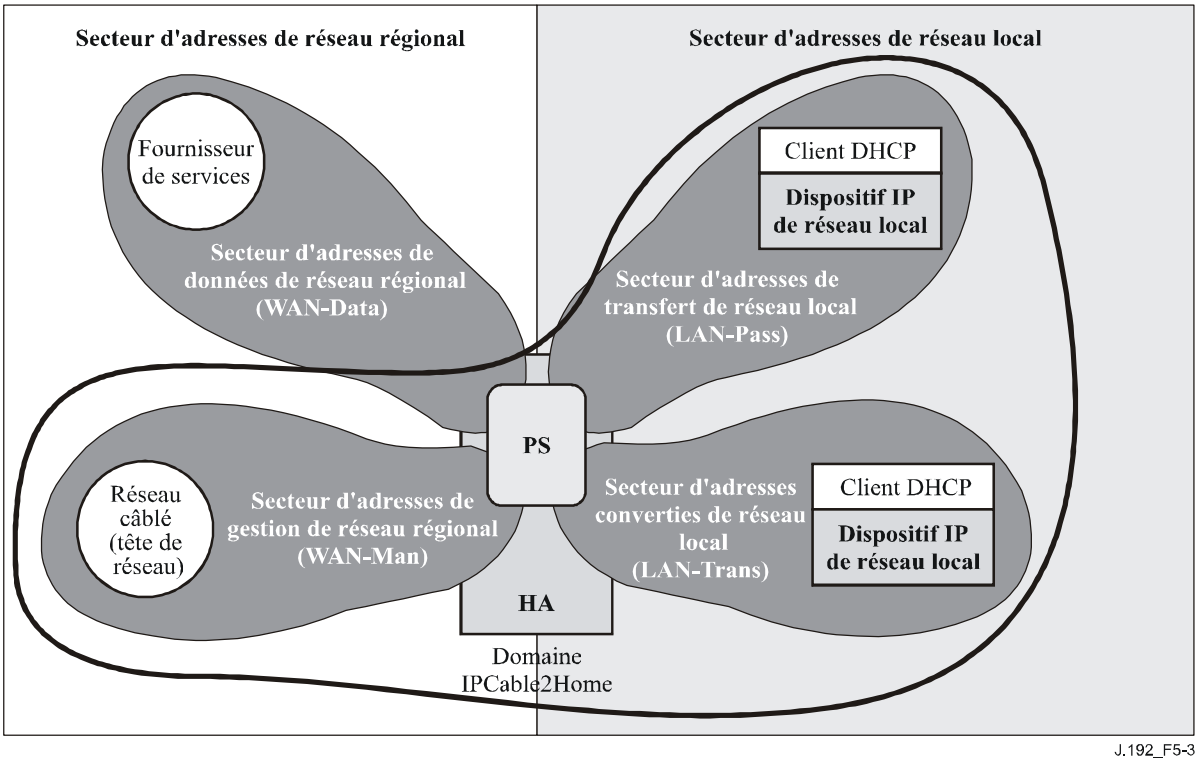


Figure 5-3/J.192 – Secteurs d'adresses IPCable2Home

Les adresses de réseau régional résident dans un seul des deux secteurs suivants: le secteur d'adresses de gestion de réseau régional (WAN-Man, *WAN management address realm*) ou le secteur d'adresses de données de réseau régional (WAN-Data, *WAN data address realm*). Les adresses de réseau local résident également dans un seul des deux secteurs suivants: le secteur d'adresses de transfert de réseau local (LAN-Pass, *LAN passthrough address realm*) ou le secteur d'adresses converties de réseau local (LAN-Trans, *LAN translated address realm*). Les propriétés de ces secteurs d'adressage sont les suivantes:

- le secteur d'adresses de gestion de réseau régional (WAN-Man) est destiné à transporter du trafic de gestion de réseau dans le réseau câblé entre le système de gestion de réseau et l'élément de services de portail. En principe, les adresses de ce secteur résideront dans l'espace privé d'adresses IP;
- le secteur d'adresses de données de réseau régional (WAN-Data) est destiné à transporter du trafic d'application d'abonné dans le réseau câblé et au-delà, en tant que trafic entre dispositifs IP du réseau local et serveurs locaux Internet. En principe, les adresses de ce secteur résideront dans l'espace public d'adresses IP;
- le secteur d'adresses converties de réseau local (LAN-Trans) est destiné à transporter du trafic d'application d'abonné et de gestion dans le réseau domestique entre dispositifs IP de réseau local et l'élément de services de portail. En principe, les adresses de ce secteur résideront dans l'espace privé d'adresses IP et pourront normalement être réutilisées par les abonnés;
- le secteur d'adresses de transfert de réseau local (LAN-Pass) est destiné à transporter du trafic d'application d'abonné, comme du trafic entre dispositifs IP de réseau local et serveurs locaux Internet, dans le réseau domestique, dans le réseau câblé et au-delà. En principe, les adresses de ce secteur résideront dans l'espace public d'adresses IP.

Du côté du réseau local, les adresses contenues dans le secteur d'adresses de transfert de réseau local (LAN-Pass) sont directement extraites des adresses contenues dans le secteur d'adresses de réseau WAN-Data. Celles-ci sont utilisées par les dispositifs IP de réseau local et par des applications comme les services IPCablecom qui n'acceptent pas la conversion d'adresse et exigent une adresse IP acheminable mondialement. De plus, du côté réseau local, les dispositifs IP de réseau local peuvent se faire attribuer des adresses converties à partir du secteur d'adresses converties de réseau local (LAN-Trans). Les secteurs d'adresses des réseaux LAN-Pass et LAN-Trans existent au niveau de chaque résidence.

Les interfaces physiques avec un réseau local, situées dans le dispositif PS, se font attribuer un indice conformément à la base MIB de groupe d'interfaces [RFC 2863] comme décrit dans le § 6.3.3.1.4.8, Base MIB de groupe d'interfaces. Une interface virtuelle avec un réseau local intégrant toutes les interfaces physiques avec un réseau local est également définie pour le dispositif PS dans le § 6.3.3.1.4.8. De même, une interface virtuelle avec un réseau local, n'intégrant que les interfaces physiques avec des réseaux locaux sans fil, est définie pour les services de portail dans le § 6.3.3.1.4.8. L'adresse IP du côté réseau local qui a été définie pour le dispositif PS est "reliée" à l'interface virtuelle avec "toutes" les interfaces physiques avec un réseau local. Les fonctions de protocole DHCP et de serveur distant de noms de domaine, ainsi que la fonction de routeur des services de portail, sont des applications mises en œuvre dans le dispositif PS adressé au moyen de l'adresse IP du côté réseau local qui est reliée à l'interface virtuelle avec un réseau local.

5.2 Modèle de référence fonctionnel IPCable2Home

Les fonctions IPCable2Home sont des services en protocole IP, définis dans la présente Recommandation et destinés à être mis en œuvre par le dispositif PS, ou par le réseau de données du câblo-opérateur, qui assurent la livraison de services par câble. Les fonctions IPCable2Home sont définies pour chacun des principaux domaines de spécification: préconfiguration, gestion, sécurité et qualité de service.

Des sous-éléments représentent des groupements de fonctionnalités associées dans le dispositif PS. L'élément logique PS peut contenir un nombre quelconque de sous-éléments. Ces derniers peuvent eux-mêmes contenir des sous-groupements de fonctions (c'est-à-dire des sous-éléments de sous-éléments).

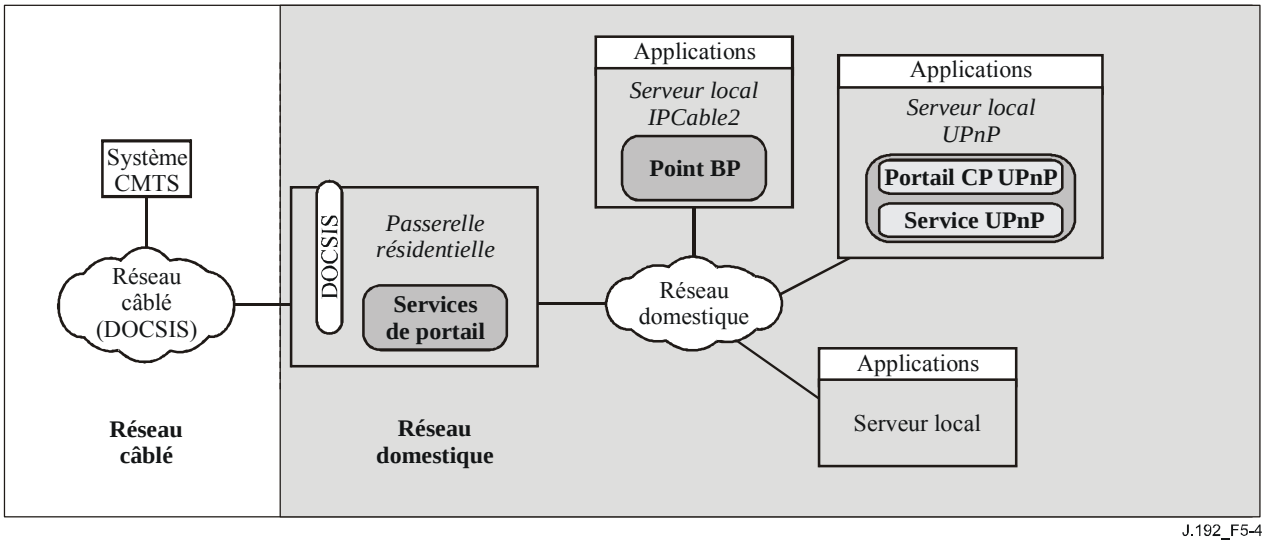


Figure 5-4/J.192 – Sous-éléments IPCable2Home

Le dispositif PS contient un certain nombre de sous-éléments, qui sont présentés ci-dessous.

5.2.1 {texte informatif: relation entre modèles CableHome et UPnP

L'architecture IPCable2Home utilise la messagerie conforme au modèle UPnP afin de gérer les dispositifs de serveur local UPnP et d'interagir avec eux. La fonctionnalité de certains sous-éléments du dispositif PS est donc décrite en termes de point de commande UPnP et de services UPnP. Par exemple, le dispositif PS comporte une fonctionnalité telle que le service UPnP de connexion IP par réseau régional à passerelle IP (IGD, *Internet gateway device*) [UWIC, *UPnP IGD WANIpConnection Service*] afin de permettre la configuration de la fonctionnalité de conversion d'adresse IPCable2Home (CAT) à partir de serveurs locaux UPnP. De même, le dispositif PS utilise la fonctionnalité de point de commande UPnP pour la découverte de dispositifs et services UPnP dans le réseau domestique. (Voir la Figure 5-5.)

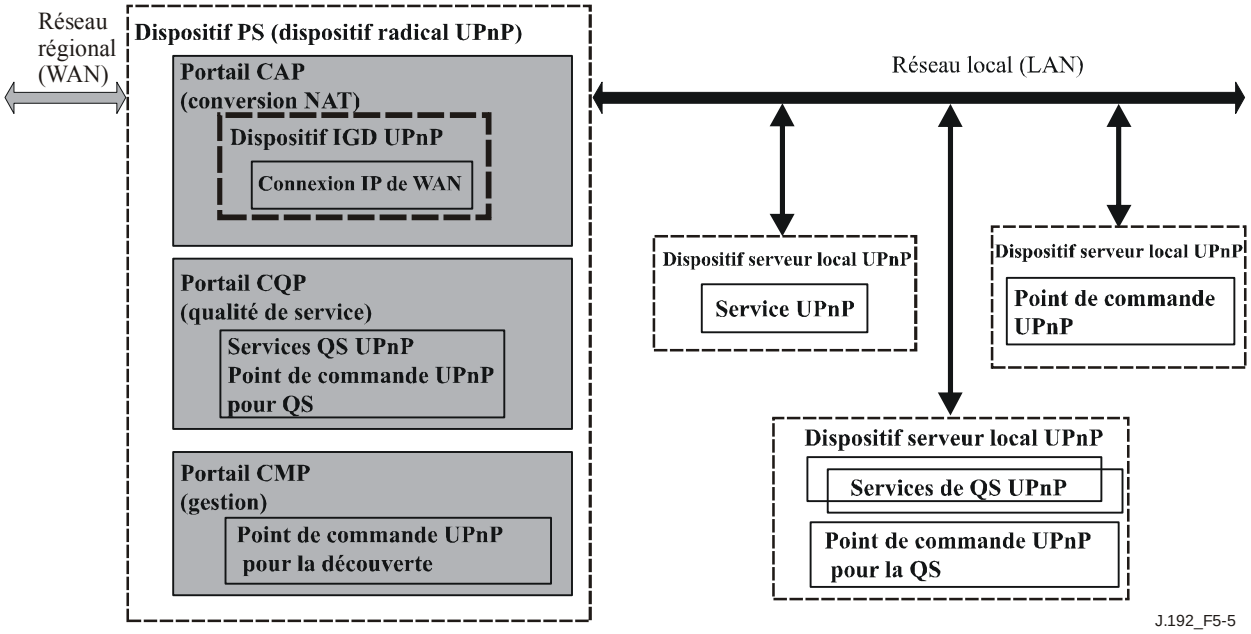


Figure 5-5/J.192 – Hiérarchie des dispositifs et services UPnP dans le modèle IPCable2Home}

5.2.2 Fonctions de gestion et de préconfiguration IPCable2Home

Afin de prendre en charge les exigences pendant la préconfiguration et la gestion de serveurs locaux à domicile, le modèle IPCable2Home fait appel à des fonctions de gestion et de préconfiguration qui résident dans le réseau de données par câble et définit des fonctions pour le dispositif PS. Les fonctions de gestion et de préconfiguration fondées sur le réseau câblé comprennent un certain nombre de services utilisés par des processus de gestion et de préconfiguration conformes à IPCable2Home. Les fonctions de gestion et de préconfiguration des services de portail sont situées dans la passerelle résidentielle. Elles comprennent des fonctionnalités d'émulation de serveur distant, d'émulation de client, et d'autres types fonctionnels. Des exemples de fonctions de réseau câblé et de services de portail sont présentés dans les Tableaux 5-1 et 5-2. Ils sont également illustrés dans la Figure 5-6.

Tableau 5-1/J.192 – Fonctions de gestion de réseau câblé

Fonctions de gestion de réseau câblé	Description
Serveur distant DHCP de réseau câblé	Le serveur DHCP est un composant de réseau câblé qui fournit aux services de portail des informations d'adresse pour les secteurs d'adresses WAN-Man et WAN-Data
Serveurs de gestion de réseau câblé	Serveurs de messagerie de gestion, de téléchargement et de notification d'événement IPCable2Home, y compris des protocoles comme SNMP, SYSLOG et TFTP [RFC 2349]
Serveur temporel de réseau câblé	Le serveur temporel (ToD) offre l'heure locale à ses clients.

Tableau 5-2/J.192 – Fonctions de gestion et de préconfiguration des services de portail

Fonctions de portail de gestion	Description
Portail d'adressage IPCable2Home (CAP)	Dans le dispositif PS, le portail CAP interconnecte les secteurs d'adresses WAN et LAN pour le trafic de données (voir CAT/Transfert). {texte informatif: cette fonction assure également l'interface avec le service UPnP de connexion IP par réseau régional à passerelle IGD afin que les points de commande UPnP configurent la table de conversion d'adresse IPCable2Home.}
Conversion d'adresse IPCable2Home (CAT)	Sous-fonction du portail CAP, une conversion CAT traduit les adresses IP de réseau public se trouvant du côté WAN-Data du portail CAP en adresses IP de réseau privé dans un seul sous-réseau logique du côté .
Transfert	Sous-fonction du portail CAP, la fonction de transfert dérive les paquets se trouvant du côté WAN-Data du portail CAP vers le côté LAN-Pass sans changement.
Portail de gestion IPCable2Home (portail CMP)	Fonction qui fournit des interfaces entre l'opérateur et la base de données du dispositif PS. {texte informatif: cette fonction permet également de découvrir, au moyen du processus de découverte UPnP, divers serveurs locaux UPnP et les services UPnP qui y sont offerts.}
Portail DHCP IPCable2Home (CDP)	Fonctions d'information d'adresse (p. ex. celles qui sont transmises par protocole DHCP) y compris un serveur distant pour le secteur LAN et un client pour les secteurs de réseau régional.
Portail de nommage IPCable2Home (CNP)	Le portail CNP offre un service DNS simple pour les dispositifs IP de réseau local qui nécessitent des services de nommage.
Portail d'essais IPCable2Home (CTP)	Le portail CTP permet d'initialiser à distance des sondages par écho et des bouclages dans le réseau local.

Tableau 5-2/J.192 – Fonctions de gestion et de préconfiguration des services de portail

Fonctions de portail de gestion	Description
Serveur distant HTTP	HTTP est le protocole de transport servant à acheminer la messagerie en protocole SOAP dans le réseau local. Le dispositif PS contient un serveur HTTP qui fournit des données sur demande d'un point extrême.
Répartiteurs-vérificateurs syntaxiques XML et SOAP	Les langages SOAP et XML sont utilisés pour la messagerie dans le réseau local. Le dispositif PS contient des répartiteurs-vérificateurs syntaxiques pour ces deux langages.

Afin de communiquer avec les fonctions de gestion PS énumérées ci-dessus, les fonctions suivantes (voir le Tableau 5-3) sont censées se trouver dans les dispositifs IP du réseau local mais ne sont pas requises par la présente Recommandation.

Tableau 5-3/J.192 – Fonctions prévues de gestion et de préconfiguration des dispositifs IP du réseau local

Fonctions de client de gestion	Description
Client de serveur local IPCable2Home en protocole DHCP	La fonction de client IPCable2Home en protocole DHCP est un composant résidentiel qui est utilisé pendant le processus de préconfiguration d'un dispositif IP de réseau local afin de demander dynamiquement des adresses IP.
{texte informatif: Point de commande ou services UPnP}	{texte informatif: le protocole UPnP sert à acheminer des messages de gestion et de découverte dans le réseau local.}

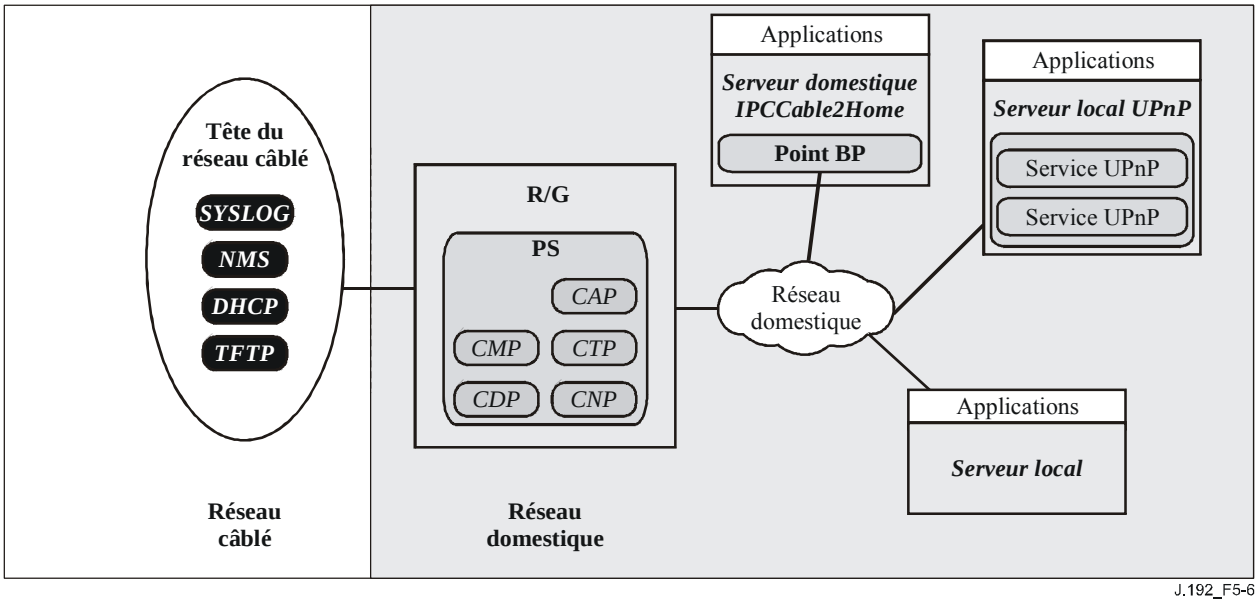


Figure 5-6/J.192 – Eléments de gestion IPCable2Home

5.2.3 Fonctions de sécurité IPCable2Home

Afin de prendre en charge les exigences de sécurité IPCable2Home (voir § 11.2.1), le modèle IPCable2Home fait appel à des fonctions de sécurité qui résident dans le réseau de données par câble, et définit des fonctions pour le dispositif PS. Les fonctions de sécurité fournies par le réseau câblé comprennent des serveurs (distants) utilisés pour la distribution de clés, le chiffrement et l'authentification. Les fonctions de sécurité des services de portail sont situées dans la passerelle résidentielle et comprennent des fonctions de client et d'autres types de fonctions. Des exemples de fonctions de sécurité fournies par le réseau câblé et par le dispositif PS sont présentés dans les Tableaux 5-4 et 5-5. Ils sont également illustrés dans la Figure 5-7.

Tableau 5-4/J.192 – Fonctions de sécuritédes services de portail

Fonctions	Description
Portail de sécurité IPCable2Home (CSP)	Le portail CSP communique avec les serveurs (distants) de sécurité de la tête de réseau. Il contient des fonctions qui assurent la participation du côté client aux processus d'authentification, d'échange de clés et de gestion de certificat. D'autres fonctions de sécurité sont la sécurité des messages de gestion, la participation aux processus de téléchargement sécurisé et la télégestion des pare-feu.
Pare-feu (FW, *firewall*)	Le pare-feu offre une fonctionnalité qui protège le réseau domestique des attaques malveillantes.

Tableau 5-5/J.192 – Fonctions de sécurité fournies par le réseau câblé

Fonctions	Description
Serveurs (distants) de centre de distribution de clés (KDC, *key distribution centre*)	Les serveurs de centre de distribution de clés (KDC) fournissent au portail CSP des services de sécurité et comportent des fonctions qui participent aux processus d'authentification et d'échange de clés.

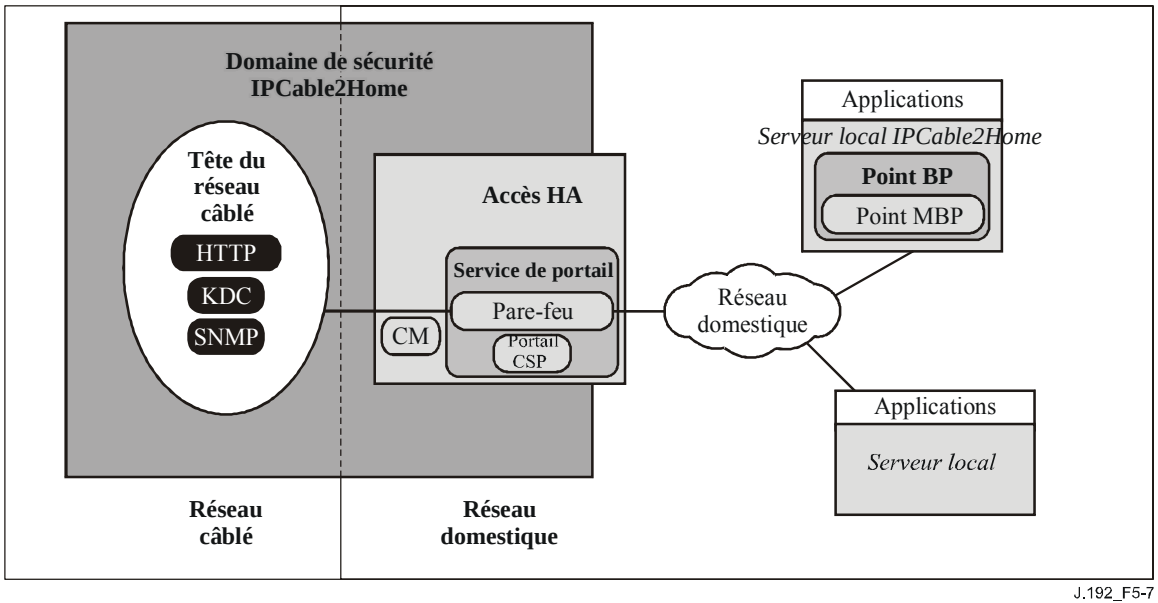


Figure 5-7/J.192 – Eléments de sécurité IPCable2Home

5.2.4 Fonctions de qualité de service IPCable2Home

Afin de prendre en charge les exigences de qualité de service (voir § 10.2.1), le modèle IPCable2Home définit des fonctions pour le dispositif PS. Les fonctions de qualité de service pour services de portail sont situées dans la passerelle résidentielle et comprennent une fonction de serveur et d'autres types de fonctions. Des exemples de fonctions de qualité de service pour services de portail et point extrême sont présentés dans les Tableaux 5-6 et 5-7. Ils sont également illustrés dans la Figure 5-8.

Tableau 5-6/J.192 – Fonctions de qualité de service pour services de portail

Fonctions	Description
Serveur distant de politique de qualité de service (QPS, *QoS policy server*)	Cette fonctionnalité conserve un répertoire de politique de qualité de service pour divers dispositifs et diverses applications à l'intérieur du réseau domestique. Elle communique la politique de qualité de service {texte informatif: lorsque celle-ci est demandée par une entité gestionnaire de qualité de service UPnP}.
Réexpédition et accès au support de la qualité de service (QFM)	La fonction QFM est chargée de la mise en file d'attente priorisée et de la réexpédition des paquets, ainsi que de l'accès au média partagé en fonction des priorités dans le service de portail.
{texte informatif: interface UPnP avec le service de dispositif de qualité de service (QD, *QoS device*)}	1) Cette interface de service déclenche le service de portail CableHome afin de négocier la qualité de service du réseau d'accès au moyen de l'interface entre le serveur local (CH) et les flux PCMM (*PacketCable MultiMedia*) pour les flux de trafic qui passent entre le réseau d'accès et le réseau domestique. 2) Cette interface reçoit les requêtes du classificateur de trafic {texte informatif: issues des entités gestionnaires de qualité de service UPnP et les place dans la base de données PS}. Ces classificateurs sont utilisés par la fonction QFM pour la classification des paquets.
Service de gestionnaire de la qualité de service (QM, *QoS manager*)	{texte informatif: dans les services de portail, un service de gestionnaire de la qualité de service UPnP fait en sorte qu'il y ait toujours au moins un service de gestionnaire de QS UPnP pour que les points de commande UPnP requièrent la qualité de service dans le réseau local domestique.}

Tableau 5-6/J.192 – Fonctions de qualité de service pour services de portail

Fonctions	Description
Fonctionnalité de qualité de service d'un point de commande du service de portail	Cette entité joue le rôle de point de commande pour différents services {texte informatif: UPnP} de qualité de service dans le réseau local domestique. La logique de découverte de la qualité de service de ce point de commande est chargée de collecter des informations relatives à la QS auprès de différents services {texte informatif: UPnP} de QS dans le réseau local domestique et de mémoriser ces informations dans la base de données PS. Cette entité recueille également les annonces, les événements et les actions à prendre en matière de qualité de service {texte informatif: UPnP} pour divers services de QS {texte informatif: UPnP}, selon les besoins.

Afin de communiquer avec les fonctions de gestion PS énumérées ci-dessus, les fonctions suivantes (voir le Tableau 5-7) sont censées se trouver dans les dispositifs IP du réseau local mais ne sont pas requises par la présente Recommandation.

Tableau 5-7/J.192 – Fonctions de qualité de service pour point extrême

Fonctions	Description
{texte informatif: UPnP QoS Control Point or Services.}	{texte informatif: la qualité de service UPnP est le protocole utilisé afin d'acheminer les messages de QS dans le réseau local.}

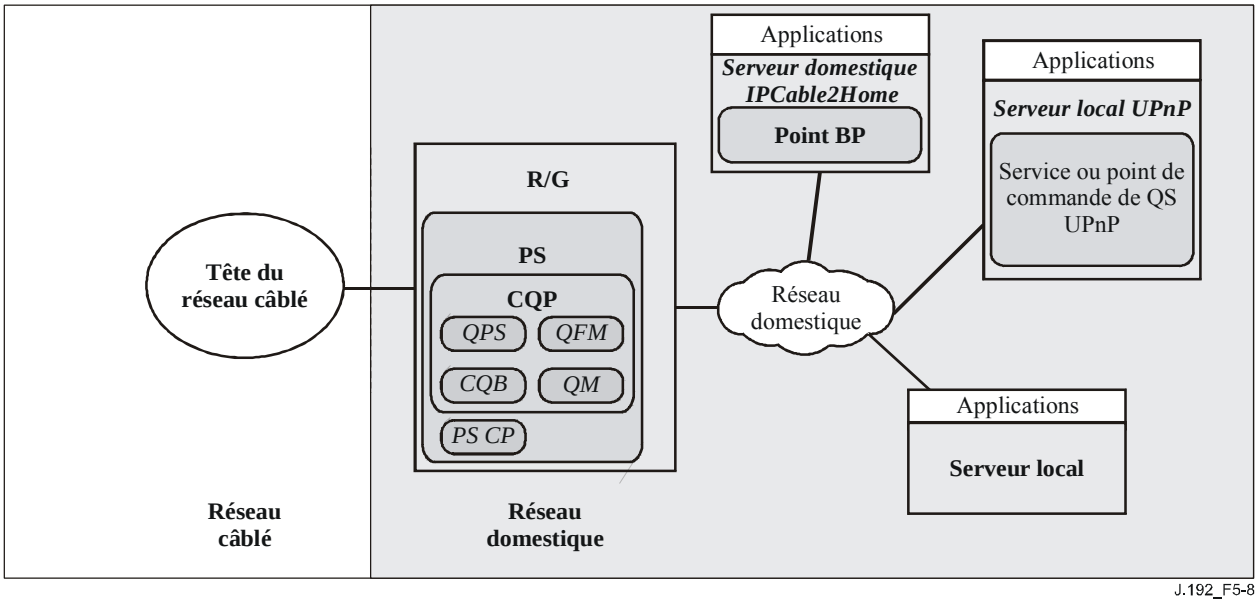


Figure 5-8/J.192 – Eléments de qualité de service IPCable2Home

5.3 Modèle d'interface de messagerie IPCable2Home

La communication entre les fonctions situées dans le réseau de données par câble, dans la passerelle résidentielle et dans les dispositifs IP de réseau local passe par les interfaces de messagerie identifiées et étiquetées dans la Figure 5-9. Les types d'interfaces de messagerie sont différenciés par les éléments qui sont impliqués dans la communication.

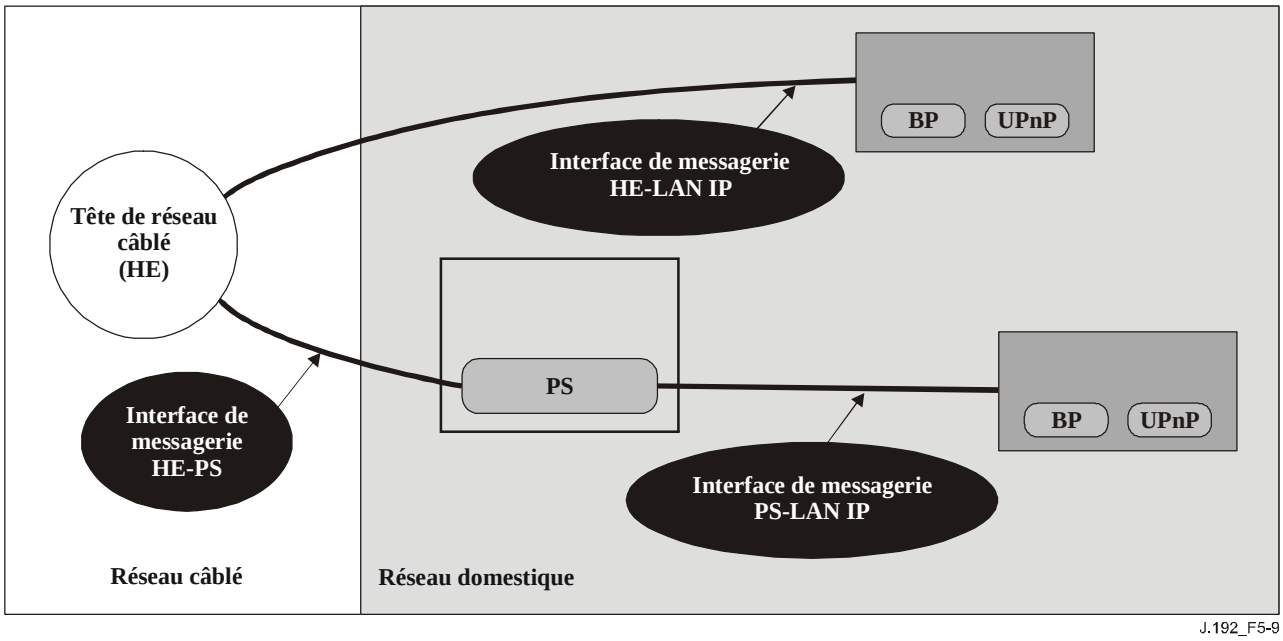


Figure 5-9/J.192 – Interfaces de référence IPCable2Home

Le Tableau 5-8 identifie les interfaces pour lesquelles le modèle IPCable2Home spécifie une messagerie.

Tableau 5-8/J.192 – Chemins d'interface valables pour chaque fonctionnalité

Fonctionnalité	Protocole	Interface		
		HE et PS	HE et dispositif IP de réseau local	PS et dispositif IP de réseau local
Service de nommage	DNS	Non spécifiée	Non spécifiée	La présente Recommandation
Téléchargement de logiciel	TFTP	La présente Recommandation	Non spécifiée	Non spécifiée
Acquisition d'adresse	DHCP	La présente Recommandation	Non spécifiée	La présente Recommandation
Gestion (simple) (en masse)	 SNMP TFTP ou HTTP	 La présente Recommandation La présente Recommandation	 Non spécifiée Non spécifiée	 Non spécifiée Non spécifiée

Tableau 5-8/J.192 – Chemins d'interface valables pour chaque fonctionnalité

Fonctionnalité	Protocole	Interface		
		HE et PS	HE et dispositif IP de réseau local	PS et dispositif IP de réseau local
Notification d'événement	SNMP SYSLOG	La présente Recommandation La présente Recommandation	Non spécifiée	Non spécifiée
Qualité de service	Protocoles de QS IPCablecom, SNMP {texte informatif: QS UPnP}	Non spécifiée La présente Recommandation Non spécifiée	IPCablecom Non spécifiée Non spécifiée	Non spécifiée Non spécifiée La présente Recommandation
Sécurité (distribution de clés)	Kerberos	La présente Recommandation	Non spécifiée	Non spécifiée
Sécurité (authentification)	Kerberos ou TLS	La présente Recommandation	Non spécifiée	Non spécifiée
Sondage par écho	ICMP	La présente Recommandation	Non spécifiée	La présente Recommandation
Bouclage/écho	UDP/TCP	Non spécifiée	Non spécifiée	La présente Recommandation
Découverte d'application	SNMP SOAP/XML	La présente Recommandation	Non spécifiée	La présente Recommandation
Découverte de dispositif	SNMP {texte informatif: découverte UPnP/SSDP}	La présente Recommandation Non spécifiée	Non spécifiée Non spécifiée	Non spécifiée La présente Recommandation

5.4 Modèle informationnel de référence IPCable2Home

Le fonctionnement du modèle de gestion est fondé sur un stockage des informations conservé dans le dispositif PS par les divers sous-éléments du dispositif PS (portails CAP, CDP, CMP, etc.). Ces sous-éléments doivent être en mesure d'interagir par échange d'informations. La base de données PS est une entité théorique qui représente la mémoire de ces informations. La base de données PS n'est pas une base de données spécifiée proprement dite, mais plutôt un outil facilitant la compréhension des informations qui sont échangées entre les divers éléments IPCable2Home.

La Figure 5-10 montre la relation entre la base de données et les fonctions de services de portail. Le Tableau 5-9 décrit les informations typiquement associées à chacune de ces fonctions. La Figure 5-11 montre un exemple détaillé d'implémentation indiquant l'ensemble des informations, les fonctions d'où découlent ces informations et les relations entre fonctions et informations.

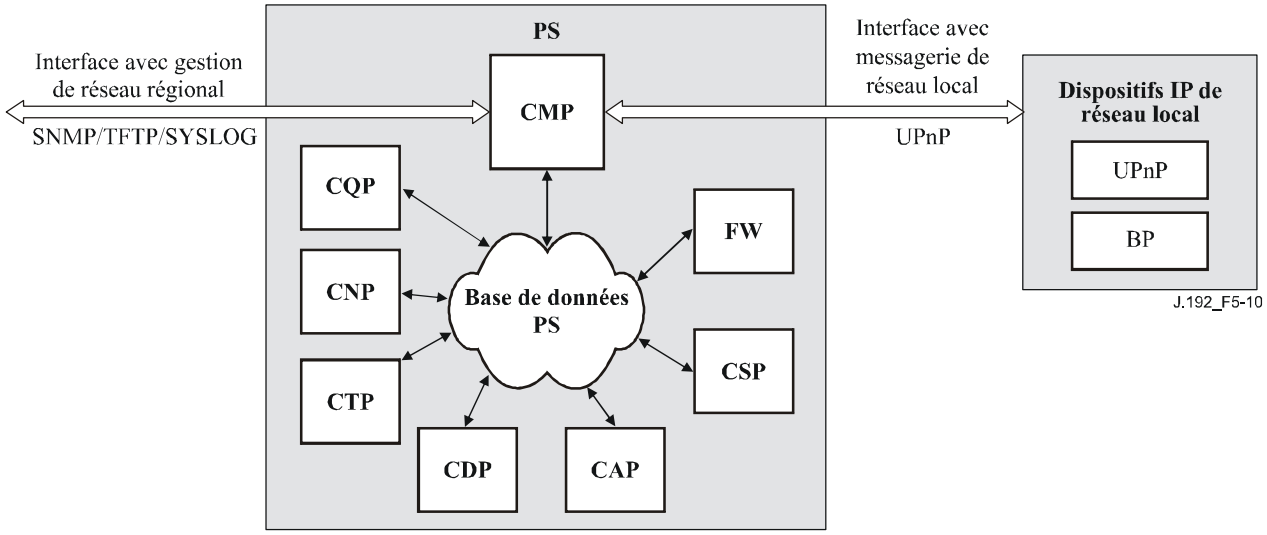


Figure 5-10/J.192 – Relation entre fonction PS et base de données PS

La base de données PS mémorise une multitude de relations entre données. Le portail CMP fournit l'interface de gestion d'un réseau régional (SNMP) à la base de données PS. Les fonctions remplies au sein des services de portail introduisent et révisent les relations entre données dans la base de données PS. De plus, les fonctions remplies au sein des services de portail peuvent restaurer des informations à partir de la base de données PS qui est tenue à jour par d'autres fonctions dans le dispositif PS.

Tableau 5-9/J.192 – Exemples typiques d'informations de base de données PS

Nom	Usage (en général)
Informations CDP	Informations associées aux adresses acquises et attribuées par protocole DHCP
Informations CAP	Informations associées aux mappages de conversion d'adresse IPCable2Home
Informations CMP	Informations associées à l'état des fonctions de services de portail. Informations sur {texte informatif: les dispositifs et services de serveur local UPnP, collectées par messagerie de découverte UPnP}.
Informations CTP	Informations associées aux résultats des essais de réseau local effectués par le portail CMP
Informations CNP	Informations associées à la résolution du nom d'un dispositif IP de réseau local
Informations USFS	Informations associées à la fonction de commutation de réexpédition sélective en amont
Informations CSP	Informations associées à l'authentification, à l'échange de clés, etc.
Informations de pare-feu	Informations associées au comportement du pare-feu (ensemble de règles), aux événements de pare-feu et à leur journalisation.
Informations d'événement	Informations associées au journal local pour tous les événements généraux, les préinterruptions, etc.
Informations de portail CQP	Politique de qualité de service reçue du câblo-opérateur et informations sur le profil de qualité de service reçues des dispositifs de serveur local de QS et des points de commande {texte informatif:UPnP, via la messagerie de qualité de service UPnP}.

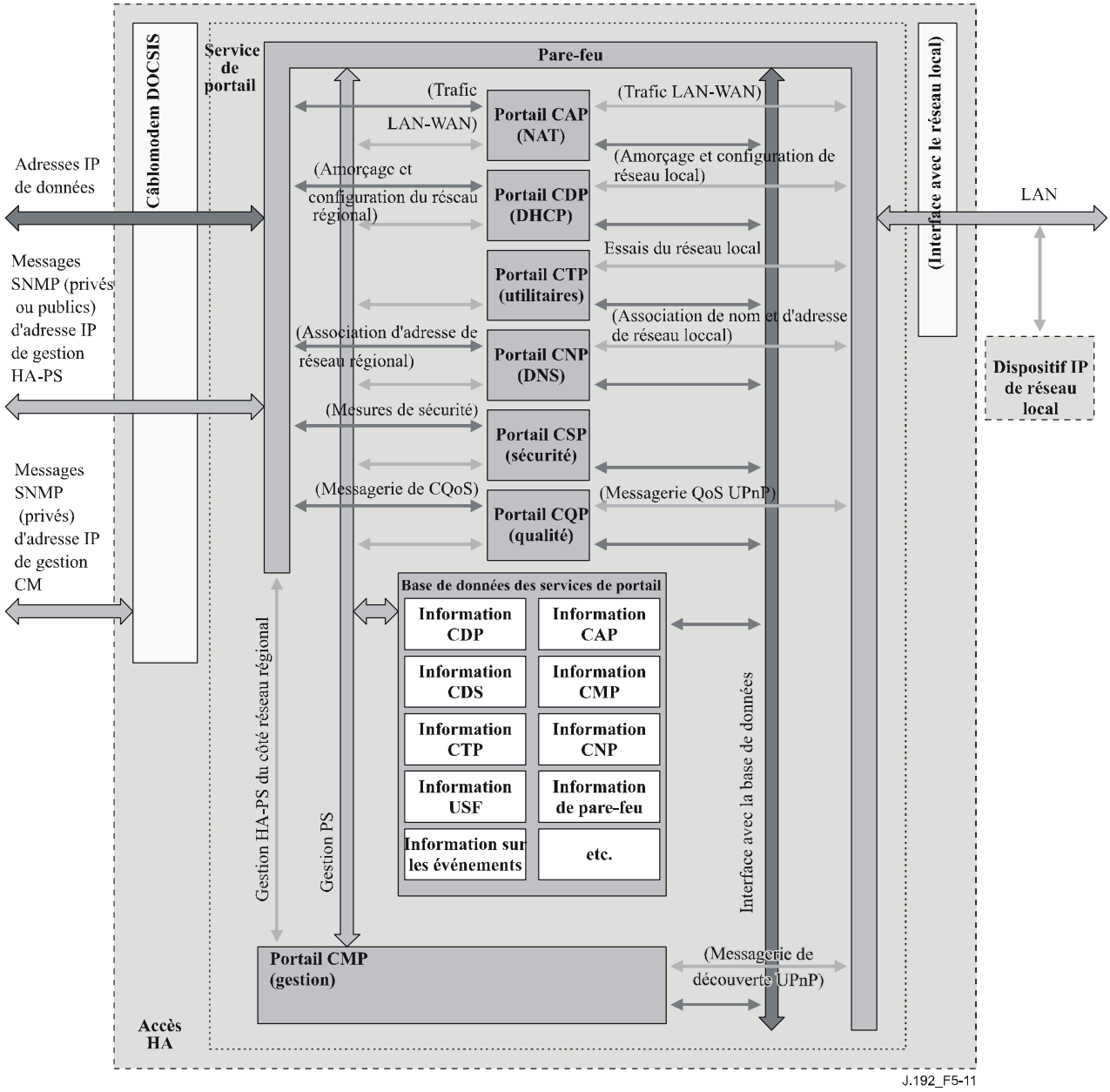


Figure 5-11/J.192 – Exemple détaillé d'implémentation d'une base de données des services de portail

Le dispositif PS est principalement géré à partir du réseau régional par le portail CMP: dans une large mesure, cela implique l'accès aux informations contenues dans la base de données PS. La gestion sert à l'initialisation et à la préconfiguration des fonctions de services de portail, ainsi qu'aux télédiagnostics ou aux états du réseau local. Les diagnostics peuvent s'appuyer sur le portail CTP afin d'obtenir une meilleure visibilité de l'état actuel du réseau local. La connexité et les performances rudimentaires du réseau peuvent être mesurées.

Le portail CNP est le serveur distant de noms de domaine (DNS, *domain name server*) du réseau local. Tous les dispositifs IP de réseau local de type LAN-Trans sont configurés par le portail CDP de façon à utiliser le portail CNP comme serveur distant de noms principal. Le portail CNP résout les noms textuels des serveurs locaux des dispositifs IP de réseau local, retourne leurs adresses IP correspondantes et, en outre, renvoie les dispositifs IP de réseau local à des serveurs DNS externes pour les demandes auxquelles les informations locales ne permettent pas de répondre.

Le portail CDP contient les fonctions d'adresse nécessaires pour prendre en charge le serveur DHCP dans le secteur LAN-Trans et implémente un client du protocole DHCP dans les secteurs de réseau régional.

Le portail CAP crée des mappages de conversion d'adresse entre les secteurs d'adresses de réseau WAN-Data et LAN-Trans. Le portail CAP est également responsable des décisions de commutation de réexpédition sélective en amont afin de préserver la largeur de bande du canal amont sur hybride HFC (réseau régional) du seul trafic local de réseau local. Enfin, le portail CAP contient la fonction de transfert, qui dérive le trafic entre les secteurs d'adresses du réseau local et du réseau régional.

Le portail CSP fournit les capacités d'authentification des services de portail ainsi que les activités d'échange de clés.

Le portail CQP fait partie d'un système qui active la qualité de service IPCable2Home. Le portail CQP offre des priorités de trafic IPCable2Home ainsi que des fonctions différenciées d'accès au support.

5.5 Modèles opérationnels IPCable2Home

La fonctionnalité de l'élément de services de portail est compatible avec diverses infrastructures de réseau câblé prises en charge par un certain nombre de différents modes de fonctionnement des services de portail, qui permettent au dispositif PS de fonctionner correctement à l'intérieur d'une infrastructure de préconfiguration de type CableModem (Rec. UIT-T J.112 ou Rec. UIT-T J.122) seulement, ainsi qu'à l'intérieur d'une infrastructure de préconfiguration CableModem plus IPCablecom. L'infrastructure de préconfiguration IPCable2Home CableModem plus IPCablecom se fonde sur les infrastructures CableModem afin d'activer des services additionnels et comprend un certain nombre de capacités qui sont semblables à celles qui se trouvent dans un système de préconfiguration IPCablecom.

Le dispositif PS peut être configuré de façon à être entièrement préconfiguré et géré par le câblo-opérateur ou peut être configuré de façon à fonctionner en tant que passerelle résidentielle non gérée et non préconfigurée (sauf pour une location d'adresse IP et une configuration fournies au moyen du protocole DHCP). En outre, un dispositif PS intégré peut être désactivé afin que le dispositif dans lequel il est implémenté puisse être déployé en tant que câblo-modem seulement.

Dans son mode entièrement préconfiguré et géré, le dispositif PS reçoit ses informations de mode opérationnel dans les messages DHCP [RFC 2131, RFC 2132] lorsqu'il démarre et demande une adresse de réseau au moyen du protocole DHCP. Selon les informations transmises dans les messages DHCP, le dispositif PS peut être configuré de façon à fonctionner dans un des deux modes de préconfiguration suivants:

- le mode de préconfiguration DHCP;
- le mode de préconfiguration SNMP.

Si le dispositif PS n'est pas configuré de façon à fonctionner soit en mode de préconfiguration DHCP ou en mode de préconfiguration SNMP, ce dispositif part du principe que la logistique administrative n'est pas actuellement disponible et va se replier par défaut sur le fonctionnement en mode CableHome inactif. En mode CableHome inactif, la passerelle résidentielle sera entièrement opérationnelle du point de vue de l'utilisateur, mais ne sera ni configurée ni gérée par l'opérateur. Si un dispositif PS est intégré dans un dispositif contenant un câblo-modem conforme au modèle [eDOCSIS], ce dispositif PS intégré peut être directement configuré par l'intermédiaire du câblo-modem, de façon à fonctionner en mode CableHome inactif. Le câblo-opérateur peut également "couper" ou désactiver la fonctionnalité de services de portail, directement au moyen du câblo-modem, dans un dispositif contenant un câblo-modem intégré et un dispositif PS intégré.

Quand le dispositif PS est configuré de façon à fonctionner en mode de préconfiguration DHCP, il peut être configuré de façon à ouvrir une session de sécurité de la couche Transport (TLS) en

protocole HTTP afin d'offrir un téléchargement sécurisé des fichiers de configuration de dispositif PS et de pare-feu.

Quand le dispositif PS fonctionne en mode de préconfiguration DHCP, il peut opérer dans un seul des deux sous-modes de gestion de réseau suivants:

- mode d'accès NmAccess;
- mode de coexistence SNMPv3.

Quand le dispositif PS est configuré de façon à fonctionner en mode de préconfiguration SNMP, il ne fonctionne qu'en mode de gestion de réseau par coexistence SNMPv3.

La Figure 5-12 décrit les divers modes de fonctionnement des services de portail ainsi que les déclencheurs associés à chacun de ces modes. Voir au § 7.3.3.2.4 (Exigences relatives au client CDC) une description complète de la détermination du mode de préconfiguration.

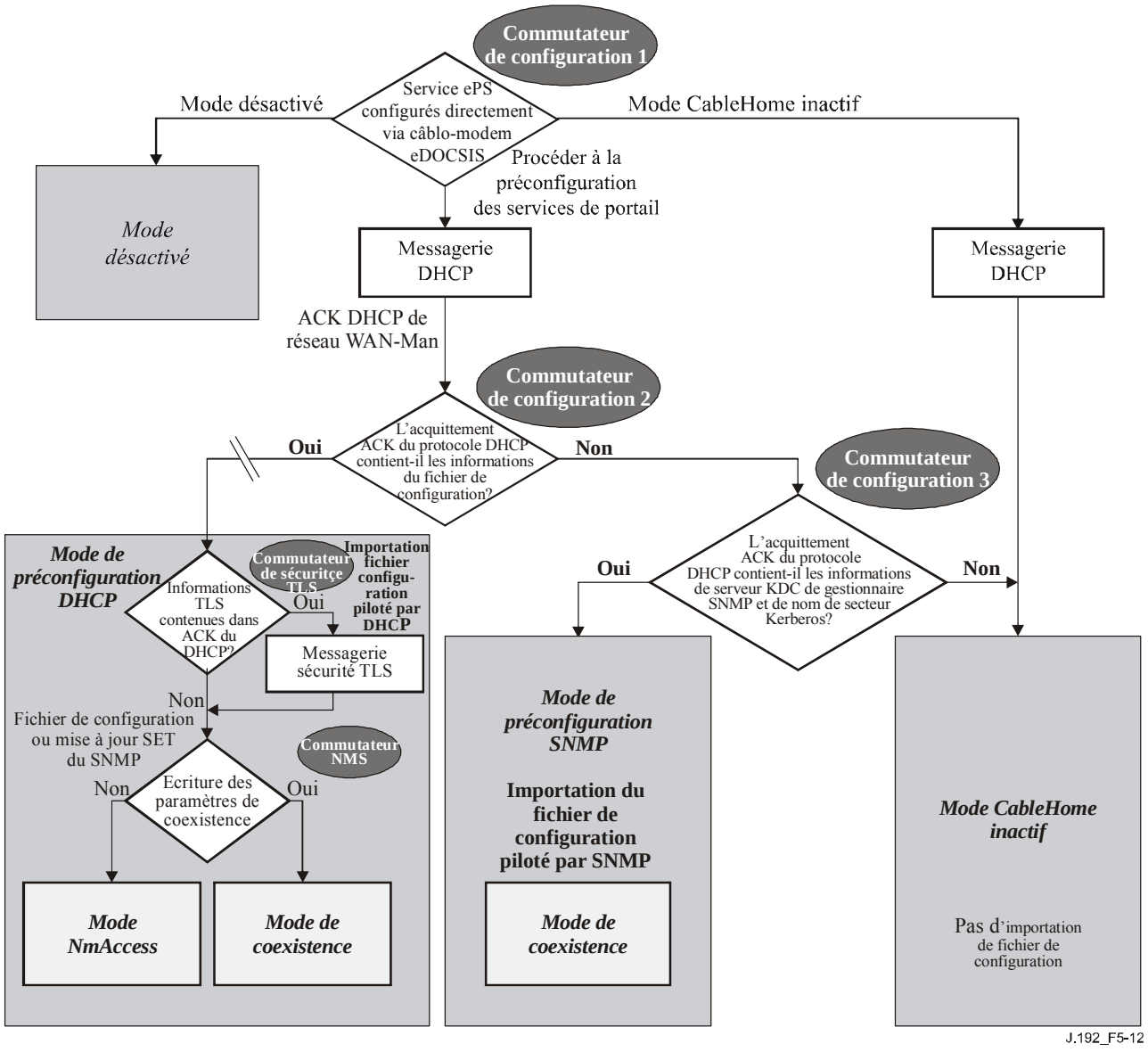


Figure 5-12/J.192 – Modes de fonctionnement des services de portail

Le Tableau 5-10 décrit les infrastructures dans lesquelles chaque mode de services de portail est destiné à fonctionner.

Tableau 5-10/J.192 – Infrastructures des services de portail

Mode	Fonctionnalité directement assurée	Infrastructure prévue
Mode de préconfiguration SNMP	Téléchargement du fichier de configuration	Infrastructure de préconfiguration CableModem plus IPCablecom
Mode de préconfiguration DHCP	Téléchargement du fichier de configuration	Infrastructures CableModem avec prise en charge du modèle IPCable2Home
Mode de préconfiguration DHCP: avec sécurité TLS/HTTP	Téléchargement sécurisé du fichier de configuration	Infrastructures CableModem avec prise en charge du modèle IPCable2Home et de la sécurité TLS
Mode de préconfiguration DHCP: mode de gestion de réseau par accès NmAccess	Version SNMP utilisée entre NMS et PS	Infrastructure J.112 (1998) (SNMP v1/v2) avec prise en charge du modèle IPCable2Home
Mode de préconfiguration DHCP: mode de gestion de réseau par coexistence SNMP	Version SNMP utilisée entre NMS et PS	Infrastructures de préconfiguration J.112 et J.122 ainsi que CableModem plus IPCablecom (SNMP v3) avec prise en charge du modèle IPCable2Home
Mode IPCable2Home inactif	Configuration et gestion	Aucune prise en charge du modèle IPCable2Home
Mode désactivé	Configuration, gestion, conversion d'adresse, réexpédition de trafic et pare-feu.	Infrastructures DOCSIS 1.0, 1.1 et 2.0 avec prise en charge IPCable2Home. Permet le déploiement d'un dispositif avec câblo-modem intégré et services de portail intégrés en tant que câblo-modem seulement.

5.6 Interfaces physiques avec la passerelle résidentielle

Il y a de nombreux types d'interfaces physiques qui peuvent être implémentés dans un dispositif contenant une fonctionnalité de services de portail. Plusieurs de ces types sont décrits dans la liste ci-dessous:

- interfaces de mise en réseau régional (WAN), avec un réseau câblé où le câblo-modem joue le rôle de pont transparent pour un dispositif PS avec un câblo-modem intégré et autres interfaces de mise en réseau régional destinées à la connexion avec un réseau régional, dans le cas d'un dispositif PS autonome;
- interfaces de mise en réseau local pour connexion à des dispositifs IP de réseau local et à des serveurs locaux IPCable2Home;
- interfaces d'essai de matériel, telles que les interfaces du groupe JTAG et d'autres approches propres à des vendeurs, qui font partie des circuits intégrés et qui ne possèdent pas toujours les commandes logicielles nécessaires pour découpler ces interfaces. Celles-ci sont des automates matériels qui restent passifs jusqu'à ce que leurs lignes d'entrée soient pointées par des données. Bien qu'elles puissent servir à lire et à écrire des données, ces interfaces nécessitent une connaissance intime des circuits intégrés et de l'arrangement de la carte imprimée, de sorte qu'elles sont difficiles à "attaquer". Des interfaces d'essai de matériel PEUVENT être présentes dans un dispositif implémentant une fonctionnalité de services de portail mais NE DOIVENT PAS être étiquetées ni décrites comme étant à l'usage du client;

- interfaces d'accès de gestion, également appelées *connecteurs de console*, qui sont des voies de communication (habituellement à la norme RS-232 mais qui peuvent être de type Ethernet, etc.) associées à un logiciel de débogage interagissant avec un utilisateur qui est invité par le logiciel à introduire des données. Le logiciel accepte les ordres de lecture et d'écriture de données dans le dispositif PS. Si le logiciel de cette interface est désactivé, la voie de communication physique l'est également. Un dispositif PS NE DOIT PAS autoriser l'accès à des fonctions PS par l'intermédiaire d'une interface d'accès de gestion. (Les fonctions PS sont définies par la présente Recommandation.) L'accès aux fonctions PS DOIT être autorisé au moyen d'interfaces spécifiquement prescrites par la présente Recommandation, p. ex. par un accès commandé par l'opérateur en protocole SNMP;
- interfaces de diagnostic en lecture seulement, qui peuvent être implémentées de nombreuses façons et qui servent à offrir aux utilisateurs d'utiles informations de débogage, de dépannage et d'état du dispositif PS. Celui-ci PEUT avoir des interfaces de diagnostic en lecture seulement;
- certains produits peuvent opter pour l'implémentation de fonctions dans les couches supérieures (comme des fonctions de réseau de transmission de données dans les locaux de clientèle), ce qui peut nécessiter une configuration par l'utilisateur. Un service de portail PEUT offrir la possibilité de configurer des fonctions autres que de type IPCable2Home. IL CONVIENT que le dispositif PS implémente une interface avec l'utilisateur permettant à celui-ci de configurer des fonctions autres que de type IPCable2Home et des fonctions de type CableHome. Il est permis que l'interface avec l'utilisateur permette à celui-ci d'accéder aux fonctions de gestion définies par le modèle CableHome (c'est-à-dire aux objets de base MIB définis par le modèle IPCable2Home) mais il est nécessaire que cette interface soit conforme aux règles d'accès configurées par le câblo-opérateur. Voir le § 6.3.3.1.4.2.2.

6 Utilitaires de gestion

6.1 Introduction/Aperçu général

Les utilitaires de gestion IPCable2Home offrent au câblo-opérateur la fonctionnalité qui lui permet de surveiller et de configurer l'élément de services de portail (PS), {texte informatif: de découvrir des dispositifs de serveur local UPnP et les services UPnP qu'ils offrent}, de vérifier à distance la connexité entre le dispositif PS et les dispositifs IP de réseau local et de signaler les événements de description d'état et d'exception dans le dispositif PS. Le présent paragraphe décrit et spécifie les exigences relatives à ces capacités.

Les différences entre les utilitaires de gestion définis dans la Rec. UIT-T J.191 et les utilitaires définis dans la présente Recommandation sont énumérées ci-dessous:

- la présente Recommandation ajoute l'exigence que les services de portail assurent la gestion SNMP à partir de toute interface avec un réseau local;
- {texte informatif: la présente Recommandation ajoute l'exigence que le dispositif PS prenne en charge la messagerie de découverte UPnP afin de permettre aux câblo-opérateurs de découvrir divers dispositifs UPnP ainsi que leurs capacités dans le réseau local domestique};
- la présente Recommandation ajoute les objets de base MIB suivants aux services de portail:
  - objets requis afin de prendre en charge la qualité de service priorisée dans le réseau local;
  - objets prenant en charge la fonctionnalité améliorée de pare-feu;
  - {texte informatif: objets permettant au câblo-opérateur de voir les attributs et les capacités de dispositifs de serveur local UPnP dans le réseau local.}

6.1.1 Objectifs

Les objectifs des utilitaires de gestion IPCable2Home sont les suivants:

- {texte informatif: permettre au câblo-opérateur de découvrir des dispositifs de serveur local UPnP;}
- offrir aux câblo-opérateurs une visibilité sur des dispositifs IP de réseau local;
- {texte informatif: offrir aux câblo-opérateurs une visibilité sur les applications et services offerts par les dispositifs UPnP;}
- définir un ensemble minimal d'utilitaires de télédiagnostic qui permettront au câblo-opérateur de vérifier la connexité entre l'élément de services de portail et tout dispositif IP de réseau local;
- offrir aux câblo-opérateurs, par les bases MIB, l'accès à des données internes de l'élément de services de portail et permettre au câblo-opérateur de surveiller des paramètres spécifiés par le modèle IPCable2Home et de configurer ou reconfigurer, selon le cas, des capacités spécifiées par le modèle IPCable2Home;
- permettre la signalisation d'exceptions et d'autres événements sous la forme de préinterruptions (préinterruptions TRAP) en protocole SNMP, de messages adressés à un journal local, ou de messages adressés à un journal du système (SYSLOG) dans le réseau câblé.

6.1.2 Hypothèses

Les hypothèses sur l'environnement de gestion de réseau IPCable2Home sont les suivantes:

- les dispositifs conformes au modèle IPCable2Home implémentent la version 4 de la suite protocolaire Internet (IPv4);
- {texte informatif: les dispositifs de serveur local UPnP implémentent des protocoles de découverte de dispositif et de service UPnP comme spécifié par l'architecture de dispositif UPnP 1.0 [UDA 1.0];}
- le protocole SNMP sert à l'échange de messages de gestion entre le système NMS du réseau câblé et le dispositif PS contenu dans le dispositif de passerelle résidentielle IPCable2Home. Le protocole SNMP donne au système NMS une visibilité sur les interfaces avec le dispositif PS, par l'accès aux données internes des services de portail et par l'intermédiaire des bases MIB requises;
- l'une quelconque des versions SNMPv1/v2c/v3 peut être utilisée comme protocole de gestion entre le système NMS et l'élément de services de portail du modèle IPCable2Home;
- les dispositifs IP de réseau local implémentent un client du protocole DHCP;
- la passerelle résidentielle IPCable2Home et les dispositifs IP de réseau local prennent en charge le protocole ICMP;
- l'utilitaire de sondage par écho (sondeur PING) fournit des fonctionnalités suffisantes pour donner au câblo-opérateur des informations sur la connexité entre l'élément de services de portail et les dispositifs IP de réseau local.

6.2 Architecture de gestion

6.2.1 Directives de conception du système

Les directives de conception du système d'utilitaires de gestion sont énumérées dans le Tableau 6-1. Cette liste donne des indications sur la mise au point des spécifications relatives aux utilitaires de gestion IPCable2Home.

Tableau 6-1/J.192 – Directives de conception du système d'utilitaires de gestion

Référence	Directives de conception du système d'utilitaires de gestion
Mgmt 1	Le dispositif PS implémentera les protocoles SNMPv1/v2c/v3 afin d'offrir l'accès aux données internes des services de portail.
Mgmt 2	Le dispositif PS sera capable d'envoyer une commande ICMP (de sondage par écho) à tout dispositif IP de réseau local spécifié par le câblo-opérateur et de mémoriser les résultats dans la base de données PS. Les résultats des essais de sondage par écho seront accessibles par les objets de base MIB de portail CTP.
Mgmt 3	Le dispositif PS sera capable d'exécuter un essai de vitesse de connexion avec un dispositif IP de réseau local spécifié par le câblo-opérateur et de mémoriser les résultats dans la base de données PS. Les résultats de l'essai à distance de vitesse de connexion seront accessibles aux objets de base MIB de portail CTP.
Mgmt 4	L'élément de services de portail sera capable de signaler les événements.
Mgmt 5	{texte informatif: l'élément de services de portail sera capable de communiquer avec les dispositifs de serveur local UPnP contenus dans les secteurs LAN-Pass et LAN-Trans pour l'échange des attributs de dispositif, des priorités de qualité de service et des informations de services et d'application de serveur local UPnP.}
Mgmt 6	Si le dispositif PS perd sa connexité avec le réseau de données par câble et ses applications, la fonction de découverte et la fonction de messagerie LAN continueront à fonctionner.

6.2.2 Description du système d'utilitaires de gestion

Comme représenté dans la Figure 6-1, l'architecture des utilitaires de gestion IPCable2Home comporte les composants suivants:

1) le portail de gestion IPCable2Home (portail CMP);
2) le portail d'essais IPCable2Home (CTP);
3) une base d'informations de gestion (MIB, *management information base*);
4) un système de gestion de réseau (NMS, *network management system*) en protocole SNMP qui fait partie du réseau câblé.

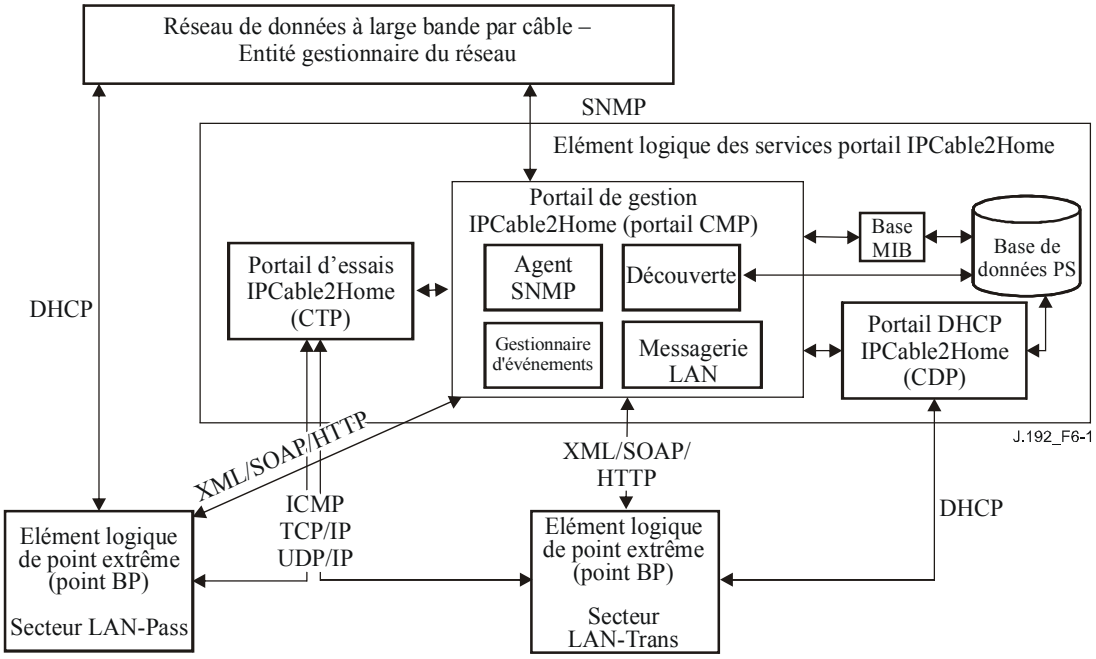


Figure 6-1/J.192 – Architecture de gestion IPCable2Home

Le système NMS du réseau de données par câble surveille et configure le dispositif PS en accédant à la base de données PS à travers les bases MIB spécifiées dans le § 6.3.3.1.4.7. {texte informatif: le câblo-opérateur accède aux attributs de dispositif de serveur local UPnP et de passerelle résidentielle IPCable2Home par la base MIB d'objets PsDev [Annexe E.4] et par la base MIB de qualité de service [Annexe E.7]. Il configure les dispositifs de serveur local IPCable2Home avec la politique de qualité de service (sous la forme de priorités de qualité de service) en utilisant le dispositif PS comme mandataire. Le dispositif PS IPCable2Home implémente un point de commande (PS CP) UPnP afin d'obtenir des informations de découverte auprès des dispositifs de serveur local UPnP.}

Le système NMS peut également communiquer directement avec les dispositifs IP de réseau local dans le secteur LAN-Pass du modèle IPCable2Home.

Le portail DHCP IPCable2Home, décrit dans le paragraphe relatif aux utilitaires de préconfiguration (§ 7), joue un rôle dans la découverte de base des dispositifs IP de réseau local. Par communication en protocole DHCP entre dispositifs IP de réseau local et portail CDP, le dispositif IP de réseau local offre son adresse matérielle et peut fournir des informations de configuration au portail CMP par les codes d'option DHCP. Le portail CMP utilisera ces informations afin de régler la valeur des objets de table d'adresses de réseau local contenus dans une base MIB du portail CDP (objet cabhCdpLanAddrTable).

Les éléments fonctionnels des portails CMP et CTP résident dans le dispositif PS. L'élément logique des services de portail peut être corésident avec un câblo-modem intégré ou être autonome, sans fonctionnalité de câblo-modem intégré, comme décrit dans le § 5.1.2.1.1.

CM et PS sont des entités de gestion distinctes et indépendantes. Dans le cas d'un dispositif PS avec câblo-modem intégré, aucun partage de données entre CM et PS n'est impliqué, sauf exceptions suivantes:

1) le téléchargement d'image logicielle est régi par la base MIB du câblo-modem;

2) la base MIB pour le protocole SNMP [RFC 3418], le groupe de bases MIB-2 du protocole SNMP (mib-2 11) [RFC 1213], le groupe IP et le groupe ICMP des bases MIB du protocole SNMPv2 pour IP [RFC 2011], ainsi que la base MIB SNMPv2 pour le protocole UDP [RFC 2013] sont autorisés à être partagés entre PS et CM.

Dans un dispositif PS avec câblo-modem intégré, les objets docsDevSoftware du câblo-modem font l'objet d'un accès afin de configurer, de lancer et de surveiller le téléchargement d'une même image logicielle combinée. Ce processus est décrit dans le § 11.8, Téléchargement sécurisé de logiciel pour le dispositif PS.

En raison de cette indépendance de gestion, le câblo-modem et le dispositif PS répondent à des adresses IP de gestion qui sont différentes et indépendantes. Les objets de base MIB d'un CM ne sont visibles que lorsque le gestionnaire y accède par l'adresse IP de gestion du modem CM. Ils ne sont pas visibles par l'adresse IP de gestion des services de portail (et vice versa). Les droits d'accès SNMP aux services de portail et aux entités CM DOIVENT être réglés indépendamment. Le modèle IPCable2Home n'exclut pas l'utilisation d'un seul agent SNMP pour un dispositif PS avec CM intégré.

L'élément de services de portail accepte les protocoles SNMPv1, SNMPv2c et SNMPv3. Le paragraphe 5.5 a présenté les modes de préconfiguration acceptés par un élément de services de portail et le § 7 donne des détails supplémentaires sur ces modes. Le mode de préconfiguration dans lequel le dispositif PS fonctionne détermine partiellement la version du protocole SNMP qui est utilisée par le dispositif PS. Des détails supplémentaires figurent au § 6.3.3.

6.3 Elément logique des services de portail – Portail de gestion IPCable2Home (portail CMP)

Le portail de gestion IPCable2Home (portail CMP) est un sous-élément de l'élément logique des services de portail. Il sert de concentrateur des commande de gestion du dispositif PS et de découvreur des dispositifs présents dans le réseau local.

Le portail CMP agrège et interconnecte les informations de gestion contenues dans les secteurs WAN-Man et LAN-Trans, car ils ne sont pas directement accessibles l'un à l'autre.

6.3.1 Objectifs du portail CMP

Les objectifs du portail de gestion IPCable2Home sont les suivants:

- permettre au système NMS de voir et de mettre à jour à distance les informations de configuration du portail d'adressage IPCable2Home (CAP);
- permettre au système NMS de voir et de mettre à jour à distance les informations de configuration du pare-feu;
- permettre des essais de connexité à distance entre la passerelle résidentielle IPCable2Home et les dispositifs IP de réseau local dans le secteur LAN-Trans, par le portail d'essais IPCable2Home (CTP);
- permettre la configuration à distance des paramètres d'adressage d'un dispositif IP de réseau local;
- permettre de voir les informations de dispositif IP de réseau local obtenues par le portail DHCP IPCable2Home (CDP);
- {texte informatif: offrir au câblo-opérateur l'accès aux attributs des dispositifs de serveur local UPnP et des services UPnP implémentés par ces dispositifs, acquis par le processus de découverte UPnP;}
- permettre de voir les résultats de la surveillance de la performance d'un dispositif IP de réseau local, assurée par le portail d'essais IPCable2Home (CTP);

- permettre au système NMS d'accéder à d'autres paramètres de configuration des services de portail;
- faciliter la sécurité en assurant l'accès aux paramètres de sécurité et l'utilisation des versions SNMPv1/v2c/v3 dans le mode de gestion de réseau approprié;
- offrir la capacité de désactiver des segments de réseau local.

6.3.2 Directives de conception du portail CMP

Les directives de conception du portail CMP sont énumérées dans le Tableau 6-2. Cette liste offre des indications pour la spécification de la fonctionnalité de portail CMP.

Tableau 6-2/J.192 – Directives de conception du système de portail CMP

Référence	Directives de conception du système de portail CMP
CMP 1	Les interfaces prendront en charge les caractéristiques et fonctions de gestion et de diagnostic nécessaires pour prendre en charge les services par câble préconfigurés dans le réseau domestique.
CMP 2	La perte de connexion entre fournisseur(s) de services à haut débit et le réseau domestique ne désactivera ni ne dégradera les fonctions internes d'établissement de réseau domestique.
CMP 3	Le réseau domestique se rétablira après une coupure de courant et les dispositifs connectés à ce réseau domestique doivent revenir à l'état opérationnel dans lequel ils se trouvaient avant la coupure.
CMP 4	Les dispositifs du réseau domestique seront faciles à installer et à configurer pour le fonctionnement, exactement comme un appareil d'utilisation domestique.
CMP 5	{texte informatif: le dispositif PS et le serveur local UPnP prendront en charge le protocole de découverte UPnP afin d'acquérir les attributs du dispositif de serveur local UPnP et sur les services UPnP qui sont implémentés par ces attributs.}
CMP 6	{texte informatif: le dispositif PS offrira au câblo-opérateur, sur demande, des informations sur les attributs du dispositif de serveur local UPnP et sur les services UPnP qui sont implémentés par ces attributs.}
CMP 7	{texte informatif: l'échange des messages du protocole de découverte dans le réseau local domestique n'en dégradera pas perceptiblement la performance.}
CMP 8	{texte informatif: la messagerie de découverte ne se propagera pas dans le réseau régional.}

6.3.3 Description du système de portail CMP

Le portail CMP est chargé des importantes capacités IPCable2Home suivantes:

- offrir des fonctions de gestion des services de portail à partir du système de gestion du réseau de transmission de données du câblo-opérateur (système NMS) en assurant l'accès à la base de données PS et à ses variables d'état au moyen des objets de base d'informations de gestion (base MIB) spécifiés par le modèle IPCable2Home;
- offrir à l'abonné une visibilité sur la base de données PS au moyen des objets de base MIB spécifiés par le modèle IPCable2Home;
- {texte informatif: permettre au gestionnaire de découvrir à distance les dispositifs connectés au réseau local et les services UPnP fonctionnant sur ces dispositifs;}
- traiter et journaliser les messages événementiels.

Le portail CMP se compose des trois fonctions suivantes afin de prendre en charge les responsabilités de gestion et de découverte énumérées ci-dessus. Ces fonctions sont également représentées dans la Figure 6-1:

1) *fonction d'agent SNMP*

   La fonction d'agent SNMP reçoit et traite les messages SNMP issus de l'interface avec un réseau régional au moyen de l'adresse IP du réseau WAN-Man, et les messages SNMP issus d'interface avec le réseau local au moyen de l'adresse IP de l'interface PS/routeur-serveur. Elle offre l'accès aux objets de base MIB afin de surveiller et/ou de configurer la fonctionnalité de dispositif PS et de dispositif IP de réseau local.

2) *Fonction de traitement des événements*

   Le portail CMP signale les événements au réseau de données du câblo-opérateur dans le réseau régional, conformément aux réglages de la table docsDevEvent. La liste des événements pris en charge figure dans l'Annexe B.

3) *Fonction de découverte*

   {texte informatif: le portail CMP, par sa fonctionnalité de découverte UPnP, acquiert des informations sur chaque dispositif de serveur local UPnP et sur les services UPnP qu'il fait fonctionner. Le portail CMP mémorise ces informations dans la base de données PS et les rend disponibles à une entité gestionnaire SNMP au moyen de la base MIB d'objets PSDev [voir § E.4] et de la base MIB d'objets QoS [voir § E.7].}

Ces fonctions sont décrites dans les § 6.3.3.1 à 6.3.3.3.

6.3.3.1 Fonction d'agent SNMP du portail CMP

6.3.3.1.1 Objectifs de la fonction d'agent SNMP

Les objectifs de la fonction d'agent SNMP du portail CMP sont énumérés ci-dessous:

- recevoir et traiter les messages SNMP reçus par l'intermédiaire des interfaces PS WAN-Man et PS/routeur-serveur (LAN);
- offrir au gestionnaire SNMP l'accès à la base de données PS au moyen des bases MIB spécifiées par le modèle IPCable2Home;
- appliquer les règles d'accès à une base de données PS, définies par la table docsDevNmAccessTable et par les points de vue du modèle VACM;
- prendre en charge les processus d'authentification et de chiffrement/déchiffrement pour le protocole SNMP, définis par les documents RFC du groupe IETF;
- observer les règles et directives d'implémentation du protocole SNMP, définies par les documents RFC du groupe IETF.

6.3.3.1.2 Fonction d'agent SNMP: directives de conception du système

Les directives de conception du système énumérées dans le Tableau 6-3 ont guidé la mise au point des exigences de la fonction d'agent SNMP.

Tableau 6-3/J.192 – Directives de conception du système

Référence	Directives
Agent SNMP 1	Le dispositif PS offrira l'accès à distance à des paramètres gérables par des bases MIB spécifiées dans la base de données PS.
Agent SNMP 2	Le dispositif PS implémentera un agent SNMP compatible avec les systèmes existants de gestion d'un réseau de transmission de données par câble.
Agent SNMP 3	Le dispositif PS prendra en charge des méthodes de contrôle d'accès permettant au câblo-opérateur de configurer le contrôle d'accès à une base de données PS.

6.3.3.1.3 Fonction d'agent SNMP – Description du système

La fonction d'agent SNMP du portail CMP sert de concentrateur des commande de gestion pour les accès du côté WAN-Man, recueille des informations pour les éléments de réseau WAN-Man et de réseau local, et en interconnecte la gestion. Elle prend également en charge la messagerie de gestion par protocole SNMP à toute interface avec un réseau local.

Le portail CMP fonctionne dans les trois modes de gestion de réseau suivants:

- mode de préconfiguration SNMP/Mode de gestion par coexistence de la version SNMPv3;
- mode de préconfiguration DHCP/Mode de gestion par table NmAccess;
- mode de préconfiguration DHCP/Mode de gestion par coexistence de la version SNMPv3.

Mode de préconfiguration SNMP/mode de gestion par coexistence avec le protocole SNMP

Comme décrit dans le § 5.5, lorsque le dispositif PS se trouve en mode de préconfiguration SNMP, il fonctionne par défaut en mode de coexistence de la version SNMPv3 sans activation des versions SNMPv1 et SNMPv2. Il fait appel au serveur Kerberos afin de distribuer les matériaux de verrouillage par clés. Le modèle de sécurité fondé sur l'utilisateur (USM, *user-based security model*) [RFC 3414] et le modèle de contrôle d'accès fondé sur le point de vue (VACM) [RFC 3415] sont pris en charge afin que le câblo-opérateur puisse implémenter la politique de gestion pour l'accès aux bases MIB spécifiées.

Mode de préconfiguration DHCP/mode de gestion par table NmAccess

Comme décrit dans le § 5.5, lorsque le dispositif PS se trouve en mode de préconfiguration DHCP, il fonctionne par défaut en mode de table NmAccess, dans lequel l'accès de gestion est régi par la table NmAccess de la base MIB de dispositif DOCSIS [RFC 2669] et dans lequel les protocoles SNMPv1/v2c sont pris en charge.

Le dispositif PS DOIT appliquer les règles suivantes afin de déterminer s'il y a lieu d'autoriser l'accès SNMP à partir d'une adresse IP de source donnée (SrcIpAddr):

si (docsDevNmAccessIp == "255.255.255.255"), autoriser l'accès à partir de toute adresse SrcIpAddr;

si (docsDevNmAccessIp ET docsDevNmAccessIpMask) == (SrcIpAddr ET docsDevNmAccessIpMask)), autoriser l'accès à partir de l'adresse SrcIpAddr.

Le dispositif PS DOIT attribuer à l'objet docsDevNmAccessIpMask la valeur par défaut 0.0.0.0.

Le Tableau 6-4 montre les règles applicables aux objets susmentionnés docsDevNmAccessIp et docsDevNmAccessIpMask en fournissant des échantillons de valeurs de base MIB et l'accès qui est accordé à chaque combinaison.

Tableau 6-4/J.192 – Exemple: accès à la base MIB accordé pour diverses valeurs des objets docsDevNmAccessIp et docsDevNmAccessIpMask

docsDevNmAccessIp	docsDevNmAccessIpMask	Accès
255.255.255.255	Tout masque d'adresse IP	Tout NMS
Toute adresse IP	0.0.0.0	Tout NMS
Toute adresse IP sauf 255.255.255.255	255.255.255.255	NMS particulier
0.0.0.0	255.255.255.255	Aucun NMS

Mode de préconfiguration DHCP/mode de gestion par coexistence de la version SNMPv3

Quand le dispositif PS fonctionne en mode de préconfiguration DHCP, le câblo-opérateur peut remplir la table de coexistence au moyen de messages SNMP de requête de mise à jour (SET) ou par fichier de configuration du dispositif PS, afin de configurer le dispositif PS de façon qu'il fonctionne en mode de gestion par coexistence de la version SNMPv3. Pour un dispositif PS configuré de façon à fonctionner en mode de coexistence de la version SNMPv3, l'accès de gestion est régi comme décrit dans le document [RFC 3584], les protocoles SNMPv1/v2c/v3 sont pris en charge, les modèles USM et VACM sont pris en charge et les matériaux SNMPv3 de verrouillage par clés sont distribués au moyen des éléments [RFC 2786] et des éléments TLV contenus dans le fichier de configuration du dispositif PS.

Le Tableau 6-5 contient les définitions des termes qui sont propres au portail CMP.

Tableau 6-5/J.192 – Définition de termes

Contrôle de gestion	Accès en lecture ou en écriture à un ensemble de paramètres qui commandent ou surveillent le comportement du dispositif PS.
Base de données de services de portail	Ensemble de paramètres qui contrôle ou surveille le comportement de l'élément de services de portail, lisible par le système de gestion du réseau régional. Il peut être conçu comme un répertoire d'informations décrivant l'état actuel du service de portail.
Utilisateur	Comme défini dans le protocole SNMP ([RFC 3414, section 2.1]), un utilisateur possède un nom qui lui est associé, des définitions de sécurité associées et un accès à une vue.
Vue	Une vue est un ensemble d'objets de base MIB assortis des droits d'accès à ces objets. Chaque vue a un nom et est associée à un utilisateur ([RFC 3415, section 2.4]).
Autorité ultime	Autorité unique qui établit, modifie ou supprime les identificateurs de l'utilisateur, les clés d'authentification, les clés de chiffrement et les droits d'accès à la base de données du service de portail. Cet utilisateur est responsable de toutes les opérations de gestion de la sécurité.
Utilisateur de maintenance	Utilisateur qui n'effectue en principe que des opérations en lecture seule sur la base de données du service de portail. Ces opérations servent surtout à effectuer la surveillance et la comptabilité.
Utilisateur-administrateur	Utilisateur qui effectue en principe à la fois des opérations de lecture et d'écriture sur la base de données du service de portail. Ces opérations servent à la configuration et la gestion des dérangements.

Exemples des types d'informations qui peuvent être lues ou manipulées par contrôle de gestion IPCable2Home: les réglages de la politique de pare-feu, les mappages de conversions NAT configurées par le système NMS, l'initialisation et l'accès aux résultats d'utilitaires de télédiagnostic, les états du dispositif PS, les informations sur le dispositif découvert et ses applications, et la configuration de l'étendue d'adressage du réseau local. Comme cela sera illustré plus loin, les diverses interfaces de messagerie de gestion peuvent disposer de droits d'accès à différents ensembles paramétriques. Un dispositif PS conforme prend en charge l'accès à la base de données PS par la hiérarchie des bases MIB à partir des deux réseaux WAN et LAN, au moyen du protocole SNMP. Les dispositifs de serveur local IPCable2Home peuvent également échanger des messages avec la passerelle résidentielle au moyen de données mises en format XML, transportées par protocole HTTPw. La Figure 6-2 indique les interfaces de messagerie de gestion:

- NMS – CMP: échange de messages de gestion entre le système NMS du réseau câblé et le portail CMP.
- CMP – Serveur local IPCable2Home/LAN-Trans: échange de messages entre le portail CMP et les serveurs locaux IPCable2Home dans le secteur LAN-Trans.
- CMP – Serveur local IPCable2Home/LAN-Pass: échange de messages entre le portail CMP et les serveurs locaux IPCable2Home dans le secteur LAN-Pass.
- NMS – Dispositif IP de réseau local: échange de messages de gestion entre le système NMS du réseau câblé et les dispositifs IP de réseau local dans le secteur LAN-Pass. Cette messagerie de gestion est hors du domaine d'application de la présente Recommandation.

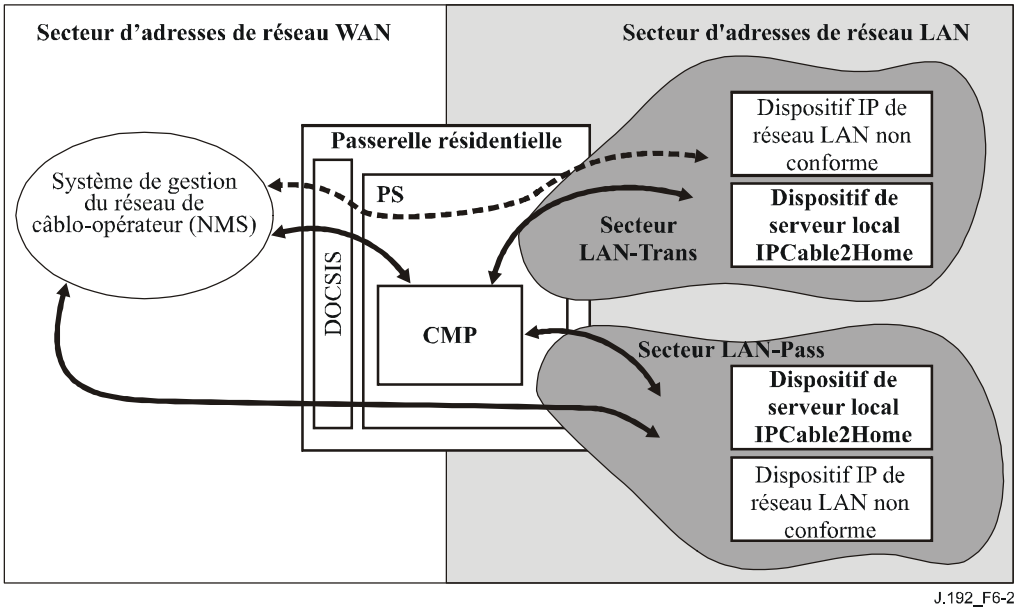


Figure 6-2/J.192 – Interfaces avec les messages de gestion IPCable2Home

Le portail CMP est essentiellement une entité à laquelle on accède (au moyen du système NMS) par un réseau régional et qui est contrôlée car ce réseau, mais qui prend également en charge l'accès à partir de l'interface PS/LAN (adresse du routeur-serveur – habituellement la passerelle par défaut pour les dispositifs IP de réseau local dans le secteur LAN-Trans). De plus, on peut faire appel au portail CMP de façon à informer en tant que de besoin le système NMS du réseau câblé au sujet de fichiers de journalisation – dans le système – d'événements ou de transferts. Un exemple d'implémentation de portail CMP est illustré dans la Figure 6-3, afin de présenter les concepts de la fonctionnalité de portail CMP.

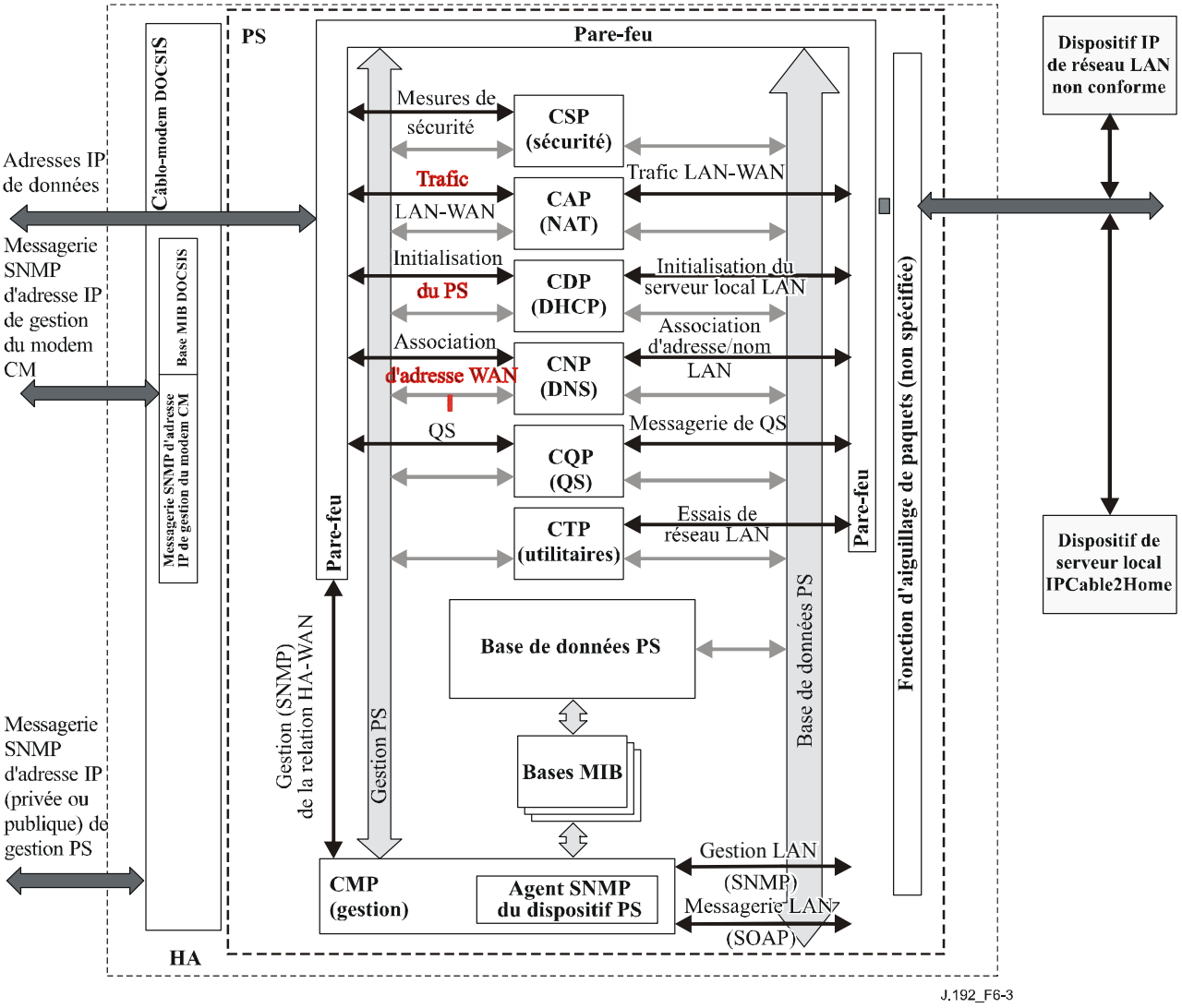


Figure 6-3/J.192 – Organigramme des services de portail

Les utilitaires de gestion du système NMS utilisent le protocole SNMP afin d'accéder aux objets et de les gérer dans le dispositif PS. Si celui-ci doit fonctionner en mode de coexistence de la version SNMPv3, ce protocole offre à l'opérateur du système NMS l'authentification de l'utilisateur auprès des services de portail, l'accès – fondé sur le point de vue – aux objets de base d'informations de gestion (base MIB) dans le dispositif PS, et le chiffrement des messages de gestion sur demande.

La fonction d'agent SNMP du portail CMP est chargée d'établir le mappage entre l'identificateur d'objet (OID) et l'instance de l'identificateur OID à tous les volets contenus dans les blocs fonctionnels des services de portail, comme le portail CAP ou un stockage local comme la base de données PS.

Un opérateur du système NMS du réseau de données par câble peut accéder aux serveurs locaux IPCable2Home – ou les gérer – de l'une des deux façons suivantes. Le câblo-opérateur peut accéder directement aux serveurs locaux IPCable2Home au moyen d'un adressage de transfert entre le réseau câblé et l'élément de dispositif de réseau local (point BP) à gérer. Le câblo-opérateur peut également accéder aux attributs du profil de dispositif BP par l'intermédiaire de la base MIB d'objets PSDev contenue dans le dispositif PS et peut accéder à une liste d'applications de point BP et à leurs priorités par l'intermédiaire de la base MIB de qualité de service contenue dans le dispositif PS. Le câblo-opérateur accède à ces bases MIB par des messages de requête SNMP de mise à jour (SET) ou par des messages de demande SNMP de requête (GET) envoyés vers l'adresse

IP de l'interface PS WAN-Man tandis que le dispositif PS, jouant le rôle de mandataire de gestion, accède à un dispositif de point BP au moyen du protocole SOAP/HTTP. Le câblo-opérateur peut approvisionner la politique de qualité de service par protocole SNMP dans le dispositif PS, sous la forme de priorités de qualité de service pour applications de serveur local IPCable2Home.

6.3.3.1.4 Exigences relatives à la fonction d'agent SNMP

Le dispositif PS DOIT implémenter un agent SNMP conforme aux documents RFC du groupe IETF comme indiqué dans le § 6.3.3.1.4.1, "Exigences relatives au protocole SNMP".

Lorsqu'il fonctionne en mode de préconfiguration DHCP ou en mode de préconfiguration SNMP (objet cabhPsDevProvMode = dhcpmode(1) ou snmpmode(2)), l'agent SNMP contenu dans le dispositif PS ne DOIT recevoir et traiter que les messages SNMP envoyés à son adresse IP du réseau WAN-Man.

Lorsqu'il fonctionne en mode de préconfiguration DHCP ou SNMP (cabhPsDevProvMode = dhcpmode(1) ou snmpmode(2)) ainsi qu'en mode primaire de traitement de paquet par conversion NAPT ou NAT (cabhCapPrimaryMode = napt(1) ou nat(2)), l'agent SNMP contenu dans le dispositif PS ne DOIT recevoir et traiter que les messages SNMP envoyés par le réseau local à son adresse de routeur-serveur de portail CDP du côté réseau local (cabhCdpServerRouter).

Lorsqu'il fonctionne en mode de préconfiguration DHCP ou SNMP (cabhPsDevProvMode = dhcpmode(1) ou snmpmode(2)) ainsi qu'en mode primaire de traitement de paquet par transfert (cabhCapPrimaryMode = passthrough(3)), l'agent SNMP contenu dans le dispositif PS ne DOIT recevoir et traiter que les messages SNMP envoyés par le réseau local à son adresse IP notoire du côté LAN du dispositif PS contenu dans le réseau local (192.168.0.1).

Lorsqu'il fonctionne en mode CableHome inactif (cabhPsDevProvMode = dormantCHmode(3)) et lorsque l'objet esafePsCableHomeModeStatus = dormantCHMode(3) [Rec. UIT-T J.126]), l'agent SNMP contenu dans le dispositif PS DOIT ignorer tous les messages SNMP issus du réseau régional et ne DOIT recevoir et traiter que les messages SNMP envoyés par le réseau local à son adresse de routeur-serveur de portail CDP du côté réseau local (cabhCdpServerRouter).

Le dispositif PS DOIT ignorer les messages SNMP reçus par l'intermédiaire d'une quelconque interface avec un réseau local et envoyés à l'adresse IP de l'interface PS WAN-Man.

Dans le cas d'un dispositif PS corésident avec un câblo-modem intégré, c'est-à-dire un dispositif PS intégré, le dispositif PS et le câblo-modem DOIVENT répondre à des adresses IP de gestion différentes et indépendantes.

Le dispositif PS DOIT implémenter les types de messages ICMP d'écho et de réponse d'écho (de types 8 et 0) comme décrit dans le document [RFC 792]. Il DOIT également répondre correctement aux demandes de sondage par écho reçues par une interface quelconque.

Si le dispositif PS doit fonctionner en mode de préconfiguration DHCP (indiqué par une valeur égale à '1' dans l'objet cabhPsDevProvMode) le dispositif PS DOIT utiliser par défaut la version SNMPv1/v2c pour la messagerie de gestion échangée avec le système NMS et suivre les règles concernant les modes de gestion NmAccess et coexistence, décrites dans le § 6.3.3.1.4.2.1, "Modes de gestion de réseau pour un dispositif PS fonctionnant en mode de préconfiguration DHCP".

Si le dispositif PS doit fonctionner en mode de préconfiguration SNMP (indiqué par une valeur égale à '2' dans l'objet de base MIB cabhPsDevProvMode), le dispositif PS DOIT utiliser la version SNMPv3 pour la messagerie de gestion avec le système NMS, conformément aux règles décrites dans le § 6.3.3.1.4.3, "Mode de gestion de réseau pour un dispositif PS fonctionnant en mode de préconfiguration SNMP".

Quand le dispositif PS doit fonctionner en mode de coexistence SNMP, le réglage par défaut d'autorité ultime DOIT être "administrateur de réseau régional" (CHAdministrator).

Le dispositif PS DOIT inclure dans l'objet sysDescr – dans l'ordre spécifié ci-dessous – la version du matériel, le nom du vendeur, la version de l'image d'amorçage en mémoire morte, la version du logiciel et le numéro du modèle (d'après [RFC 3418]). Le format des informations spécifiquement contenues dans l'objet "sysDescr" DOIT être conforme au Tableau 6-6:

Tableau 6-6/J.192 – Format des champs de l'objet "sysDescr"

Informations à signaler	Format de chaque Champ
Version du matériel	HW_REV: <version du matériel>
Nom du vendeur	VENDOR: <nom du vendeur>
Boot ROM	BOOTR: <version de mémoire d'amorçage>
Version du logiciel	SW_REV: <version du logiciel>
Numéro du modèle	MODEL: <numéro du modèle>

L'objet "sysDescr" DOIT être composé d'une liste de cinq paires de type/valeur entre doubles crochets. La séparation entre le type et la valeur est ": ", c'est-à-dire un caractère de deux points suivi d'un espace vide. Par exemple, l'objet "sysDescr" d'un dispositif PS de vendeur X, de version de matériel 5.2, de version de mémoire d'amorçage 1.4, de version du logiciel 2.2 et de numéro de modèle X apparaîtra comme suit:

texte quelconque<<HW_REV: 5.2, VENDOR: X; BOOTR: 1.4; SW_REV: 2.2; MODEL: X>>texte quelconque

Le dispositif PS DOIT signaler dans l'objet "sysDescr" au moins toutes les informations nécessaires permettant de déterminer les versions de logiciel et de politique de pare-feu que le dispositif PS est capable de prendre en charge. Si certains champs de l'objet "sysDescr" ne sont pas applicables, le dispositif PS DOIT signaler "NONE" comme valeur. Par exemple, un dispositif PS sans champ "BOOTR" va signaler "BOOTR: NONE".

La valeur de l'objet de base MIB "docsDevSwCurrentVer" DOIT contenir les mêmes informations de version du logiciel que celles qui sont contenues dans l'objet sysDescr.

Quand un dispositif PS et un câblo-modem sont intégrés dans le même dispositif, les objets sysDescr et docsDevSwCurrentVers du dispositif PS DOIVENT signaler les mêmes valeurs que celles du modem CM.

L'objet sysObjectID du groupe de système de bases MIB-2 [RFC 3418] DOIT être implémenté et DOIT persister au-delà des réinitialisations et périodes d'alimentation du dispositif.

L'objet sysUpTime objet du groupe de système de bases MIB-2 [RFC 3418] DOIT être implémenté. SysUpTime est pendant la durée qui s'est écoulée depuis la réinitialisation du système.

L'objet sysContact du groupe de système de bases MIB-2 [RFC 3418] DOIT être implémenté et DOIT persister au-delà des réinitialisations et périodes d'alimentation du dispositif. SysContact renvoie le nom de l'utilisateur ou de l'administrateur du système, s'il est connu.

L'objet sysLocation du groupe de système de bases MIB-2 [RFC 3418] DOIT être implémenté et DOIT persister au-delà des réinitialisations et périodes d'alimentation du dispositif.

L'objet sysServices du groupe de système de bases MIB-2 [RFC 3418] DOIT être implémenté et DOIT persister au-delà des réinitialisations et périodes d'alimentation du dispositif.

L'objet sysName du groupe de système de bases MIB-2 [RFC 3418] DOIT être implémenté et DOIT persister au-delà des réinitialisations et périodes d'alimentation du dispositif. L'interrogation sysName renvoie le nom du système.

La base MIB de groupe d'interfaces [RFC 2863] DOIT être implémentée conformément à l'Annexe A et aux exigences du § 6.3.3.1.4.8.

Le groupe SNMP de bases MIB-2 [RFC 3418] DOIT être implémenté.

L'objet snmpSetSerialNo du groupe snmpSet [RFC 3418] DOIT être implémenté. L'objet SnmpSetSerialNo est un verrou consultatif servant à permettre que plusieurs entités coopératives du protocole SNMPv2, agissant toutes comme gestionnaires, coordonnent leur utilisation de l'opération SET (mise à jour) du protocole SNMPv2.

Le dispositif PS DOIT compter les octets de réseau local à réseau régional et de réseau régional à réseau local comme défini par la table cabhPsDevLanIpTrafficTable [Voir § E.4], conformément à la valeur de l'objet cabhPsDevLanIpTrafficEnabled [Voir § E.4].

Quand des objets de base MIB de l'élément de services de portail sont réglés à leur valeur par défaut fixée à l'usine au moyen des objets de base MIB cabhCapSetToFactory, cabhCdpSetToFactory, cabhCtpSetToFactory, ou cabhPsDevSetToFactory, la fonctionnalité correspondante de services de portail DOIT utiliser en exploitation ces réglages par défaut fixées à l'usine sans devoir ré-approvisionner l'élément de services de portail.

6.3.3.1.4.1 Exigences relatives au protocole SNMP

Le dispositif PS DOIT observer ou mettre en œuvre, selon le cas, les documents RFC suivants du groupe IETF:

- "A Simple Network Management Protocol" (Un protocole simple de gestion de réseau) [RFC 1157];

  NOTE 1 – Cet appel à commentaires RFC a été déclaré "historique" par le document [RFC 3410]. Le dispositif PS est tenu de prendre en charge la version SNMPv1;
- "Introduction to Community-based SNMPv2" (Introduction à la version SNMPv2 du protocole fondé sur la communauté) [RFC 1901];

  NOTE 2 – Cet appel à commentaires RFC a été déclaré "historique" par le document [RFC 3410]. Le dispositif PS est tenu de prendre en charge la version SNMPv2c;
- "Introduction and Applicability Statements for Internet Standard Management Framework" (Introduction et déclarations d'applicabilité pour le cadre de gestion par la norme Internet) [RFC 3410];
- "An Architecture for Describing Simple Network Management Protocol Frameworks" (Architecture de description des cadres de gestion en protocole simple de gestion de réseau) [RFC 3411];
- "Message Processing and Dispatching for SNMP" (Traitement et distribution de messages pour le protocole SNMP) [RFC 3412];
- "Simple Network Management Applications" (Applications du protocole SNMP) [RFC 3413];
- "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol" (Modèle de sécurité fondé sur l'utilisateur (USM) pour la version 3 du protocole simple de gestion de réseau) [RFC 3414];
- "View-based Access Control Model (VACM) for the Simple Network Management Protocol" (Modèle de contrôle d'accès fondé sur le point de vue (VACM) pour la version 3 du protocole simple de gestion de réseau) [RFC 3415];
- "Version 2 of the Protocol Operations for the Simple Network Management Protocol" (Version 2 des opérations du protocole simple de gestion de réseau (SNMP)) [RFC 3416];
- "Transport Mappings for the Simple Network Management Protocol" (Mappages de transport pour le protocole simple de gestion de réseau) [RFC 3417];
- "Management Information Base (MIB) for the Simple Network Management Protocol" (Base d'informations de gestion (MIB) pour le protocole simple de gestion de réseau (SNMP)) [RFC 3418];

- "Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework" (Coexistence entre Version 1, Version 2 et Version 3 du cadre de gestion de réseau par la norme Internet) [RFC 3584].

Afin de prendre en charge la version SMIv2, le dispositif PS DOIT implémenter les documents RFC suivants du groupe IETF:

- "Structure of Management Information Version 2" (Structure des informations de gestion, version 2 (SMIv2)) [RFC 2578];
- "Textual Conventions for SMIv2" (Conventions textuelles pour la version SMIv2) [RFC 2579];
- "Conformance Statements for SMIv2" (Déclarations de conformité pour la version SMIv2) [RFC 2580].

6.3.3.1.4.2 Exigences relatives au mode de gestion de réseau

Le paragraphe 5.5 a présenté deux modes de préconfiguration (DHCP et SNMP) et deux modes de gestion de réseau (NmAccessTable et coexistence de la version SNMPv3), que le dispositif PS est tenu de prendre en charge. Les paragraphes 7.3.3.1 et 7.3.3.2 apportent des détails complémentaires sur le fonctionnement des services de portail dans chacun des deux modes de préconfiguration, en plus du mode de fonctionnement "inactif" du modèle CableHome.

Le présent paragraphe décrit les règles applicables aux modes de gestion de réseau que le dispositif PS est tenu de prendre en charge. Le paragraphe 6.3.3.1.4.2.1 et ses alinéas décrivent les modes de gestion de réseau pour un dispositif PS fonctionnant en mode de préconfiguration DHCP. Le paragraphe 6.3.3.1.4.3 et ses alinéas décrivent les modes de gestion de réseau pour un dispositif PS fonctionnant en mode de préconfiguration SNMP.

Le dispositif PS peut fonctionner en mode de gestion de réseau par coexistence SNMPv3, qu'il soit configuré de façon à fonctionner en mode de préconfiguration DHCP ou en mode de préconfiguration SNMP. Il fonctionne par défaut en mode de coexistence de la version SNMPv3 lorsqu'il est en mode de préconfiguration SNMP. Lorsqu'il fonctionne en mode de préconfiguration DHCP, le dispositif PS fonctionne par défaut en mode de gestion de réseau par table NmAccess, mais peut être configuré de façon à fonctionner en mode de coexistence de la version SNMPv3.

Le contrôle de l'accès aux bases MIB mis en œuvre par le dispositif PS dépend du mode de gestion de réseau dans lequel le dispositif PS est configuré de façon à fonctionner. Quand le dispositif PS est configuré de façon à fonctionner en mode de gestion de réseau par table NmAccess, l'accès de base MIB est régi en écriture dans l'objet docsDevNmAccessTable [RFC 2669]. Lorsqu'il fonctionne en mode de coexistence de la version SNMPv3, l'accès aux bases MIB est régi par les tables SNMPv3 ([RFC 3584], [RFC 3413], [RFC 3414] et [RFC 3415]), lesquelles peuvent être configurées par le système NMS au moyen de commandes SET (mise à jour) du protocole SNMP, ou par le fichier de configuration du dispositif PS. Le paragraphe 6.3.3.1.4.6, Mappage des champs de nuplet TLV contenus dans des rangées créées de table SNMPv3, décrit comment les paramètres de configuration du fichier de configuration du dispositif PS sont mappés dans ces tables SNMPv3.

6.3.3.1.4.2.1 Modes de gestion de réseau pour un dispositif PS fonctionnant en mode de préconfiguration DHCP

Le dispositif PS DOIT prendre en charge les protocoles SNMPv1, SNMPv2c et SNMPv3 ainsi que la coexistence avec le protocole SNMP comme décrit par les documents [RFC 3411] à [RFC 3415] et par le document [RFC 3584]. Le dispositif PS DOIT également prendre en charge le mode NmAccess comme défini par le document [RFC 2669]. La prise en charge des modes de gestion de réseau par un dispositif PS fonctionnant en mode de préconfiguration DHCP fait l'objet des directives décrites dans les § 6.3.3.1.4.2.2, 6.3.3.1.4.3 et 6.3.3.1.4.4.

6.3.3.1.4.2.2 Fonctionnement de base d'un dispositif PS fonctionnant en mode de préconfiguration DHCP

Le fonctionnement initial du dispositif PS configuré en mode de préconfiguration DHCP peut être considéré comme comportant trois étapes: 1) le comportement du dispositif PS après qu'il a été configuré en mode de préconfiguration DHCP mais avant que son mode de gestion de réseau ait été configuré par le fichier de configuration du dispositif PS; 2) la détermination du mode de gestion de réseau; 3) le comportement du dispositif PS après que son mode de gestion de réseau ait été configuré. Les règles de fonctionnement à chacune de ces étapes sont les suivantes:

1) Une fois que le dispositif PS a été configuré de façon à fonctionner en mode de préconfiguration DHCP (indiqué par une valeur d'objet cabhPsDevProvMode égale à '1' (DHCPmode)), mais avant qu'il ait été configuré pour un mode de gestion de réseau, le dispositif PS DOIT fonctionner comme suit:
   - tous les paquets SNMP sont abandonnés;
   - aucune des bases MIB du protocole SNMPv3 (base MIB de communauté, base MIB de cible, base MIB de modèle VACM, base MIB de modèle USM, base MIB de notification) n'est accessible au gestionnaire SNMP contenu dans le système NMS;
   - aucun des éléments contenus dans la base SNMP-USM-DH-OBJECTS-MIB n'est accessible au gestionnaire SNMP contenu dans le système NMS;
   - le fichier de configuration du dispositif PS spécifié dans le message OFFER du protocole DHCP est téléchargé et traité;
   - le traitement réussi de tous les éléments de base MIB contenus dans le fichier de configuration du dispositif PS DOIT être achevé avant le début du calcul des valeurs publiques dans la table USMDHKickstart.
2) Si un dispositif PS doit fonctionner en mode de préconfiguration DHCP, le contenu du fichier de configuration du dispositif PS détermine le mode de gestion de réseau, comme décrit ci-dessous:
   - le dispositif PS est en mode d'accès docsDevNmAccess du protocole SNMPv1/v2c si le fichier de configuration du dispositif PS contient SEULEMENT le réglage de table docsDevTable NmAccess pour le contrôle d'accès par protocole SNMP;
   - si le fichier de configuration du dispositif PS ne contient pas d'éléments de contrôle d'accès par protocole SNMP (docsDevNmAccessTable ou snmpCommunityTable ou TLV 34.1/34.2 ou TLV38), alors le dispositif PS est en mode d'accès NmAccess;
   - si le fichier de configuration du dispositif PS contient le réglage snmpCommunityTable et/ou un nuplet TLV de type 34.1 et 34.2 et/ou un nuplet TLV de type 38, alors le dispositif PS est en mode de coexistence SNMP. Dans ce cas, toutes les entrées effectuées dans la table docsDevNmAccessTable sont ignorées.
3) Après achèvement du processus de préconfiguration décrit dans le § 13.2 (indiqué par la valeur 'pass' (1) dans l'objet cabhPsDevProvState), le dispositif PS fonctionne dans un des deux modes de gestion de réseau. Le mode de gestion de réseau est déterminé par le contenu du fichier de configuration du dispositif PS comme décrit ci-dessus. Les règles de fonctionnement des services de portail pour chacun des deux modes de gestion de réseau sont les suivantes.

   Mode d'accès NmAccess utilisant la version SNMPv1/v2c

   - le dispositif PS DOIT traiter les paquets SNMPv1/v2c et abandonner les paquets SNMPv3;
   - la table docsDevNmAccessTable commande les destinations d'accès et de préinterruption comme décrit dans le document [RFC 2669]. Le dispositif PS fonctionnant en mode de gestion de réseau NmAccess DOIT appliquer la politique

d'accès de gestion, comme défini par la table NmAccess pour tout accès aux objets de base MIB spécifiés par le modèle IPCable2Home, sans tenir compte de l'interface (telle qu'une interface d'utilisateur graphique (GUI, *graphical user interface*) propre à un vendeur) ou du protocole d'accès utilisé;

- aucune des bases MIB du protocole SNMPv3 (base MIB de communauté, base MIB de cible, base MIB de modèle VACM, base MIB de modèle USM, base MIB de notification) n'est accessible.

Quand le dispositif PS doit fonctionner en mode d'accès NmAccess du protocole SNMP v1/v2c, il DOIT prendre en charge la capacité d'envoyer des préinterruptions comme spécifié par l'objet de base MIB suivant (extension de base MIB proposée pour la table docsDevNmAccess):

```
DocsDevNmAccessTrapVersion OBJECT-TYPE
     SYNTAX INTEGER {
               DisableSNMPv2trap(1),
               EnableSNMPv2trap(2),
                }
     MAX-ACCESS read-create
     STATUS current
     DESCRIPTION
          "Specifies the TRAP version that is sent to this NMS. Setting
          this object to disableSNMPv2trap(1) causes the trap in SNMPv1
          format to be sent to particular NMS. Setting this object to
          EnableSNMPv2trap(2) causes the trap in SNMPv2 format be sent to
          particular NMS" DEFVAL { DisableSNMPv2trap }
     ::={docsDevNmAcessEntry 8}
```

Mode de coexistence utilisant la version SNMPv1/v2c/v3

En mode de coexistence de la version SNMPv3, le dispositif PS DOIT prendre en charge les exigences spécifiées dans les § 11.4.4.1.3 et 11.4.4.1.4: "Initialisation SNMPv3" et "Changements de clé à codage Diffie-Helman". Ces exigences comprennent le calcul des paramètres publics de la table de démarrage du modèle USM à codage Diffie-Helman. Les règles de fonctionnement suivantes des services de portail s'appliquent pendant et après le calcul des paramètres (valeurs) publics comme indiqué:

Pendant le calcul des valeurs publiques de la table usmDHKickstartTable:

- le dispositif PS NE DOIT PAS permettre d'accès SNMP à partir du réseau régional;
- le dispositif PS PEUT continuer afin de permettre l'accès à partir du réseau local avec la limitation d'accès configurée par la base MIB de modèle USM, par la base MIB de communauté et par la base MIB de modèle VACM.

Après calcul des valeurs publiques de la table usmDHKickstartTable:

- le dispositif PS DOIT envoyer le message TRAP de démarrage à froid ou à chaud afin d'indiquer que le dispositif PS est maintenant entièrement gérable par la version SNMPv3;
- les paquets SNMPv1/v2c/v3 sont traités comme décrit par les documents [RFC 3411], [RFC 3412], [RFC 3413], [RFC 3414], [RFC 3415] et [RFC 3584];
- la table docsDevNmAccessTable n'est pas accessible;
- les destinations des messages de contrôle d'accès et de préinterruption sont déterminées par la table snmpCommunityTable, par la base MIB de notification, par la base MIB de cible, par la base MIB de modèle VACM et par la base MIB de modèle USM. Le dispositif PS DOIT appliquer la politique d'accès de gestion définie par la vue de modèle VACM configurée par le câblo-opérateur, pour tout accès aux objets de base MIB spécifiés par le modèle IPCable2Home, sans tenir compte de l'interface ou du protocole d'accès utilisé;

- la base MIB de communauté commande la conversion de la chaîne communautaire de paquets SNMPv1/v2c en un nom de sécurité qui choisit les entrées dans la base MIB de modèle USM. Le contrôle d'accès est offert par la base MIB de modèle VACM;
- la base MIB de modèle USM et la base MIB de modèle VACM commandent les paquets SNMPv3;
- les destinations des messages TRAP sont spécifiées dans la base MIB de cible et dans la base MIB de notification.

En cas d'échec d'achèvement de l'initialisation SNMPv3 pour un utilisateur (c'est-à-dire que le système NMS ne peut pas accéder au dispositif PS par unité PDU du protocole SNMPv3), la table d'utilisateur du modèle USM DOIT être supprimée pour cet utilisateur, le dispositif PS est en mode de coexistence et le dispositif PS ne permettra l'accès en version SNMPv1/v2c que si et seulement si les entrées de la base MIB de communauté (et les entrées qui s'y rapportent) sont configurées.

6.3.3.1.4.3 Mode de gestion de réseau pour un dispositif PS fonctionnant en mode de préconfiguration SNMP

Si le dispositif PS doit fonctionner en mode de préconfiguration SNMP après acquittement ACK en protocole DHCP (ce qui est indiqué par une valeur '2' (SNMPmode) dans l'objet cabhPsDevProvMode), ce dispositif passe en mode de coexistence de la version SNMPv3 et utilise cette version par défaut afin d'échanger des messages de gestion avec le système NMS. Il fait également appel au serveur Kerberos afin d'échanger des données de clé avec le centre KDC, conformément aux règles décrites dans le présent paragraphe. Exactement comme lorsque le dispositif PS doit fonctionner en mode de préconfiguration DHCP et a été configuré en mode de gestion de réseau par coexistence SNMPv3, quand le dispositif PS doit fonctionner en mode de préconfiguration SNMP et en mode de gestion de réseau par coexistence SNMPv3, il est tenu d'ignorer les tentatives de configurer la table docsDevNmAccessTable.

6.3.3.1.4.4 Vues de gestion

Les commandes de gestion définies pour le modèle IPCable2Home résident dans la fonction de portail CMP du dispositif PS. Les réglages fondés sur le mode de gestion définissent les droits d'accès qui sont accordés à un utilisateur pour l'accès à la base de données PS par l'intermédiaire de bases MIB spécifiées dans le modèle IPCable2Home, en protocole SNMP à partir des interfaces PS WAN-Man ou PS/routeur-serveur de LAN. Un seul utilisateur est défini par la présente Recommandation.

Le concept de vues de gestion a été présenté avec la version SNMPv3 et est défini dans les documents [RFC 3410] à [RFC 3415] et dans le document [RFC 3584]. C'est une méthode permettant de spécifier quel ou quels utilisateurs sont autorisés à accéder à quels objets de base MIB.

La Figure 6-4 décrit quelques vues de gestion possibles pour le dispositif PS. Une vue d'administrateur de réseau régional (vue CHAdministrator) et un utilisateur-administrateur de réseau régional (utilisateur CHAdministrator) sont définis par la présente Recommandation. D'autres vues et utilisateurs, comme la vue de maintenance de réseau régional, la vue d'administrateur de réseau régional, ou la vue d'utilisateur de réseau local peuvent être établis par l'autorité ultime (CHAdministrator), conformément aux règles définies dans les documents [RFC 3414] et [RFC 3415].

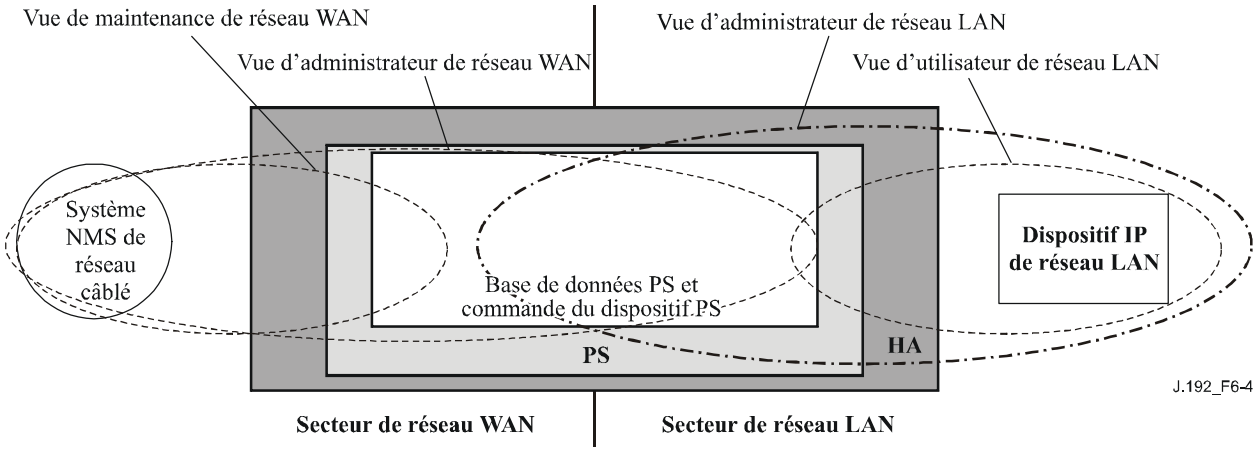


Figure 6-4/J.192 – Vues de gestion

Les paramètres gérés et définis par IPCable2Home sont mémorisés dans la base de données PS. Comme représenté dans la Figure 6-4, il y a un concept de vues d'accès à la base de données PS et à la commande de ces services qui permet une gestion simultanée à partir des deux réseaux locaux et régionaux en définissant des vues de gestion dans la base de données PS et dans la fonction de commande des services de portail. Ces vues sont un mécanisme permettant d'offrir la confidentialité et la sécurité. La politique correspondante peut être réglée séparément par l'utilisateur-administrateur IPCable2Home.

L'autorité ultime (utilisateur CHAdministrator) possède ses propres identificateurs et clés d'utilisateur, avec les responsabilités suivantes:

- établissement de toutes les vues d'accès aussi bien à l'interface de gestion de réseau local qu'à l'interface de gestion de réseau régional;
- création et gestion de tous les profils d'utilisateur, y compris les identificateurs d'utilisateur, les clés et les privilèges d'accès aux bases de données des services de portail;
- établissement de la politique d'accès du côté réseau local comme du côté réseau régional.

Des descriptions du mode de fonctionnement du modèle de contrôle d'accès fondé sur le point de vue et du modèle de sécurité fondé sur l'utilisateur sont offertes dans les documents [RFC 3414] et [RFC 3415].

La vue CHAdministrator offre un accès complet en lecture et en écriture à toutes les bases MIB spécifiées parle modèle IPCable2Home.

Les exigences relatives à la vue de gestion sont spécifiées dans le § 6.3.3.1.4.5.

6.3.3.1.4.4.1 Contrôle d'accès au réseau régional

Le modèle IPCable2Home définit deux méthodes de contrôle d'accès à des paramètres gérables au moyen de bases MIB définies par IPCable2Home. La table docsDevNmAccessTable [RFC 2669] définit l'accès de gestion lorsque le dispositif PS est en fonctionnement dans le mode de gestion de réseau NmAccess (§ 6.3.3.1.4.2.2). Lorsque le dispositif PS est en fonctionnement dans le mode de gestion de réseau par coexistence SNMPv3 (§ 6.3.3.1.4.2.2) conformément au modèle de sécurité fondé sur l'utilisateur (USM) [RFC 3414] et au modèle de contrôle d'accès fondé sur le point de vue (VACM) [RFC 3415], les réglages de cette table sont utilisés afin de commander l'accès aux objets de base MIB spécifiés par le modèle IPCable2Home, sans tenir compte de l'interface (telle qu'une interface d'utilisateur graphique) par laquelle la requête arrive. Le modèle VACM définit un ensemble de services qui peuvent être utilisés afin de vérifier les droits d'accès. Les groupes du modèle VACM définissent les droits d'accès au portail CMP.

Comme défini dans le document [RFC 3415] § 2.4, une "vue de base MIB" est un ensemble spécifique de types d'objet géré qui peuvent être définis. Ce concept est utilisé dans le modèle IPCable2Home afin d'assurer la gestion par réseau régional du dispositif PS. L'accès et la vue de l'utilisateur CHAdministrator sont spécifiés dans les § 11.4.4.1.3 et 6.3.3.1.4.5. Un exemple de séquence d'accès à une base de données PS à partir de l'interface avec un réseau régional est donné dans le § 12.3.1.

6.3.3.1.4.4.2 Sécurité

La sécurité des messages de gestion est assurée par le protocole SNMPv3. Voir au paragraphe 11 une description détaillée de la façon dont le protocole SNMPv3 est utilisé. Le portail CMP peut utiliser le protocole SNMPv3 afin de contrer les menaces identifiées dans l'Annexe C.

Afin de se protéger contre les attaques par réexécution, une horloge en temps réel sert à fournir des marqueurs temporels de messagerie. Les exigences de sécurité de la messagerie de gestion sont spécifiées dans le § 11.4.

6.3.3.1.4.5 Exigences relatives au modèle de commande d'accès fondé sur la vue (VACM)

Afin d'assurer l'accès contrôlé aux informations de gestion et la création de secteurs de gestion distincts pour un dispositif PS fonctionnant en mode de coexistence SNMPv3, le modèle de commande d'accès fondé sur la vue (VACM) DOIT être employé comme défini par le document [RFC 3415].

La vue d'administrateur de réseau régional DOIT être implémentée dans un élément de services de portail conforme. Les vues par défaut autres que la vue d'administrateur de réseau régional NE DOIVENT PAS être disponibles dans le dispositif PS. D'autres vues PEUVENT être créées par l'autorité ultime au moyen du système NMS du réseau câblé par configuration de la base MIB du modèle VACM.

La spécification d'utilisateur concernant la vue d'administrateur de réseau régional DOIT être implémentée comme suit:

vacmSecurityModel	3 (USM)
vacmSecurityName	'CHAdministrator'
vacmGroupName	'CHAdministrator'
vacmSecurityToGroupStorageType	permanent
vacmSecurityToGroupStatus	actif

La spécification de groupe pour la vue CHAdministrator DOIT être implémentée comme suit:

CHAdministrator Group	
vacmGroupName	'CHAdministrator'
vacmAccessContextPrefix	
vacmAccessSecurityModel	3 (USM)
vacmAccessSecurityLevel	AuthPriv
vacmAccessContextMatch	exact
vacmAccessReadViewName	'CHAdministratorView'
vacmAccessWriteViewName	'CHAdministratorView'
vacmAccessNotifyViewName	'CHAdministratorView'
vacmAccessStorageType	permanent
vacmAccessStatus	actif

La vue de modèle VACM pour la vue CHAdministrator DOIT être implémentée comme suit:

sous-arborescence de vue CHAdministratorView § 1.3.6.1 (base MIB entière)

6.3.3.1.4.6 Mappage des champs de nuplet TLV dans des rangées créées de table SNMPv3

Le présent paragraphe décrit en détail comment l'élément du fichier de configuration (TLV de type 38) *Récepteur de notification SNMP* est mappé dans les tables fonctionnelles SNMPv3. Voir au § 7.4.4.1.10, Récepteur de notification SNMP, une description du paramètre de configuration TLV de type 38. Les détails de la façon dont les clés de chiffrement sont échangées pour le fonctionnement du protocole SNMPv3 sont présentés dans le § 11.4.4.2.2.

Dès réception d'un élément du fichier de configuration de type 38, le dispositif PS DOIT introduire des entrées de table de base MIB conformément à la procédure décrite dans les Tableaux 6-7 (snmpNotifyTable) à 6-16 (vacmSecurityToGroupTable), au moyen des valeurs transmises dans le nuplet TLV comme décrit ci-dessous. Les tables de base MIB dont le dispositif PS est tenu de régler la valeur quand il reçoit un élément de type 38 du fichier de configuration sont énumérées ci-dessous par commodité:

- snmpNotifyTable;
- snmpTargetAddrTable;
- snmpTargetAddrExtTable;
- snmpTargetParamsTable;
- snmpNotifyFilterProfileTable;
- snmpNotifyFilterTable;
- snmpCommunityTable;
- usmUserTable;
- vacmSecurityToGroupTable;
- vacmAccessTable;
- vacmViewTreeFamilyTable.

Un fichier de configuration du dispositif PS est autorisé à contenir des éléments TLV de base MIB (de type 28) qui créent des entrées dans l'une quelconque des 11 tableaux énumérés ci-dessus.

Les tableaux contenus dans le présent paragraphe montrent comment les champs extraits de l'élément TLV du fichier de configuration du dispositif PS (les balises entre chevrons <>) sont placés dans les tables du protocole SNMPv3.

La correspondance entre champs de nuplet TLV et balises de table <TAG> est indiquée ci-dessous:

PS<IP Address> TLV 38.1

<Port> TLV 38.2

<Trap type> TLV 38.3

<Timeout> TLV 38.4

<Retries> TLV 38.5

<Filter OID> TLV 38.6

<Security Name> TLV 38.7

Ces tableaux sont représentés dans l'ordre où l'agent les explorera de haut en bas quand une notification sera produite afin de déterminer le destinataire de cette notification et la façon de remplir le paquet de notification.

snmpNotifyTable

Créer deux rangées avec des valeurs fixes, si un ou plusieurs éléments TLV sont présents.

Tableau 6-7/J.192 – snmpNotifyTable [RFC 3413]

SNMP-NOTIFICATION-MIB	Première rangée	Deuxième rangée
Nom de colonne (* = partie de l'indice)	Valeur de colonne	Valeur de colonne
* snmpNotifyName	"@PSconfig_inform"	"@PSconfig_trap"
snmpNotifyTag	"@PSconfig_inform"	"@PSconfig_trap"
snmpNotifyType	inform(2)	trap(1)
snmpNotifyStorageType	volatile	volatile
snmpNotifyRowStatus	Active(1)	Active(1)

snmpTargetAddrTable

Créer une seule rangée pour chaque élément TLV contenu dans le fichier de configuration du dispositif PS.

Tableau 6-8/J.192 – snmpTargetAddrTable [RFC 3413]

SNMP-TARGET-MIB	Nouvelle rangée
Nom de colonne (* = partie de l'indice)	Valeur de colonne
* snmpTargetAddrName	"@PSconfig_n", où n va de 0 à m – 1 et où m est le nombre d'éléments TLV de récepteur de notification contenus dans le fichier de configuration du dispositif PS.
snmpTargetAddrTDomain	snmpUDPDomain – snmpDomains
snmpTargetAddrTAddress (Adresse IP et port UDP du récepteur de notification)	Chaîne d'octets (6) Octets 1 – 4: <IP address> Octets 5 – 6: <Port>
snmpTargetAddrTimeout	<Timeout> d'après l'élément TLV
snmpTargetAddrRetryCount	<Retries> d'après l'élément TLV
snmpTargetAddrTagList	Si <Trap type> == 1, 2, ou 4 "@PSconfig_trap" Sinon si <Trap type > = 3 ou 5 "@PSconfig_inform"
snmpTargetAddrParams	"@PSconfig_n" (même valeur que snmpTargetAddrName)
snmpTargetAddrStorageType	volatile
snmpTargetAddrRowStatus	active(1)

snmpTargetAddrExtTable

Créer une seule rangée pour chaque élément TLV contenu dans le fichier de configuration du dispositif PS.

Tableau 6-9/J.192 – snmpTargetAddrExtTable [RFC 3584]

SNMP-COMMUNITY MIB	Nouvelle rangée
Nom de colonne (* = partie de l'indice)	Valeur de colonne
* snmpTargetAddrName	"@PSconfig_n", où n va de 0 à m – 1 et où m est le nombre d'éléments TLV de récepteur de notification contenus dans le fichier de configuration du dispositif PS.
snmpTargetAddrMask	<chaîne d'octets de longueur égale à zéro>
snmpTargetAddrMMS	0

snmpTargetParamsTable

Créer 1 rangée pour chaque élément TLV contenu dans le fichier de configuration. Si <Trap type> est 1, 2, ou 3, ou si le champ <Security Name> a une longueur égale à zéro, créer le tableau comme suit:

Tableau 6-10/J.192 – snmpTargetParamsTable pour <Trap Type> 1, 2, ou 3 [RFC 3413]

SNMP-TARGET-MIB	Nouvelle rangée
Nom de colonne (* = partie de l'indice)	Valeur de colonne
* snmpTargetParamsName	"@PSconfig_n", où n va de 0 à m – 1 et où m est le nombre d'éléments TLV de récepteur de notification contenus dans le fichier de configuration du dispositif PS.
snmpTargetParamsMPModel SYNTAX: SnmpMessageProcessingModel	Si <Trap type> = 1 SNMPv1(0) Sinon si <Trap type> = 2 ou 3 SNMPv2c(1) Sinon si <Trap type> = 4 ou 5 SNMPv3(3)
snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	Si <Trap type> = 1 SNMPv1(1) Sinon si <Trap type> = 2 ou 3 SNMPv2c(2) Sinon si <Trap type> = 4 ou 5 USM(3) NOTE – Le mappage vers une valeur des types du protocole SNMP est ici différent de la colonne snmpTargetParamsMPModel.
snmpTargetParamsSecurityName	"@PSconfig"
snmpTargetParamsSecurityLevel	noAuthNoPriv
snmpTargetParamsStorageType	volatile
snmpTargetParamsRowStatus	active(1)

Si le champ <Trap type> est 4 ou 5 et si le champ <Security Name> a une longueur différente de zéro, créer le tableau comme suit.

Tableau 6-11/J.192 – Tableau snmpTargetParamsTable pour <Trap Type> 4 ou 5 [RFC 3413]

SNMP-TARGET-MIB	Nouvelle rangée
Nom de colonne (* = partie de l'indice)	Valeur de colonne
* snmpTargetParamsName	"@PSconfig_n", où n va de 0 à m – 1 et où m est le nombre d'éléments TLV de récepteur de notification contenus dans le fichier de configuration du dispositif PS
snmpTargetParamsMPModel SYNTAX: SnmpMessageProcessingModel	Si <Trap type> = 1 SNMPv1(0) Sinon si <Trap type> = 2 ou 3 SNMPv2c(1) Sinon si <Trap type> = 4 ou 5 SNMPv3(3)
snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	Si <Trap type> = 1 SNMPv1(1) Sinon si <Trap type> = 2 ou 3 SNMPv2c(2) Sinon si <Trap type> = 4 ou 5 USM(3) NOTE – Le mappage vers une valeur des types du protocole SNMP est ici différent de la colonne snmpTargetParamsMPModel.
snmpTargetParamsSecurityName	<nom de sécurité>
snmpTargetParamsSecurityLevel	Niveau de sécurité du <Security Name>
snmpTargetParamsStorageType	volatile
snmpTargetParamsRowStatus	active(1)

snmpNotifyFilterProfileTable

Créer une seule rangée pour chaque nuplet TLV qui possède un champ <Filter Length> différent de zéro.

Tableau 6-12/J.192 – snmpNotifyFilterProfileTable [RFC 3413]

SNMP-NOTIFICATION-MIB	Nouvelle rangée
Nom de colonne (* = partie de l'indice)	Valeur de colonne
*snmpTargetParamsName	"@PSconfig_n", où n va de 0 à m – 1 et où m est le nombre d'éléments TLV de récepteur de notification contenus dans le fichier de configuration du dispositif PS.
snmpNotifyFilterProfileName	"@PSconfig_n", où n va de 0 à m – 1 et où m est le nombre d'éléments TLV de récepteur de notification contenus dans le fichier de configuration du dispositif PS.
snmpNotifyFilterProfileStorType	volatile
snmpNotifyFilterProfileRowStatus	active(1)

snmpNotifyFilterTable

Créer une seule rangée pour chaque TLV qui a une <Filter Length> différente de zéro.

Tableau 6-13/J.192 – snmpNotifyFilterTable [RFC 3413]

SNMP-NOTIFICATION-MIB	Nouvelle rangée
Nom de colonne (* = partie de l'indice)	Valeur de colonne
* snmpNotifyFilterProfileName	"@PSconfig_n", où n va de 0 à m – 1 et où m est le nombre d'éléments TLV de récepteur de notification contenus dans le fichier de configuration du dispositif PS.
* snmpNotifyFilterSubtree	<Filter OID > d'après l'élément TLV
snmpNotifyFilterMask	<Zero Length Octet String>
snmpNotifyFilterType	inclus(1)
snmpNotifyFilterStorageType	volatile
snmpNotifyFilterRowStatus	active(1)

snmpCommunityTable

Créer une seule rangée avec des valeurs fixes si 1 ou plusieurs éléments TLV sont présents. Il en découle que les notifications selon les versions SNMPv1 et v2c contiennent la chaîne communautaire dans le nom snmpCommunityName.

Tableau 6-14/J.192 – snmpCommunityTable [RFC 3584]

SNMP-COMMUNITY-MIB	Première rangée
Nom de colonne (* = partie de l'indice)	Valeur de colonne
* snmpCommunityIndex	"@PSconfig"
snmpCommunityName	"public"
snmpCommunitySecurityName	"@PSconfig"
snmpCommunityContextEngineID"	<The PS engine ID>
snmpCommunityContextName	<Zero length octet string>
snmpCommunityTransportTag	<Zero length octet string>
snmpCommunityStorageType	volatile
snmpCommunityStatus	active(1)

usmUserTable

Créer une seule rangée avec des valeurs fixes si un ou plusieurs éléments TLV sont présents. D'autres rangées sont créées chaque fois que l'identificateur d'automate d'un récepteur de messages TRAP est découvert. Ce tableau spécifie le nom d'utilisateur auquel les récepteurs de notifications distants doivent envoyer les notifications.

Une seule rangée est créée dans la table usmUserTable. Puis, dès que l'identificateur d'automate de chaque récepteur de notification est découvert, l'agent copie cette rangée dans une nouvelle rangée et remplace la valeur 0x00 figurant dans la colonne usmUserEngineID par la valeur qui vient d'être découverte.

Tableau 6-15/J.192 – usmUserTable [RFC 3414]

SNMP-USER-BASED-SM-MIB	Première rangée
Nom de colonne (* = partie de l'indice)	Valeur de colonne
* usmUserEngineID	0
* usmUserName	"@PSconfig" Quand d'autres rangées sont créées, celle-ci est remplacée par le champ <Security Name> d'après l'élément TLV.
usmUserSecurityName	"@PSconfig" Quand d'autres rangées sont créées, celle-ci est remplacée par le champ <Security Name> d'après l'élément TLV.
usmUserCloneFrom	<don't care> – cette rangée ne peut pas être clonée.
usmUserAuthProtocol	Néant. Quand d'autres rangées sont créées, celle-ci est remplacée par Néant ou par MD5, selon le niveau de sécurité de l'utilisateur de la version v3.
usmUserAuthKeyChange	<don't care> – écriture seulement
usmUserOwnAuthKeyChange	<don't care> – écriture seulement
usmUserPrivProtocol	Néant. Quand d'autres rangées sont créées, celle-ci est remplacée par Néant ou par DES, selon le niveau de sécurité de l'utilisateur de la version v3.
usmUserPrivKeyChange	<don't care> – écriture seulement
usmUserOwnPrivKeyChange	<don't care> – écriture seulement
usmUserPublic	<Zero length string>
usmUserStorageType	volatile
usmUserStatus	active(1)

vacmSecurityToGroupTable

Créer trois rangées avec des valeurs fixes, si un ou plusieurs éléments TLV sont présents.

Il s'agit des trois rangées ayant des valeurs fixes. Elles sont utilisées pour les entrées d'élément TLV dont le <Trap Type> est réglé à 1, 2, ou 3 ou dont le champ <Security Name> a une longueur égale à zéro.

Tableau 6-16/J.192 – vacmSecurityToGroupTable [RFC 3415]

SNMP-VIEW-BASED-ACM-MIB	Première rangée	Deuxième rangée	Troisième rangée
Nom de colonne (* = partie de l'indice)	Valeur de colonne	Valeur de colonne	Valeur de colonne
* vacmSecurityModel	SNMPv1(1)	SNMPv2c(2)	USM(3)
* vacmSecurityName	"@PSconfig"	"@PSconfig"	"@PSconfig"
vacmGroupName	"@PSconfigv1"	"@PSconfigv2"	"@PSconfigUSM"
vacmSecurityToGroupStorageType	volatile	volatile	volatile
vacmSecurityToGroupStatus	active(1)	active(1)	active(1)

6.3.3.1.4.7 Exigences relatives aux bases MIB IPCable2Home

Le dispositif PS DOIT met en œuvre chacun des objets de base MIB énumérés dans l'Annexe A. Si la colonne "Objet persistant" concernant un objet de base MIB énuméré dans l'Annexe A contient la valeur "oui", le dispositif PS DOIT conserver la valeur de cet objet après un cycle d'alimentation ou un réamorçage du dispositif PS, en rendant accessible à un gestionnaire SNMP, immédiatement après une préconfiguration complète (objet cabhPsDevProvState = pass(1)) effectué à la suite d'un réamorçage, la valeur qui était accessible à ce gestionnaire SNMP immédiatement avant ce réamorçage.

Les objets de base MIB requis proviennent des documents relatifs aux bases MIB suivantes:

- base MIB de groupe d'interfaces [RFC 2863];
- base MIB de dispositif DOCSIS par câble [RFC 2669];
- base MIB de définition CableLabs [voir § E.6];
- base MIB de dispositif PsDev IPCable2Home [voir § E.4];
- base MIB de portail CAP IPCable2Home [voir § E.1];
- base MIB de portail CDP IPCable2Home [voir § E.2];
- base MIB de portail CTP IPCable2Home [voir § E.3];
- base MIB de sécurité IPCable2Home [voir § E.5];
- base MIB d'objets de qualité de service IPCable2Home [voir § E.7];
- [draft-ietf-ipcdn-bpiplus-mib-05];
- base MIB du protocole IP (SNMPv2) [RFC 2011];
- base MIB du protocole UDP (SNMPv2) [RFC 2013];
- clé de modèle USM à codage Diffie-Helman [RFC 2786];
- base MIB d'adresses INET [RFC 3291];
- base MIB d'objets DOCS IF [RFC 2670];
- base MIB d'objets ifType IANA [IANAType];
- base MIB d'objets IEEE 802.11 [802dot11MIB].

Dans une passerelle résidentielle IPCable2Home ou dans tout autre dispositif comportant un dispositif PS intégré et un câblo-modem intégré, l'entité gestionnaire du câblo-modem et l'entité gestionnaire des services de portail (portail CMP) DOIVENT répondre à des adresses IP de gestion différentes et indépendantes. La Rec. UIT-T J.112 et la présente Recommandation spécifient certains objets de base MIB qui leur sont communs mais, si un câblo-modem conforme à la Rec. UIT-T J.112 et un élément PS conforme au modèle IPCable2Home sont intégrés dans le même dispositif, chacun est tenu de conserver sa propre instance distincte des objets de base MIB spécifiés, accessibles par différentes adresses IP de gestion, à l'exception du groupe SNMP de bases MIB 2 et de la base MIB du protocole SNMPv2, qui PEUVENT être communs et partagés entre le câblo-modem et l'élément de services de portail, et qui PEUVENT être accessibles par l'adresse IP de gestion du câblo-modem ou par l'adresse IP de gestion du dispositif PS.

Dans un dispositif PS avec câblo-modem intégré, le téléchargement du logiciel de l'image unique des logiciels combinés du câblo-modem et des services de portail est régi par le câblo-modem. Les objets suivants du groupe docsDevSoftware [RFC 2669] NE DOIVENT PAS être implémentés dans un dispositif PS avec un câblo-modem intégré, c'est-à-dire que ces objets NE DOIVENT être accessibles que par l'adresse IP de gestion du câblo-modem contenu dans un dispositif PS avec CM intégré:

- docsDevSwServer;
- docsDevSwFilename;

- docsDevSwAdminStatus;
- docsDevSwOperStatus.

Le groupe d'objets docsDevSoftware DOIT être implémenté dans un dispositif PS autonome. La modification des objets docsDevSoftware (comme spécifié dans le § 11.8.4) par le câblo-opérateur en vue du téléchargement de l'image logicielle du dispositif PS autonome DOIT se traduire par une opération correcte et sécurisée de téléchargement de logiciel.

Dans un dispositif PS avec câblo-modem intégré, les objets de base MIB de câblo-modem NE DOIVENT être visibles et accessibles QUE quand le gestionnaire y accède par l'adresse IP de gestion du câblo-modem et NE DOIVENT PAS être visibles ou accessibles au moyen d'une quelconque adresse IP de services de portail, à l'exception du groupe SNMP de bases MIB 2 et de la base MIB SNMPv2, dont les objets sont autorisés à être partagés entre les entités de gestion CM et PS.

Dans un dispositif PS avec câblo-modem intégré, les objets de base MIB spécifiés par le modèle IPCable2Home NE DOIVENT être visibles et accessibles QUE quand le gestionnaire y accède par l'adresse IP de gestion des services de portail (adresse IP de l'interface PS WAN-Man) ou par l'adresse IP de l'interface PS/routeur-serveur du réseau local et NE DOIVENT PAS être visibles ou accessibles par l'adresse IP de gestion du câblo-modem, à l'exception du groupe SNMP de bases MIB 2 et de la base MIB SNMPv2 dont les objets sont autorisés à être partagés entre les entités de gestion CM et PS.

La hiérarchie générale des bases MIB est illustrée dans la Figure 6-5. Les identificateurs OID spécifiquement requis pour les bases MIB individuelles sont énumérés dans l'Annexe A.

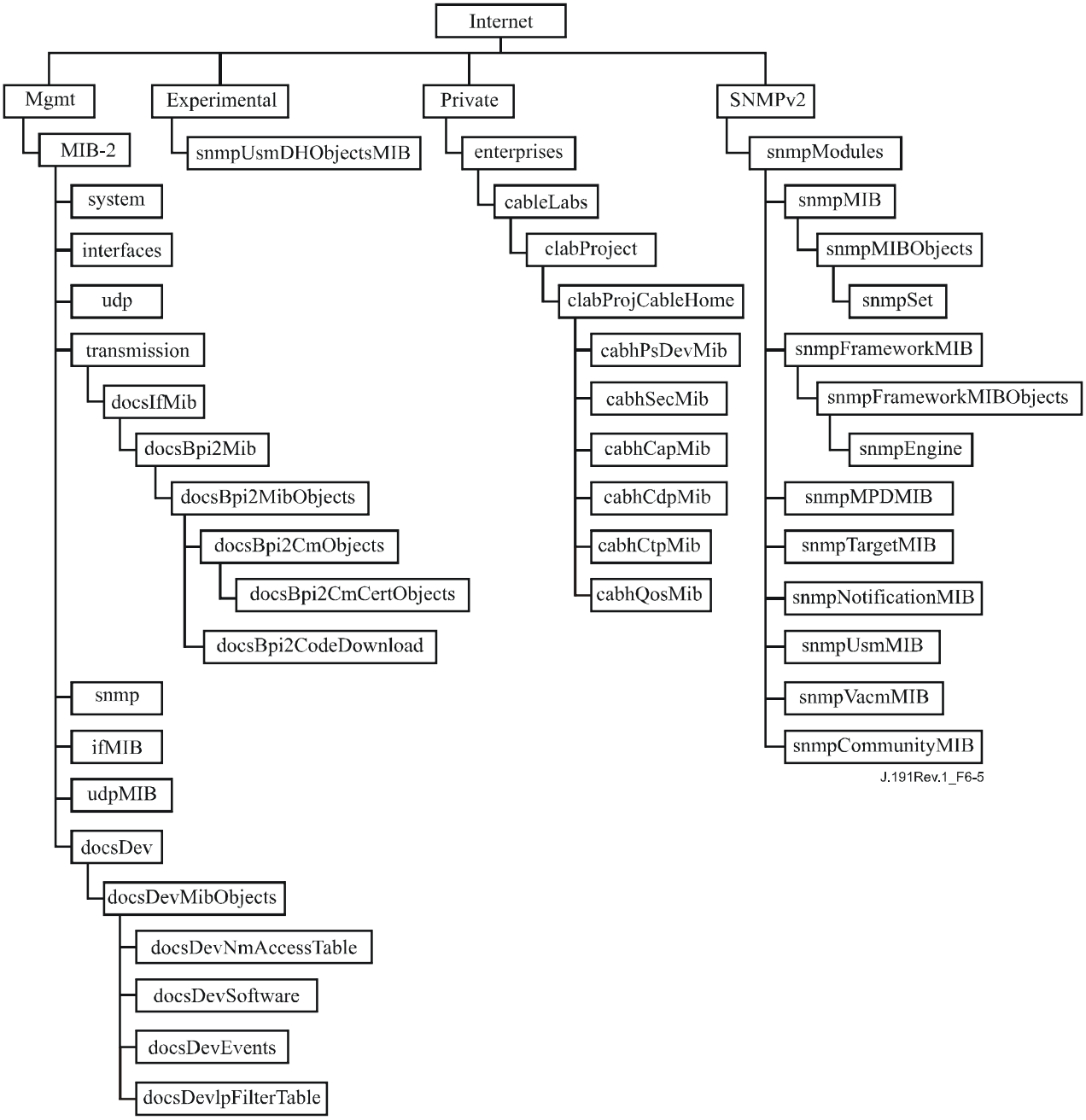


Figure 6-5/J.192 – Hiérarchie des bases MIB dans le modèle IPCable2Home

6.3.3.1.4.8 Base MIB de groupe d'interfaces

La base MIB de groupe d'interfaces [RFC 2863] offre un outil puissant afin de permettre aux câblo-opérateurs de comprendre l'état et de voir les statistiques de toutes les interfaces physiques avec l'élément de services de portail. Une *interface physique* est un élément pour lequel un connecteur est exposé à l'extérieur de l'enveloppe du dispositif et pour lequel l'objet *ifConnectorPresent* est Vrai. Afin de permettre une utilisation intelligente de cette base MIB, un système de numérotage des interfaces est essentiel. Il est donc nécessaire que les éléments de services de portail soient conformes aux exigences suivantes:

le dispositif PS DOIT implémenter une instance de l'objet ifEntry pour l'interface entre l'élément PS et le WAN-Data, même si cette interface est interne – comme cela se produit dans le cas d'un dispositif PS intégré utilisant une solution à microcircuit intégré.

Le dispositif PS DOIT implémenter une instance de l'objet ifEntry pour chaque interface physique avec un réseau local de l'élément de services de portail.

Le dispositif PS DOIT DOIT implémenter une instance de l'objet ifEntry pour une interface du groupe des "interfaces avec le côté signaux résultants de réseau local" qui est identifiée par la valeur d'indice ifIndex 255.

Le dispositif PS DOIT implémenter une instance de l'objet ifEntry pour une interface (virtuelle) du groupe des "interfaces avec le côté signaux résultants de réseau local sans fil" représentant le surensemble de toutes les interfaces physiques avec un réseau local sans fil qui sont implémentées dans le produit et qui sont identifiées par la valeur d'indice ifIndex 254.

Les interfaces de la table ifTable des services de portail DOIVENT être numérotées comme représenté dans le Tableau 6-17.

Tableau 6-17/J.192 – Numérotage des interfaces dans la table ifTable

Interface	Description
1	Interface avec réseau WAN-Man
2	Interface avec réseau WAN-Data
2 + n	Interface avec chaque réseau local
254	Interface avec côté résultant d'un réseau local sans fil
255	Interface avec côté résultant de réseau local

Si le statut ifAdminStatus d'une interface donnée a la valeur "down", cette interface NE DOIT PAS accepter ou réexpédier un quelconque trafic. L'objet ifAdminStatus correspondant à la valeur 255 de l'indice ifIndex DOIT assurer la commande administrative de toutes les interfaces avec un réseau local et DOIT être implémenté en lecture-écriture.

Le dispositif PS DOIT attribuer la valeur other(1) aux entrées ifType de l'objet ifTable [RFC 2863] correspondant à l'indice ifIndex 255. Le dispositif PS DOIT attribuer la valeur other(1) aux entrées ifType de l'objet ifTable correspondant à l'indice ifIndex 254. Un élément PS intégré DOIT attribuer la valeur other(1) aux entrées ifType de l'objet ifTable correspondant aux valeurs 1 et 2 de l'indice ifIndex. Un élément PS autonome DOIT attribuer la valeur appropriée du type IANAifType [IANAType] à l'entrée ifType de l'objet ifTable correspondant aux valeurs 1 et 2 de l'indice ifIndex.

La valeur de l'objet ifTable ifPhysAddress correspondant à l'indice ifIndex 255 DOIT être une chaîne d'octets de longueur égale à zéro.

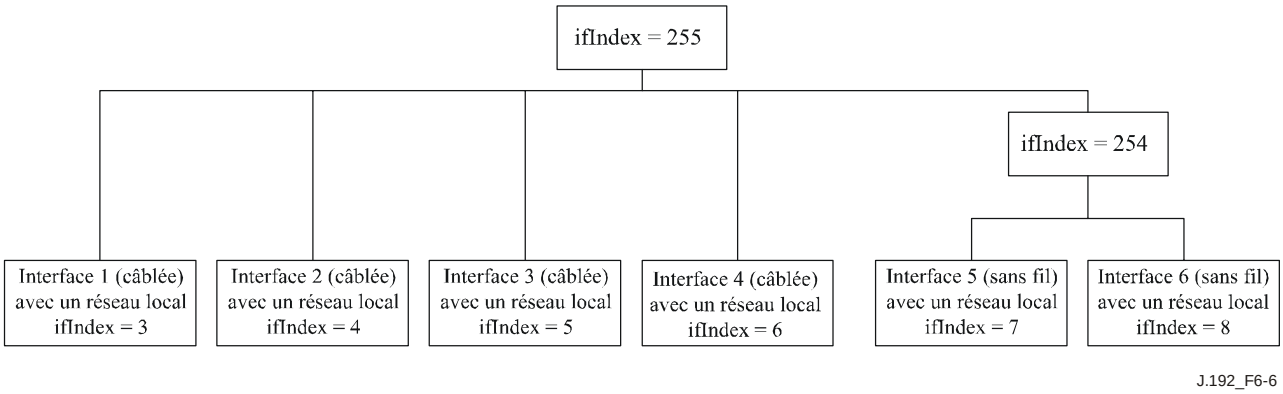
La valeur de l'objet ifTable ifPhysAddress correspondant à l'indice ifIndex 254 DOIT être une chaîne d'octets de longueur égale à zéro.

Les compteurs d'interfaces avec un réseau régional ayant les valeurs 1 et 2 d'indice ifIndex dans la table ifTable DOIVENT être partagés entre les deux interfaces. Le dispositif PS Peut implémenter des compteurs ifTable pour les valeurs 254 et 255 de l'indice ifIndex.

Les interfaces avec le dispositif PS DOIVENT être implémentées conformément aux définitions relatives aux couches et aux sous-couches décrites dans le § 3.1 du document [RFC 2863], toutes les interfaces PS d'indice compris entre 3 et 254 étant implémentées en tant que sous-couches de l'interface 255 et toutes les interfaces physiques entre PS et réseau local sans fil étant implémentées en tant que sous-couches de l'interface 254.

Le groupe de pile d'interfaces (groupe ifStack) selon [RFC 2863] DOIT être implémenté afin d'identifier les relations entre l'interface de couche supérieure avec le groupe des "interfaces du côté signaux résultants de réseau local" et les sous-interfaces (câblées) de couche inférieure avec un réseau local; afin d'identifier la relation entre l'interface de couche supérieure avec le groupe des

"interfaces du côté signaux résultants d'un réseau local" et l'interface de couche inférieure avec le groupe des "interfaces du côté signaux résultants de réseau local sans fil"; et afin d'identifier la relation entre l'interface avec le groupe des "interfaces du côté signaux résultants d'un réseau local sans fil" et les sous-interfaces de couche inférieure avec un réseau local sans fil. La Figure 6-6 décrit l'utilisation du groupe ifStack dans un dispositif PS possédant quatre interfaces câblées et deux interfaces sans fil avec un réseau local.



Implémentation du groupe ifStack dans cet exemple:

ifStackHigherLayer	0	1	0	2	0	255	255	255	255	255	254	254	3-8
ifStackLowerLayer	1	0	2	0	255	3	4	5	6	254	7	8	0

Figure 6-6/J.192 – Exemple d'implémentation du groupe ifStack

6.3.3.1.4.9 Base MIB d'objets de réseau local sans fil selon IEEE 802.11

Si le dispositif PS implémente la fonctionnalité de réseau local sans fil selon IEEE 802.11, alors le dispositif PS DOIT prendre en charge la base MIB d'objets de réseau local sans fil 802.11 et les extensions applicables à l'implémentation selon [802.11A-1999], [802.11B/Cor1-2001], [802.11D], [802.11G-2003], comme spécifié dans l'Annexe A.

Tableau 6-18/J.192 – Exigences relatives au module de base MIB d'objets IEEE 802.11

Structure de la base MIB	Notes
dot11StationConfigEntry	Requis
dot11WEPDefaultKeysTable	Requis
dot11PrivacyEntry	Requis
dot11OperationEntry	Requis
dot11PhyTxPowerEntry	Requis
dot11PhyDSSSEntry	Requis pour 802.11B et 802.11G
dot11PhyOFDMTable	Requis si 802.11A est pris en charge
cabhPsDev802dot11BaseTable	Requis
dot11AuthenticationAlgorithmsEntry	Facultatif
dot11MultiDomainCapabilityEntry	Facultatif
dot11PhyOperationEntry	Facultatif
dot11RegDomainsSupportEntry	Facultatif
dot11SupportedDataRatesTxEntry	Facultatif

Tableau 6-18/J.192 – Exigences relatives au module de base MIB d'objets IEEE 802.11

Structure de la base MIB	Notes
dot11SupportedDataRatesRxEntry	Facultatif
dot11PhyHRDSSSTable	Facultatif seulement si 802.11B est pris en charge
dot11PhyERPTable	Facultatif seulement si 802.11G est pris en charge

Les paragraphes suivants détaillent les exigences spécifiques IPCable2Home applicables à celles qui sont énumérées dans le Tableau 6-18 pour cette base MIB .

6.3.3.1.4.9.1 Exigences spécifiques de base MIB 802.11

Les objets de base MIB 802.11 non énumérés dans l'Annexe A sont considérés comme FACULTATIFS, et PEUVENT ne pas avoir besoin d'être instanciés dans les tableaux requis.

Si les objets de base MIB 802.11 FACULTATIFS ici définis sont instanciés, cela indique que les primitives de protocole associées à la couche de gestion PHY ou MAC sont implémentées, et donc que les valeurs DOIVENT être signalées en conséquence, à savoir:

– les compteurs et statistiques DOIVENT s'incrémenter sur la base de leurs opérations;

– les objets de base MIB dynamique avec SYNTAXE de lecture seulement DOIVENT signaler des valeurs exactes;

– les objets de base MIB configurable avec SYNTAXE de lecture-écriture PEUVENT être implémentés comme étant en lecture seulement.

6.3.3.1.4.9.1.1 Exigences pour dot11StationConfigEntry

Les objets de base MIB dot11BeaconPeriod, dot11DTIMPeriod et dot11AssociationResponseTimeOut PEUVENT être implémentés comme étant en lecture seulement.

L'objet de base MIB dot11OperationalRateSet, qui PEUT avoir un accès en lecture seulement, DOIT correspondre aux valeurs contenues dans le contexte de l'objet cabhPsDev802dot11PhyOperMode. Si l'objet de base MIBdot11OperationalRateSet implémente un accès en lecture-écriture , une opération "SET" du protocole SNMP à un débit binaire non contenu dans le contexte de l'objet cabhPsDev802dot11PhyOperMode DOIT signaler une erreur SNMP 'wrongValue'.

La prise en charge d'éléments de service multidomanial [802.11D] varie selon le domaine administratif, en particulier pour le domaine administratif 0x00 (FCC) (US), la prise en charge des objets de base MIB dot11MultiDomainCapabilityImplemented, dot11MultiDomainCapabilityEnabled et dot11CountryString est FACULTATIVE et si elle est implémentée, la prise en charge de l'objet dot11MultiDomainCapabilityImplemented DOIT être 'false'.

6.3.3.1.4.9.1.2 Exigences pour dot11WEPDefaultKeysTable

Le dispositif PS DOIT implémenter la clause de SYNTAXE de l'objet de base MIB dot11WEPDefaultKeyValue avec la valeur "OCTET STRING (0|5|13)", ce qui signifie que les clés de 40 bits et de 104 bits sont prises en charge.

Le dispositif PS ne PEUT prendre en charge qu'une seule entrée pour ce tableau, auquel cas l'objet dot11WEPDefaultKeyID PEUT avoir un accès en lecture seulement ou bien DOIT être restreint à la valeur 0, afin d'éviter des défauts de configuration non détectés.

6.3.3.1.4.9.1.3 Exigences pour dot11OperationEntry

Les objets de base MIB dot11RTSThreshold et dot11FragmentationThreshold PEUVENT avoir un accès en lecture seulement.

6.3.3.1.4.9.1.4 Exigences pour dot11PhyTxPowerEntry

Le dispositif PS DEVRAIT implémenter les valeurs en milliwatts des objets de base MIB contenus dans l'entrée dot11PhyTxPowerEntry qui sont équivalentes à une valeur figurant dans l'étendue des pourcentages de puissance maximale de sortie du dispositif pour le mode opérationnel configuré dans l'objet cabhPsDev802dot11PhyOperMode, comme décrit dans le Tableau 6-19. Cette configuration simplifie le réglage de la valeur de puissance d'émission dans l'objet de base MIB dot11CurrentTxPowerLevel.

Si le dispositif PS est conforme aux valeurs de configuration indiquées dans le Tableau 6-19, il DOIT prendre en charge les huit instances de (1..8) de l'objet de base MIB dot11NumberSupportedPowerLevels qui permettent à l'implémentation de prendre en charge 8 ou 4 niveaux de puissance. Par exemple, la dernière colonne de droite du Tableau 6-19 indique les valeurs des objets de base MIB contenus dans l'entrée dot11PhyTxPowerEntry pour la bande inférieure de l'infrastructure UNII (unlicensed national information infrastructure) définie dans le Tableau 89 de la référence [802.11A-1999]. En particulier, les niveaux impairs (1, 3, 5, 7) représentent des références déterministes à 100%, 75%, 50% et 25 % de la puissance maximale du dispositif; alors que les niveaux pairs (2, 4, 6, 8) ont des valeurs de puissance comprises dans les étendues des nombres impairs supérieurs et inférieurs correspondants (1-3, 3-5, 5-7, 7-).

Tableau 6-19/J.192 – Niveaux de puissance recommandés

Niveau de puissance	Pourcentage du niveau relatif de la puissance maximale du PS en mW	Limite supérieure en % de la puissance en mW	Limite inférieure en % de la puissance en mW	Bande 5,15-5,25 GHz 40 (mW)
Dot11TxPowerLevel1	100%	100%	100%	40
Dot11TxPowerLevel2	100%-75%	100%	75%	40-30
Dot11TxPowerLevel3	75%	75%	75%	30
Dot11TxPowerLevel4	75%-50%	75%	50%	30-20
Dot11TxPowerLevel5	50%	50%	50%	20
Dot11TxPowerLevel6	50%-25%	50%	25%	20-10
Dot11TxPowerLevel7	25%	25%	25%	10
Dot11TxPowerLevel8	25%-12%	25%	12%	10-5

6.3.3.1.4.9.1.5 Objet dot11PhyDSSSEntry

Le dispositif PS DOIT prendre en charge l'objet de base MIB dot11CurrentChannel pour les implémentations conformes aux modes PHY des normes 802.11B/Cor1-2001 ou 802.11G-2003.

6.3.3.1.4.9.1.6 Exigences pour dot11PhyOFDMEntry

Le dispositif PS DOIT implémenter l'objet dot11PhyOFDMEntry s'il fonctionne dans un mode PHY conforme à la norme 802.11A.

6.3.3.1.4.9.2 Exigences pour les extensions de configuration IPCable2Home d'une base MIB 802.11

Si le dispositif PS implémente la fonctionnalité de réseau local sans fil IEEE 802.11, il DOIT implémenter les objets de base MIB indiqués par l'identificateur OBJECT IDENTIFIER cabhPsDevPs802dot11.

6.3.3.1.4.9.2.1 Exigences pour l'objet cabhPsDev802dot11BaseEntry

L'objet de base MIB cabhPsDev802dot11BaseAdvertiseSSID PEUT être implémenté en lecture seulement.

6.3.3.1.4.10 Exigences relatives à la table ipNetToMediaTable

La table ipNetToMediaTable [RFC 2011] mappe des adresses IP sur des adresses physiques et son emploi est clair si chaque adresse IP est associée à une seule interface physique et si chaque interface physique est associée à une seule adresse physique. Le dispositif PS, cependant, implémente différentes adresses IP qui peuvent s'appliquer à plusieurs interfaces physiques. Il associe également l'interface physique avec un réseau régional à deux adresses de matériel. Le dispositif PS implémente également différents modes primaires de traitement de paquet, ce qui a aussi un effet sur la table ipNetToMediaTable. Le dispositif PS DOIT énumérer, dans la table ipNetToMediaTable chacune des adresses IP qui font partie de sa configuration active, en créant une seule entrée par valeur IP distincte et en appliquant le Tableau 6-20 ci-après pour les modes primaires de traitement de paquet par conversion NAPT et NAT (y compris le mode mixte) et en appliquant le Tableau 6-21 pour le mode primaire de traitement de paquet par transfert en dérivation.

Tableau 6-20/J.192 – Entrées statiques dans la table ipNetToMediaTable pour les modes NAPT, NAT et mixte du dispositif PS

ipNetToMediaAddress	ipNetToMediaPhys Address	ipNetTo MediaIfIndex	ipNetTo MediaType
Adresse IP de réseau WAN-Man	Adresse matérielle de réseau WAN-Man	1	static(4)
1re adresse IP de réseau WAN-Data	Adresse matérielle de réseau WAN-Data	2	static(4)
2e adresse IP de réseau WAN-Data	Adresse matérielle de réseau WAN-Data	2	static(4)
ne adresse IP de réseau WAN-Data	Adresse matérielle de réseau WAN-Data	2	static(4)
Adresse IP de routeur-serveur de portail CDP	Chaîne d'octets de longueur nulle	255	static(4)
Adresse IP notoire du réseau local PS (si différente de l'adresse IP du routeur-serveur)	Chaîne d'octets de longueur nulle	255	static(4)

Tableau 6-21/J.192 – PS static entries in the ipNetToMediaTable for passthrough mode

ipNetToMediaAddress	ipNetToMediaPhys Address	ipNetToMediaIf Index	ipNetToMediaType
Adresse IP du réseau WAN-Man	Adresse matérielle WAN-Man	1	static(4)
Adresse IP notoire du routeur-serveur de réseau local PS	Chaîne d'octets de longueur nulle	255	static(4)

Cet élément du dispositif PS DOIT acquérir dynamiquement les adresses IP et matérielles des dispositifs de couche 3 OSI à partir de chacune de ses interfaces physiques et actives avec le réseau local et à partir de chacune de ses interfaces actives avec le réseau régional. Les adresses IP et matérielles acquises par l'élément du dispositif PS, en association avec les numéros d'indice ifIndex et les informations ipNetToMediaType du dispositif PS, DOIVENT être accessibles au système NMS (par l'intermédiaire du portail CMP) via la table [RFC 2011] ipNetToMediaTable. Toutes les entrées dynamiquement acquises dans la table ipNetToMediaTable DOIVENT avoir une valeur ipNetToMediaType égale à dynamic(3).

Une entrée de rangée pour le câblo-modem du dispositif PS NE DOIT PAS apparaître dans la table ipNetToMediaTable du dispositif PS car le câblo-modem joue le rôle de pont transparent du point de vue du service de portail.

A la suite du processus de préconfiguration du dispositif PS, celui-ci DOIT créer une entrée de rangée dans sa table ipNetToMediaTable afin de représenter le prochain routeur d'interconnexion pour l'interface avec le réseau WAN-Man, avec valeur d'indice d'interface de 1, des valeurs d'adresse ipNetToMediaPhysAddress et ipNetToMediaNetAddress propres à ce routeur, et une valeur de type ipNetToMediaType égale à dynamic(3). Si le dispositif PS possède une interface active avec le réseau WAN-Data, le dispositif PS DOIT créer une entrée de rangée dans sa table ipNetToMediaTable afin de représenter le prochain routeur d'interconnexion pour cette interface WAN-Data, avec une valeur d'indice d'interface de 2, des valeurs d'adresse ipNetToMediaPhysAddress et ipNetToMediaNetAddress propres à ce routeur, et une valeur de type ipNetToMediaType égale à dynamic(3).

L'élément du dispositif PS DOIT supprimer de sa table ipNetToMediaTable les entrées qui ont une valeur de type ipNetToMediaType égale à dynamic(3) quand une temporisation de la période d'inactivité propre à l'implémentation arrive à expiration.

6.3.3.1.5 Commande d'interface avec l'utilisateur du dispositif PS

Le portail CMP prend en charge la configuration d'une interface avec l'utilisateur (UI, *user interface*), si une telle interface est implémentée, par l'intermédiaire d'un ensemble d'objets définis dans la base MIB d'objets PSDev [voir § E.4]. Ces objets permettent au câblo-opérateur de sélectionner l'interface UI qui est présentée à l'utilisateur quand celui-ci pointe son navigateur IP sur l'adresse IP du routeur-serveur du dispositif PS. La base MIB prend en charge cette sélection entre une interface UI de constructeur local, une interface UI de câblo-opérateur local, une interface UI fournie par le serveur distant du réseau. La base MIB permet également de désactiver l'interface UI. Elle permet également au câblo-opérateur de configurer un identifiant et un mot de passe d'interface UI pour l'abonné. Voir dans l'Annexe E les diverses bases MIB d'interface IPCable2Home avec l'utilisateur.

6.3.3.2 Fonction de signalisation d'événement de portail CMP

Le portail CMP est tenu de prendre en charge le traitement et la signalisation des événements produits par le dispositif PS, pour le domaine de réseau régional. Les messages événementiels définis par IPCable2Home pour l'élément de services de portail peuvent être signalés par transfert

SNMP au récepteur de notification du câblo-opérateur, au moyen d'un message de journalisation du système envoyé au serveur de journalisation du système du câblo-opérateur, ou par un journal localisé dans le dispositif PS et accessible par des objets de base MIB spécifiés. Les événements définis pour le dispositif PS sont énumérés dans l'Annexe B: format et contenu des messages événementiels SYSLOG et Trap du protocole SNMP. Il s'agit des processus déjà définis dans les spécifications DOCSIS pour la signalisation des événements dans les câblo-modems.

Les dispositifs de serveur local IPCable2Home ne sont pas tenus de prendre en charge la messagerie de signalisation des événements, qui n'est donc pas définie par la présente Recommandation pour le domaine de réseau local.

Signalisation des événements pour le domaine de réseau régional

Le modèle IPCable2Home fait appel aux mécanismes [RFC 2669] de signalisation et de commande des événements produits dans le dispositif PS (portail CMP). Le document [RFC 2669] définit un format normalisé pour la signalisation des informations relatives aux événements, sans tenir compte du type de message, y compris une table locale de journalisation des événements dans laquelle certaines entrées persisteront après un réamorçage du dispositif PS. Noter que des événements peuvent être produits par une partie quelconque d'un dispositif PS, mais que le portail CMP journalise et/ou signale l'événement localement ou en l'envoyant à un serveur de messages Syslog ou Trap.

6.3.3.2.1 Fonction de signalisation des événements: objectifs

Les objectifs de la fonction de signalisation des événements de portail CMP sont énumérés ci-dessous:

- permettre le transfert des messages non sollicités du dispositif PS au système NMS dans le réseau régional sous la forme de messages Trap et SYSLOG en protocole SNMP;
- permettre la journalisation des informations relatives aux états et aux exceptions contenues dans la base de données PS (journal local);
- permettre l'accès aux informations relatives aux états et aux exceptions contenues dans le journal local, par les objets de base MIB;
- conserver la compatibilité avec la signalisation des événements définie dans les spécifications DOCSIS.

6.3.3.2.2 Fonction de signalisation des événements: directives de conception du système

Les directives de conception du système énumérées dans le Tableau 6-22 ont guidé la spécification de la fonction de signalisation d'événement de portail CMP.

Tableau 6-22/J.192 – Fonction de signalisation d'événement de portail CMP: directives de conception du système

Référence	Fonction de signalisation d'événement de portail CMP – Directives de conception du système
EvRep 1	Le dispositif PS prendra en charge la signalisation des informations relatives aux états et aux exceptions, telles que les notifications SNMP, les messages SYSLOG et les messages de journalisation locale, volatils et non volatils.
EvRep 2	Le dispositif PS prendra en charge les ralentisseurs et limiteurs d'événements configurables.
EvRep 3	Le dispositif PS prendra en charge les priorités événementielles configurables.

6.3.3.2.3 Fonction de signalisation des événements: description du système

La signalisation des événements permet à un élément de signaler un état ou une condition d'erreur dans un message non sollicité. Le modèle IPCable2Home prend en charge quatre types de signalisation des événements:

1) notification ou préinterruption SNMP;
2) messagerie SYSLOG;
3) journal local non volatil;
4) journal local volatil.

Il est nécessaire d'utiliser la base MIB de dispositif DOCSIS [RFC 2669] afin de configurer le dispositif PS en indiquant la destination des préinterruptions (notifications) et des messages SYSLOG en protocole SNMP, ainsi que les valeurs de limitation et de ralentissement des événements. La notification d'événement par le dispositif PS est entièrement configurable. La présente Recommandation définit la destination des messages par lesquels le dispositif PS doit signaler les événements qui ont reçu une priorité particulière (voir le Tableau 6-23). La base MIB de dispositif DOCSIS permet de configurer la priorité de chaque événement. La base MIB de dispositif DOCSIS tient également à jour des statistiques concernant la fréquence de chaque événement. La table d'événements (docsDevEventTable) contenue dans la base MIB de dispositif DOCSIS comprend une entrée pour chaque événement unique qui a été signalé par le dispositif PS, le décompte du nombre d'occurrences de chaque entrée d'événement unique, et l'instant auquel la dernière entrée a été effectuée, pour chaque entrée d'événement.

Le modèle IPCable2Home définit la procédure de réindexation de la table d'événements si le dispositif PS est réinitialisé de telle sorte que les entrées du journal local volatil soient perdues. Quand les entrées du journal local volatil sont perdues, le dispositif PS est tenu de réindexer la table d'événements de telle sorte que les entrées restantes du journal local (volatil) soient indexées en séquence.

6.3.3.2.4 Fonction de signalisation des événements: exigences

Les exigences des services de portail pour la fonction de signalisation d'événement de portail CMP sont spécifiées dans les § 6.3.3.2.4.1 à 6.3.3.2.4.9.

6.3.3.2.4.1 Notification d'événement

Le dispositif PS DOIT produire des événements asynchrones qui indiquent d'importants événements et d'importantes situations comme spécifié (voir l'Annexe B). Les événements peuvent être mémorisés dans un journal interne d'événements, être conservés en mémoire non volatile, être signalés à d'autres entités SNMP (comme les messages Trap ou Inform du protocole SNMP), ou être envoyés sous forme de messages événementiels SYSLOG au serveur SYSLOG dont l'adresse IP est transmise dans l'option DHCP 7 du message DHCP OFFER reçu du serveur DHCP de la tête de réseau par l'interface PS WAN-Man.

Le dispositif PS DOIT prendre en charge les mécanismes suivants de notification d'événement:

- journalisation locale des événements où certaines entrées dans le journal local peuvent être identifiées comme persistant après un réamorçage du dispositif PS;
- messages Trap et Inform du protocole SNMP;
- journal SYSLOG.

Le dispositif PS DOIT mettre en œuvre la table docsDevEvControlTable à partir du document [RFC 2669] afin de contrôler la signalisation des événements. Les valeurs activées par fanion (bit) suivantes DOIVENT être prises en charge par le dispositif PS pour l'objet docsDevEvReporting [RFC 2669]:

- local-nonvolatile(0);

- traps(1);
- syslog(2);
- local-volatile(3).

Les messages de requête SET (mise à jour) du protocole SNMP envoyés à l'objet [RFC 2669] docsDevEvReporting au moyen des valeurs suivantes DOIVENT se traduire par une erreur de type 'Valeur erronée' pour les unités PDU du protocole SNMP:

- 0x20 = SYSLOG seulement;
- 0x40 = préinterruption seulement;
- 0x60 = (préinterruption + SYSLOG) seulement.

Un événement signalé par un message Trap, SYSLOG, ou Inform DOIT également produire une entrée de journalisation locale, volatile ou non volatile selon le Tableau 6-23 et comme décrit dans le § 6.3.3.2.4.2.

6.3.3.2.4.2 Journalisation locale des événements

Le dispositif PS DOIT conserver une seule table d'événements de journalisation locale contenant les événements mémorisés, aussi bien locaux-volatils que locaux-non volatils. Les événements mémorisés comme étant locaux-non volatils DOIVENT persister après un réamorçage du dispositif PS. La table d'événements de journalisation locale DOIT être organisée comme une mémoire tampon cyclique avec un minimum de dix entrées. La table unique d'événements de journalisation locale DOIT être accessible par l'intermédiaire de la table docsDevEventTable comme défini dans le document [RFC 2669].

Les descriptions d'événement NE DOIVENT PAS avoir une longueur supérieure à 255 octets, ce qui est le maximum défini pour la chaîne SnmpAdminString.

L'identificateur d'événement (EventId) est un entier non signé de 32 bits. Les identificateurs EventId allant de 0 à ((2^31) – 1) sont réservés. L'identificateur EventId DOIT être converti à partir des codes d'erreur définis dans l'Annexe B. Les identificateurs EventId allant de 2^31 à ((2^32) – 1) DOIVENT être utilisés comme des identificateurs EventId propres au vendeur, au moyen du format suivant:

- le bit 31 est activé afin d'indiquer un événement propre au vendeur;
- les bits 30 à 16 contiennent les 15 éléments binaires inférieurs du numéro d'entreprise SNMP du vendeur;
- les bits 15 à 0 sont utilisés par le vendeur afin de numéroter ses événements.

L'objet [RFC 2669] docsDevEvIndex sert à ordonner plus ou moins les événements dans le journal. Le marquage des événements du journal local comme étant locaux-volatils ou locaux-non volatils nécessite une méthode afin de synchroniser les valeurs de l'objet docsDevEvIndex entre ces deux types d'événement après un réamorçage du dispositif PS. Après un réamorçage du dispositif PS, afin de synchroniser les valeurs de l'objet docsDevEvIndex pour les événements volatils et non volatils, la procédure suivante DOIT être utilisée:

- les valeurs de l'objet docsDevEvIndex pour les événements de journal local marqués comme étant locaux-non volatils DOIVENT être renumérotées en commençant par 1;
- le journal local DOIT ensuite être initialisé avec les événements marqués comme étant locaux-non volatils, dans l'ordre qu'ils avaient immédiatement avant le réamorçage;
- les événements subséquemment mémorisés dans le journal local, si marqués comme étant locaux-volatils ou locaux-non volatils, DOIVENT utiliser des valeurs croissantes de l'objet docsDevEvIndex.

Une réinitialisation du journal lancée par une requête SNMP de mise à jour (SET) de l'objet [RFC 2669] docsDevEvControl DOIT supprimer tous les événements du journal local, y compris les événements du journal marqués comme étant à la fois locaux-volatils et locaux-non volatils.

6.3.3.2.4.3 Messages Trap et Inform du protocole SNMP

Le dispositif PS DOIT prendre en charge l'unité PDU "Trap" du protocole SNMP comme décrit dans le document RFC 3411. Le dispositif PS DOIT prendre en charge l'unité PDU "INFORM" du protocole SNMP comme décrit dans le document RFC 3411. Le message INFORM est une variante de préinterruption exigeant du serveur de réception qu'il accuse réception de l'arrivée d'une unité PDU de requête "InformRequest" par une unité PDU "InformResponse".

Quand une préinterruption normalisée du protocole SNMP est activée dans le dispositif PS, celui-ci DOIT envoyer des notifications pour chaque événement de cette catégorie dont la priorité est soit une "erreur" ou une "remarque".

Le dispositif PS PEUT prendre en charge des événements propres au vendeur. S'ils sont pris en charge, les événements PS propres au vendeur communicables par préinterruption Trap du SNMP DOIVENT être décrits dans une base MIB privée qui est distribuée avec le dispositif PS. Lors de la définition d'une préinterruption SNMP propre au vendeur, la déclaration "OBJECTS" de la définition de la préinterruption privée DEVRAIT contenir au moins les objets décrits ci-dessous:

- EvLevel;
- EvIdText;
- EventThreshold (s'il y a un seuil pour le préinterruption);
- IfPhysAddress (l'adresse physique associée à l'adresse IP de réseau WAN-Man du dispositif PS).

D'autres objets peuvent être contenus dans la déclaration "OBJECTS", au besoin.

6.3.3.2.4.4 Messages SYSLOG

Les messages SYSLOG envoyés par le dispositif PS DOIVENT être dans le format suivant:

<level>PortalServicesElement[vendor]: <eventId> text

Où:

niveau – présentation en caractères ASCII de la priorité de l'événement, entre chevrons, qui est construite comme l'opérateur OU au niveau des bits de la ressource par défaut (128) et de la priorité de l'événement (0 à 7). Le niveau résultant est compris entre 128 et 135.

vendeur – Nom du vendeur pour les messages SYSLOG propres au vendeur ou "CABLEHOME" pour les messages normalisés IPCable2Home.

eventId – présentation en caractères ASCII du nombre entier INTEGER en format décimal, entre chevrons, qui identifie de façon univoque le type d'événement. Cet identificateur EventID DOIT être le nombre qui a été mémorisé dans l'objet docsDevEvId de la table docsDevEventTable. Pour les événements normalisés IPCable2Home, ce nombre est converti à partir du code d'erreur selon les règles ci-après:

- c'est un nombre décimal à 8 chiffres;
- les deux premiers chiffres (à gauche) constituent le code ASCII (décimal) de la lettre figurant dans le code d'erreur;
- les quatre chiffres suivants constituent les 2 ou 3 chiffres situés entre la lettre et le point du code d'erreur, l'espace vide à gauche étant rempli avec des zéros;
- les deux derniers chiffres constituent le nombre situé après le point dans le code d'erreur, l'espace vide à gauche étant rempli avec des zéros.

Par exemple, l'événement D04.2 est converti en 68000402 et l'événement I114.1 est converti en 73011401.

Noter que cette notion ne fait appel qu'à une petite partie de l'espace numérique disponible qui est réservé pour IPCable2Home (de 0 à 2^31 – 1). La première lettre d'un code d'erreur est toujours en majuscule.

texte – pour les messages normalisés, cette chaîne DOIT avoir la description textuelle définie dans l'Annexe B.

Exemple d'événement syslog pour l'événement D04.2: "Heure locale reçue en format non valide":

<132>Portal ServicesElement[CABLEHOME]: <68000402> heure locale reçue en format non valide.

Dans l'exemple ci-dessus, le nombre 68000402 est celui qui a été attribué à cet événement particulier.

6.3.3.2.4.5 Format des événements

Les messages événementiels de gestion IPCable2Home PEUVENT contenir l'une quelconque des informations suivantes:

- compteur d'événements – indicateur de séquence d'événements;
- heure d'événement – heure d'apparition de l'événement;
- priorité d'événement – sévérité de la condition. Le document [RFC 2669] définit huit niveaux de sévérité. La sévérité d'événement par défaut peut être remplacée par une valeur différente pour chaque événement donné via l'interface avec le protocole SNMP;
- numéro d'entreprise de l'événement – Ce numéro identifie l'événement comme étant soit normalisé soit défini par le vendeur;
- identificateur d'événement – identifie l'événement exact lorsqu'il est combiné avec le numéro d'entreprise de l'événement. Les vendeurs définissent leurs propres identificateurs d'événement. Les événements de gestion normalisés selon IPCable2Home sont définis dans l'Annexe B. Chaque événement de gestion décrit dans l'Annexe reçoit un ID d'événement;
- texte de l'événement – décrit l'événement sous une forme lisible par l'homme;
- adresse de commande MAC d'interface PS WAN-Man – décrit l'adresse de couche MAC de l'élément de services de portail servant à la gestion du bloc;
- adresse de commande MAC d'interface PS WAN-Data – décrit l'adresse de couche MAC de l'élément de services de portail servant facultativement à la gestion des données.

Le format exact de ces informations pour les messages Trap et Inform est défini dans l'Annexe B. Le format des messages SYSLOG est défini dans la partie du présent paragraphe qui concerne les exigences.

6.3.3.2.4.6 Priorités d'événement

Le document RFC 2669 définit 8 différents niveaux de priorité et les mécanismes de signalisation correspondant à chaque niveau. Les événements normalisés qui sont spécifiés dans la présente Recommandation utilisent ces niveaux de priorité.

– **Evénement d'urgence (priorité 1)**

  Réservé aux erreurs "fatales" de matériel ou de logiciel propres au vendeur qui empêchent le fonctionnement normal du système et causent le réamorçage du système de signalisation. Chaque vendeur peut définir son propre ensemble d'événements d'urgence. Des exemples de tels événements pourraient être: 'aucune mémoire tampon disponible', 'échec des essais de mémoire' etc.

– **Evénement d'alerte (priorité 2)**

  Echec sérieux qui provoque le réamorçage du système de signalisation sans que ce réamorçage soit causé par un dysfonctionnement du matériel ou du logiciel. Après reprise sur l'événement, le système DOIT envoyer la notification de démarrage à froid/à chaud.

– **Evénement critique (priorité 3)**

  Echec sérieux qui empêche le dispositif de transmettre des données mais dont il peut se remettre sans réamorçage du système. Après reprise sur événement critique, le dispositif PS DOIT envoyer la notification de liaison activée. Des exemples de tels événements pourraient être des problèmes de fichier de configuration du dispositif PS ou l'incapacité d'obtenir une adresse IP par protocole DHCP.

– **Evénement d'erreur (priorité 4)**

  Echec qui pourrait interrompre le flux normal de données mais qui ne cause pas de réamorçage du dispositif. Les événements d'erreur peuvent être signalés en temps réel au moyen du mécanisme Trap ou SYSLOG.

– **Evénement d'avertissement (priorité 5)**

  Echec qui pourrait interrompre le flux normal de données. La signalisation par messages SYSLOG et Trap est activée par défaut pour ce niveau.

– **Evénement de remarque (priorité 6)**

  Evénement d'importance qui n'est pas un échec et qui pourrait être signalé en temps réel au moyen du mécanisme de messages Trap ou SYSLOG. Des exemples d'événement de type NOTICE sont: 'Démarrage à froid', 'Démarrage à chaud', 'Liaison activée' et 'Mise à jour logicielle réussie'.

– **Evénement d'information (priorité 7)**

  Evénement d'importance qui n'est pas un échec, mais qui pourrait être utile afin de garder la trace du fonctionnement normal du dispositif.

– **Evénement de débogage (priorité 8)**

  Priorité réservée aux événements non critiques, propres au vendeur.

La priorité associée aux événements normalisés NE DOIT PAS être changée.

Le Tableau 6-23 montre les types de notification par défaut pour les diverses priorités événementielles. Le dispositif PS DOIT implémenter les types de notification par défaut définis dans le Tableau 6-23: types de notification par défaut pour priorités événementielles des services de portail, pour les huit priorités événementielles. Par exemple, le type de notification par défaut pour les événements d'urgence et d'alerte consiste à les placer dans le journal local comme entrées non volatiles.

Tableau 6-23/J.192 – Types de notification par défaut pour priorités événementielles des services de portail

Priorité d'événement	Local non volatil (bit 0)	Message TRAP du SNMP (bit 1)	Message SYSLOG (bit 2)	Local-volatil (bit 3)	Note
1 Urgence	Oui	Non	Non	Non	Propre au vendeur
2 Alerte	Oui	Non	Non	Non	Selon la présente Recommandation
3 Critique	Oui	Non	Non	Non	Selon la présente Recommandation

Tableau 6-23/J.192 – Types de notification par défaut pour priorités événementielles des services de portail

Priorité d'événement	Local non volatil (bit 0)	Message TRAP du SNMP (bit 1)	Message SYSLOG (bit 2)	Local-volatil (bit 3)	Note
4 Erreur	Oui	Oui	Oui	Non	Selon la présente Recommandation
5 Avertissement	Oui	Oui	Oui	Non	Selon la présente Recommandation
6 Remarque	Non	Oui	Oui	Oui	Selon la présente Recommandation
7 Information	Non	Non	Non	Non	Selon la présente Recommandation et propre au vendeur
8 Débogage	Non	Non	Non	Non	Propre au vendeur

Le dispositif PS DOIT prendre en charge la capacité d'être configuré de façon à produire tous les types de notification pour chacun des niveaux de priorité d'événement énumérés dans le Tableau 6-23.

6.3.3.2.4.7 Evénements normalisés

Le dispositif PS DOIT envoyer les préinterruptions génériques suivantes en protocole SNMP, comme défini dans les documents [RFC 3418] et [RFC 2863]:

- coldStart [RFC 3418] (démarrage à froid);
- linkUp [RFC 2863] (liaison activée);
- linkDown [RFC 2863] (liaison désactivée);
- SNMP authentification-Failure [RFC 3418] (échec d'authentification SNMP).

Le dispositif PS DOIT être capable de produire des notifications d'événement fondées sur les événements normalisés qui sont énumérés dans l'Annexe B.

6.3.3.2.4.8 Ralentissement et limitation des événements

Le dispositif PS DOIT prendre en charge le ralentissement et la limitation des événements Trap/Inform et SYSLOG du protocole SNMP comme décrit dans le document [RFC 2669].

Le dispositif PS DOIT considérer que les événements sont identiques si leurs identificateurs EventId sont identiques.

Le document [RFC 2669] spécifie quatre états de ralentissement:

- l'état "unconstrained(1)" (sans contraintes) provoque la transmission des messages Trap et SYSLOG sans considération du réglage de seuil;
- l'état "maintainBelowThreshold(2)" (maintien au-dessous du seuil) provoque la suppression de la transmission des messages Trap et SYSLOG de façon que le nombre de préinterruptions ne dépasse pas le seuil;
- l'état "stopAtThreshold(3)" (maintien au niveau du seuil) provoque la cessation de la transmission des préinterruptions au-delà du seuil et sa non-reprise jusqu'à ordre contraire;
- l'état "inhibited(4)" (inhibition) provoque la suppression de toute transmission de messages Trap et SYSLOG.

Un événement isolé DOIT être traité comme un événement unique en terme de comptage d'événements de seuil, c'est-à-dire qu'un événement provoquant à la fois un message Trap et un message SYSLOG continue à être traité comme un événement unique.

6.3.3.2.4.9 Signalisation des événements de téléchargement sécurisé de logiciel

Le Tableau B.1 de l'Annexe B, Format et contenu des messages événementiels SYSLOG et Trap du protocole SNMP, décrit les événements associés aux mises à jour logicielles des services de portail, selon les trois catégories suivantes: initialisation de mise à jour logicielle (SW UPGRADE INIT), échec général de mise à jour logicielle et succès de mise à jour logicielle. Ces événements ne s'appliquent qu'au dispositif PS autonome, car la mise à jour logicielle (également appelée *téléchargement sécurisé de logiciel*) d'un dispositif PS avec câblo-modem intégré est régie et gérée par le câblo-modem DOCSIS. Le paragraphe 11.8, Téléchargement de logiciel vers des éléments PS intégrés ou autonomes, définit des exigences de téléchargement sécurisé de logiciel pour les deux classes d'élément de services de portail. Le dispositif PS intégré, tel que défini dans le § 5.1.2.1, Dispositif PS intégré et dispositif PS autonome, NE DOIT PAS produire d'événements de la catégorie "Initialisation de mise à jour logicielle" (SW UPGRADE INIT), d'événements de la catégorie "Échec général de mise à jour logicielle" (SW UPGRADE GENERAL FAILURE), ni d'événements de la catégorie "Succès de mise à jour logicielle" (SW UPGRADE SUCCESS) selon le Tableau B.1, Evénements définis pour IPCable2Home.

{texte informatif:

6.3.3.3 Fonction de découverte du portail CMP

6.3.3.3.1 Objectifs de la fonction de découverte

Les objectifs de la fonction de découverte du portail CMP sont énumérés ci-dessous:

- offrir aux câblo-opérateurs une visibilité sur les attributs des dispositifs de serveur local UPnP et sur les attributs des dispositifs de passerelle résidentielle IPCable2Home;
- offrir aux câblo-opérateurs une visibilité sur les services UPnP qui sont implémentés dans des dispositifs de serveur local UPnP.

Hypothèses

Les hypothèses relatives à la capacité de découverte du portail CMP sont les suivantes:

- les dispositifs de serveur local IPCable2Home, les dispositifs de serveur local UPnP et les dispositifs de passerelle résidentielle IPCable2Home implémentent la suite protocolaire IP (IPv4);
- les dispositifs de serveur local UPnP implémentent un dispositif UPnP pour la découverte, pour la description et pour la commande, comme spécifié dans l'architecture de dispositif UPnP (UDA);
- les dispositifs de serveur local UPnP implémentent facultativement des services de QoS UPnP.

6.3.3.3.1.1 Fonction de découverte: directives de conception du système

Les directives de conception du système énumérées dans le Tableau 6-24 offrent des indications pour la mise au point de la spécification relative à la fonction de découverte du portail CMP.

Tableau 6-24/J.192 – Directives de conception du système de découverte du dispositif PS

Référence	Directives de conception du système de découverte
Découverte 1	Le dispositif PS implémentera une fonctionnalité de découverte de dispositif UPnP compatible avec l'architecture de dispositif UPnP 1.0.
Découverte 2	Le dispositif PS offrira au câblo-opérateur, sur demande, des informations sur les dispositifs UPnP présents dans le réseau local domestique.
Découverte 3	Le dispositif PS implémentera une fonctionnalité de point de commande UPnP compatible avec l'architecture de dispositif UPnP 1.0 pour la découverte, la description et la commande de dispositifs et services UPnP.
Découverte 4	Le dispositif PS implémentera une hiérarchie spécifiée des dispositifs et services UPnP.
Découverte 5	La messagerie du protocole de découverte UPnP ne se propagera pas dans le réseau régional.

6.3.3.3.2 Fonction de decouverte: description du système

L'objet de la fonction de découverte du portail CMP est d'offrir au câblo-opérateur des informations sur les dispositifs de serveur local UPnP et sur les services UPnP qui sont disponibles dans un réseau local d'abonné.

La fonction de découverte du dispositif PS offre un répertoire central des informations relatives aux dispositifs et services UPnP disponibles dans le réseau local d'abonné. Le dispositif PS implémente un point de commande (PS CP) UPnP qui lui permet de découvrir dans le réseau domestique toutes les instances de dispositif et de service UPnP. Par ailleurs, la fonction de découverte peut demander des détails complémentaires sur des dispositifs et services UPnP spécifiques, sous la forme de documents descriptifs de dispositif et de service UPnP.

6.3.3.3.3 Exigences relatives à la fonction de découverte

1) Lorsque la base MIB cabhPsDevUpnpCommand est mise à discoveryInfo et que l'objet cabhPsDevUpnpCommandUpdate est mis à la valeur "TRUE", le dispositif PS DOIT invoquer la découverte UPnP au moyen d'une recherche M-Search avec comme cible de recherche (ST, *search target*) upnp:rootdevice et une valeur maximale (MX, maximum) d'attente inférieure ou égale à 3 s, comme spécifié dans l'architecture de dispositif UPnP (UDA1.0).

2) Le dispositif PS DOIT remplir la base de données du dispositif PS avec les informations de description de dispositif qui sont accessibles via la table de base MIB cabhPsDevUpnpInfoTable MIB. Tout en mettant à jour sa base de données avec les informations de découverte de dispositif reçues en réponse à la recherche M-Search, le dispositif PS DOIT filtrer ces informations sur la base de la base MIB cabhPsDevUpnpCommandIp.

   - Si la base cabhPsDevUpnpCommandIp est mise à 255.255.255.255, le dispositif PS DOIT remplir sa base de données avec les informations de découverte de dispositif en provenance de tous les dispositifs UPnP radicaux se trouvant dans le réseau domestique; il DOIT également inclure ses propres informations de découverte de dispositif UPnP.
   - Si la base cabhPsDevUpnpCommandIp est mise à 192.168.0.1, le dispositif PS DOIT remplir sa base de données avec ses propres informations de découverte de dispositif UPnP.

3) Tous les identificateurs URI exposés par le dispositif PS pour les communications UPnP DOIVENT utiliser des adresses IP et NE DOIVENT PAS utiliser de noms de serveur local.

4) Si le dispositif PS vise à changer un fichier de description de dispositif ou de service, alors il DOIT d'abord quitter le réseau UPnP en envoyant un message ssdp:byebye puis rejoindre le réseau UPnP avec les nouveaux fichiers XML au moyen d'un message ssdp:alive.

5) Le dispositif PS DOIT envoyer toutes ses annonces de découverte avec l'en-tête HTTP LOCATION 192.168.0.1

6) Le type (deviceType) du dispositif radical contenu dans le dispositif PS DOIT être urn:schemas-cablelabs-com:device:CableHomePSDevice:1.

7) Le dispositif PS DOIT annoncer le dispositif IGD 1.0 comme un appareil intégré dans le dispositif CableHomePS radical.

8) Le dispositif PS DOIT annoncer tous les services de qualité de service UPnP comme des services du dispositif CableHomePS radical.

9) Le dispositif PS DOIT annoncer la hiérarchie suivante dans le cadre de son document descriptif de dispositif UPnP:

- Dispositif PS CableHome
  - Dispositif IGD 1.0
    - Dispositif IGD 1.0 de réseau régional
      - Dispositif IGD 1.0 de connexion de réseau régional
        - Dispositif IGD 1.0 du service de connexion IP de réseau régional
  - Service de gestionnaire de qualité de service 1.0
  - Service de détenteur de la politique de qualité de service 1.0
  - Service de dispositif de qualité de service 1.0 (facultatif)

(Voir à l'Appendice I un exemple de cette hiérarchie.)

10) Afin de fournir une dénomination unique pour tous les dispositifs UPnP dans les descriptions de dispositif CableHome PS radical, il est suggéré d'utiliser le format ci-après lors de la construction des noms uniques de dispositif pour tous les dispositifs UPnP des services de portail CableHome.

- un nom unique de dispositif PS CableHome DEVRAIT être formaté comme suit: "CableHomeDevice-1_0-00aabbccddee", où la chaîne "00aabbccddee" correspond à l'adresse de commande MAC de l'interface PS WAN-Man du dispositif PS.
- un nom unique de dispositif de passerelle Internet (IGD) DEVRAIT être formaté comme suit: "InternetGatewayDevice-1_0-00aabbccddee", où la chaîne "00aabbccddee" correspond à l'adresse de commande MAC de l'interface PS WAN-Man du dispositif PS.
- un nom unique de dispositif de connexion par réseau régional DEVRAIT être formaté comme suit: "WANConnectionDevice-1_0-00aabbccddee", où la chaîne "00aabbccddee" correspond à l'adresse de commande MAC de l'interface PS WAN-Man du dispositif PS.

11) Lorsqu'un service UPnP implémenté par le dispositif PS est désactivé, le dispositif PS DOIT avoir avoir comportement suivant:

- le dispositif PS DOIT multidiffuser le message SSDP:byebye pour ce service;
- le dispositif PS NE DOIT PAS annoncer le service désactivé dans les futures annonces SSDP;
- le dispositif PS NE DOIT PAS renvoyer le service désactivé dans la description de dispositif radical;

- le dispositif PS NE DOIT PAS répondre à une recherche M-SEARCH pour le service désactivé;
- le dispositif PS NE DOIT PAS répondre à une action pour le service désactivé.

}

6.4 Elément logique des services de portail – Portail d'essais IPCable2Home (CTP)

6.4.1 Objectifs du portail CTP

Les objectifs du portail d'essais IPCable2Home sont les suivants:

- permettre les diagnostics de dérangement de dispositif IP de réseau local et de serveur local IPCable2Home;
- offrir une visibilité sur les dispositifs IP de réseau local et serveurs locaux IPCable2Home, ainsi que l'accès aux numéros et aux types de dispositif IP de réseau local et de serveur local IPCable2Home;
- permettre la surveillance de la performance du dispositif IP de réseau local et du serveur local IPCable2Home.

6.4.2 Directives de conception du portail CTP

Les directives de conception du système de portail d'essais sont énumérées dans le Tableau 6-25. Un certain nombre de ces directives reprennent les directives de conception du portail CMP. Cette liste offrait des indications pour la spécification de la fonctionnalité de portail CTP.

Tableau 6-25/J.192 – Directives de conception du système de portail CTP

Référence	Directives de conception du système de portail CTP
CTP 1	Il est nécessaire que les interfaces acceptent les caractéristiques de gestion et de diagnostic ainsi que les fonctions requises afin de prendre en charge des services par câble fournis dans le réseau domestique.
CTP 2	Il est nécessaire que des capacités de surveillance locales et distantes permettent de surveiller le fonctionnement du réseau domestique et aident le consommateur et le câblo-opérateur à identifier les zones de problème.
CTP 3	Le système NMS du réseau câblé exige une méthode pour rassembler les informations d'identification sur chaque dispositif IP connecté au réseau domestique.
CTP 4	Le système NMS du réseau câblé exige une méthode pour détecter si un dispositif connecté est en état de fonctionnement.

6.4.3 Description du système de portail CTP

Le portail CTP (portail d'essais IPCable2Home) contient les "utilitaires distants" avec lesquels le système NMS peut collecter d'autres informations de dispositif de réseau local. Les essais doivent être effectués à distance, car contourner une fonction de conversion d'adresse de réseau (NAT, *network address translation*) dans un routeur risque d'être très difficile. Par exemple, un sondage par écho de réseau régional à réseau local ne pourra pas passer à travers un dispositif PS, à moins que le portail CAP n'ait été préconfiguré de façon à laisser passer ce trafic. Le portail CTP est un mandataire local servant à interpréter et à exécuter la classe de dérangements/diagnostics à distance des messages SNMP qu'il reçoit de l'opérateur du système NMS. Ces essais de dispositif IP de réseau local et de serveur local IPCable2Home sont définis sur la base des problèmes susceptibles d'être rencontrés dans les réseaux de type domestique IPCable2Home 1.1: les diagnostics de connexité et de débit utile.

Ces fonctions sont appelées *utilitaire de vitesse de connexion de portail CTP* et *utilitaire de sondage par écho de portail CTP*. Ces utilitaires permettent au centre de prise en charge des

consommateurs du câblo-opérateur et au centre d'exploitation du réseau d'en savoir plus sur la connexion entre l'élément de services de portail et les dispositifs IP de réseau local ou les serveurs locaux IPCable2Home domestiques.

6.4.3.1 Fonction d'utilitaire de vitesse de connexion du portail CTP

6.4.3.1.1 Fonction d'utilitaire de vitesse de connexion: objectifs

L'objectif de la fonction de vitesse de connexion est de permettre au gestionnaire du système IPCable2Home d'acquérir à distance des objets métrologiques sur la performance du réseau local domestique entre le dispositif PS et un dispositif IP de réseau local ou un serveur local IPCable2Home spécifique.

6.4.3.1.2 Fonction d'utilitaire de vitesse de connexion: directives de conception du système

Les directives de conception énumérées dans le Tableau 6-25: *Directives de conception du système de portail CTP* ont servi à orienter la spécification de la fonction d'utilitaire de vitesse de connexion.

6.4.3.1.3 Fonction d'utilitaire de vitesse de connexion: description du système

La fonction d'utilitaire de vitesse de connexion sert à obtenir une mesure grossière de la performance en terme de débit utile dans la liaison entre le dispositif PS et un dispositif IP de réseau local ou un serveur local IPCable2Home. Il envoie une rafale de paquets entre le dispositif PS et le dispositif IP de réseau local ou serveur local IPCable2Home en essai, et le temps d'aller-retour est mesuré pour la rafale. En général, l'opérateur du système NMS introduit quelques paramètres et déclenche la fonction, dont les résultats sont mémorisés dans la base de données PS pour récupération ultérieure par la base MIB du portail CTP [voir § E.3].

La fonction de vitesse de connexion repose sur l'intégration d'une "fonction de bouclage" ou d'un "service d'écho" dans les dispositifs IP de réseau local et serveurs locaux IPCable2Home. L'Autorité chargée de l'assignation des numéros Internet (IANA, *Internet assigned numbers authority*) a attribué le port 7 du service d'écho aux deux protocoles: TCP et UDP [RFC 347]. La valeur par défaut de l'adresse IP d'origine (objet cabhCtpConnSrcIp) est la même que celle de la passerelle PS-LAN par défaut (objet cabhCdpServerRouter). La valeur de l'objet cabhCtpConnSrcIp peut être réglée à toute adresse IP valide d'interface PS WAN-Data ou PS LAN. L'adresse IP de l'interface PS WAN-Man n'est pas utilisée comme adresse IP d'origine pour un utilitaire de portail CTP car, quand une adresse IP de l'interface PS WAN-Man est présente mais qu'une adresse IP d'interface PS WAN-Data ne l'est pas, le dispositif PS doit fonctionner en mode primaire de traitement de paquet par transfert et le câblo-opérateur peut au besoin essayer directement des dispositifs IP de réseau local et des serveurs locaux IPCable2Home à partir de la console du système NMS. Cette méthode d'essai ne fonctionne que sur les dispositifs IP de réseau local et serveurs locaux IPCable2Home se trouvant dans les secteurs adresses LAN-Trans ou LAN-Pass qui implémentent la fonction de service d'écho comme décrit dans le document [RFC 347].

Le paragraphe ci-dessous sur les exigences contrôlables du portail CTP énumère les paramètres et les réponses pour l'utilitaire de vitesse de connexion. Le paragraphe 12.2.1.1 décrit en détail le fonctionnement de l'utilitaire de vitesse de connexion.

6.4.3.1.4 Fonction d'utilitaire de vitesse de connexion: exigences

Le dispositif PS DOIT implémenter l'utilitaire de vitesse de connexion et DOIT être conforme aux valeurs par défaut et aux étendues de valeurs définies pour les objets spécifiques de l'utilitaire de vitesse de connexion contenus dans la base MIB de portail CTP [voir § E.3].

Le dispositif PS DEVRAIT transmettre les octets de données d'essai aussi rapidement que possible lorsqu'il fait fonctionner l'utilitaire de vitesse de connexion.

Le dispositif PS DOIT utiliser le port numéro 7 comme port de destination lorsqu'il fait fonctionner l'utilitaire de vitesse de connexion.

Le dispositif PS NE DOIT PAS produire de paquets à la sortie d'une quelconque interface avec un réseau régional lorsqu'il utilise la fonction d'utilitaire de vitesse de connexion.

Quand le système NMS déclenche le lancement de l'utilitaire de vitesse de connexion par le portail CTP en réglant l'objet cabhConnControl à la valeur = start(1), le dispositif PS DOIT effectuer ce qui suit:

- réinitialiser le temporisateur;
- régler l'objet cabhCtpConnStatus à la valeur = running(2);
- transmettre un nombre de paquets égal à la valeur de l'objet cabhCtpConnNumPkts, chaque paquet ayant une longueur égale à la valeur de l'objet cabhCtpConnPktSize, à l'adresse IP égale à la valeur de l'objet cabhCtpConnDestIp et au numéro de port 7, au moyen du protocole spécifié par l'objet cabhCtpConnProto;
- armer le temporisateur avec le premier bit transmis;
- fermer le temporisateur quand le dernier bit est reçu en retour du dispositif IP de réseau local cible ou quand la valeur du temporisateur est égale à celle de l'objet cabhCtpConnTimeOut, selon celle qui se produit en premier;
- quand le temporisateur est fermé, régler l'objet cabhCtpConnStatus à la valeur = complete(3) et signaler l'événement approprié (voir l'Annexe B – Evénements de portail CTP);
- mémoriser la valeur du temporisateur (en milliseconds) dans l'objet cabhCtpConnRTT;
- si l'essai par utilitaire de vitesse de connexion expire avant que le dernier bit ait été reçu du dispositif IP de réseau local ou serveur local IPCable2Home cible, signaler l'événement approprié (voir l'Annexe B – Evénements de portail CTP);
- calculer le débit utile comme défini dans la prescription ci-dessous et mémoriser la valeur dans l'objet cabhCtpConnThroughput.

Si l'utilitaire de vitesse de connexion est fermé par le système NMS en réglant l'objet cabhCtpConnControl à la valeur = abort(2) ou pour toute autre raison avant que le dernier bit soit reçu du dispositif IP de réseau local ou du serveur local IPCable2Home cible ou avant que l'essai par utilitaire de vitesse de connexion arrive à expiration, le dispositif PS DOIT régler l'objet cabhCtpConnStatus à la valeur = aborted(4) et signaler l'événement approprié (voir l'Annexe B – Evénements de portail CTP).

Quand la fonction d'utilitaire de vitesse de connexion est en cours d'exécution, le dispositif PS DOIT déterminer la valeur moyenne du débit utile d'aller-retour entre le dispositif PS et le dispositif IP de réseau local ou un serveur local IPCable2Home dont l'adresse est transmise dans l'objet cabhCtpConnDestIp (le dispositif IP de réseau local cible) en kilobits par seconde, puis arrondir ce nombre au plus proche entier et mémoriser le résultat dans l'objet cabhCtpConnThroughput.

Le dispositif PS DOIT réinitialiser à une valeur égale à 0 chacun des objets cabhCtpConnPktsSent, cabhCtpConnPktsRecv, cabhCtpConnRTT et cabhCtpConnThroughput quand l'utilitaire de vitesse de connexion est lancé (c'est-à-dire quand la valeur de l'objet cabhCtpConnControl est réglée à start(1)).

Le temps RTT de l'utilitaire de vitesse de connexion est mesuré dans le dispositif PS comme étant la durée écoulée entre le premier bit du premier paquet envoyé et le dernier bit du dernier paquet reçu. Le temps RTT n'est valide que si le nombre de paquets reçus est égal au nombre de paquets envoyés.

Le dispositif PS DOIT permettre le réglage de l'adresse IP de destination de l'utilitaire de vitesse de connexion (objet cabhCtpConnDestIp) à toute adresse IPv4 valide de tout dispositif IP de réseau

local accessible par une quelconque interface LAN/PS exécutant l'utilitaire de vitesse de connexion de portail CTP.

Le réglage de l'objet de commande de l'utilitaire de vitesse de connexion, cabhCtpConnControl, à la valeur start(1) DOIT se traduire par l'exécution de l'utilitaire de vitesse de connexion.

Le réglage de l'objet de commande de l'utilitaire de vitesse de connexion, cabhCtpConnControl, à la valeur abort(2) DOIT se traduire par la fin de l'exécution de l'utilitaire de vitesse de connexion.

La valeur par défaut de l'objet cabhCtpConnStatus est notRun(1), ce qui indique que l'utilitaire de vitesse de connexion n'a jamais été exécuté.

Le dispositif PS DOIT régler la valeur de l'objet cabhCtpConnStatus à running(2) si l'utilitaire a été chargé de démarrer, n'a pas été fermé et si le temporisateur de vitesse de connexion n'est pas arrivé à expiration.

Le dispositif PS DOIT régler la valeur de l'objet cabhCtpConnStatus à complete(3) quand le dernier paquet émis par l'utilitaire de vitesse de connexion est reçu par le portail CTP.

Le dispositif PS DOIT régler la valeur de l'objet cabhCtpConnStatus à aborted(4) si l'utilitaire de vitesse de connexion est fermé après avoir été lancé par une commande SNMP de mise à jour (SET) à la valeur abort(2) de l'objet cabhCtpConnControl, ou si l'essai est fermé autrement avant que le dernier paquet émis par l'utilitaire de vitesse de connexion ait été reçu et avant que le temporisateur de l'utilitaire de vitesse de connexion (objet cabhCtpConnTimeOut) arrive à expiration.

Le dispositif PS DOIT régler la valeur de l'objet cabhCtpConnStatus à timedOut(5) si le temporisateur de l'utilitaire de vitesse de connexion (objet cabhCtpConnTimeOut) arrive à expiration avant que le dernier paquet émis par l'utilitaire de vitesse de connexion ait été reçu par le portail CTP.

Le dispositif PS NE DOIT PAS utiliser de quelconque adresse IP comme adresse IP d'origine de l'utilitaire de vitesse de connexion (objet cabhCtpConnSrcIp) à l'exception d'une adresse IP actuelle et valide d'interface PS WAN-Data (c'est-à-dire une valeur active de l'objet cabhCdpWanDataAddrIp) ou d'une adresse IP actuelle et valide d'interface PS LAN. Si une valeur non valide est configurée pour l'objet cabhCtpConnSrcIp, le dispositif PS DOIT traiter l'exécution de l'essai comme un cas abandonné et régler l'objet d'état de l'utilitaire de vitesse de connexion, cabhCtpConnStatus, à la valeur 'aborted' puis signaler l'événement approprié (voir le Tableau B.1).

6.4.3.2 Fonction d'utilitaire de sondage par écho du portail CTP

6.4.3.2.1 Fonction d'utilitaire de sondage par écho: objectifs

L'objectif de la fonction d'utilitaire de sondage par écho est de permettre au gestionnaire du système d'essayer ou de vérifier à distance la connexité entre le dispositif PS et un dispositif IP de réseau local spécifique.

6.4.3.2.2 Fonction d'utilitaire de sondage par écho: directives de conception du système

Les directives de conception énumérées dans le Tableau 6-25, Directives de conception du système de portail CTP, ont servi à orienter la spécification de la fonction d'utilitaire de sondage par écho.

6.4.3.2.3 Fonction d'utilitaire de sondage par écho: description du système

La fonction d'utilitaire de sondage par écho est appelée à vérifier la connexité entre le dispositif PS et des dispositifs IP de réseau local ou dispositifs de serveur local IPCable2Home individuels. Les résultats de multiples exécutions de l'essai par utilitaire de sondage par écho peuvent être rassemblés par le système NMS afin de créer une exploration par le réseau des dispositifs IP de réseau local ou des dispositifs de serveur local IPCable2Home. La table DHCP du portail CDP contient une liste historique de dispositifs, mais seulement de ceux qui emploient le protocole DHCP. Le sondage par écho peut saisir un état actuel incluant des clients non DHCP. Afin de

garder une certaine simplicité au dispositif PS, on suppose que le système NMS augmente l'adresse et mémorise les résultats dans l'utilitaire du système NMS afin d'exécuter l'exploration d'un sous-réseau local.

L'utilitaire de sondage par écho est lancé par une série de messages SNMP de requête de mise à jour (SET) envoyés par la console du système NMS du réseau câblé vers l'adresse de gestion des services de portail.

Le paragraphe 12.2.1.2 décrit en détail le fonctionnement de l'utilitaire de sondage par écho.

6.4.3.2.4 Fonction d'utilitaire de sondage par écho: exigences

L'utilitaire de sondage par écho du portail CTP DOIT être implémentée au moyen de la fonction "écho" du protocole de message de commande Internet (ICMP, *Internet control message protocol*). Le portail CTP enverra une demande d'écho ICMP et le dispositif IP de réseau local est censé renvoyer une réponse d'écho ICMP.

Le portail CTP DOIT ignorer et exclure du décompte cabhCtpPingNumRecv toute réponse d'écho reçue après l'expiration de la temporisation cabhCtpPingTimeOut.

Le dispositif PS DOIT implémenter l'utilitaire de sondage par écho du portail CTP et DOIT être conforme aux valeurs par défaut et aux étendues de valeurs définies pour les objets spécifiques de l'utilitaire de sondage par écho contenus dans la base MIB de portail CTP [voir § E.3].

Quand le système NMS déclenche le lancement par le dispositif PS de l'utilitaire de sondage par écho en réglant l'objet cabhPingControl à la valeur = start(1), le dispositif PS DOIT effectuer ce qui suit:

- régler l'objet cabhCtpPingStatus à la valeur = running(2);
- envoyer à l'adresse IP définie par la valeur de l'objet cabhCtpPingDestIp autant de sondages par écho (requêtes ICMP) que spécifié par la valeur de l'objet cabhCtpPingNumPkts, en utilisant comme adresse d'origine de chaque requête la valeur de l'objet cabhCtpPingSrcIp. La longueur de chaque trame d'essai est la valeur de l'objet cabhCtpPingPktSize. La temporisation de chaque validation (paire de demande/réponse d'écho ICMP) est la valeur de l'objet cabhCtpPingTimeOut;
- si la valeur de l'objet cabhCtpPingNumPkts est supérieure à 1, attendre pendant la durée définie par la valeur de l'objet cabhCtpPingTimeBetween entre chaque demande de validation envoyée par le portail CTP.

Si le portail CTP reçoit toutes les réponses de validation avant l'expiration d'un de leurs temporisateurs individuels, le dispositif PS DOIT régler l'objet cabhCtpPingStatus à la valeur = complete(3) et signaler l'événement approprié (voir l'Annexe B – Evénements de portail CTP).

Si l'utilitaire de sondage par écho est fermé par le système NMS par réglage de l'objet cabhCtpPingControl à la valeur = abort(2) ou pour toute autre raison avant que le dernier bit soit reçu du dispositif IP de réseau local cible et avant que le temporisateur soit fermé, le dispositif PS DOIT régler l'objet cabhCtpPingStatus à la valeur = aborted(4) et signaler l'événement approprié (voir l'Annexe B – Evénements de portail CTP).

Si un temporisateur arrive à expiration pendant au moins un des sondages avant que sa réponse soit reçue du dispositif IP de réseau local cible, le dispositif PS DOIT régler l'objet cabhCtpPingStatus à la valeur = timedOut(5) et signaler l'événement approprié (voir l'Annexe B – Evénements de portail CTP).

Quand la fonction d'utilitaire de sondage par écho du portail CTP est lancée, le dispositif PS DOIT calculer la valeur moyenne du temps d'aller-retour entre le dispositif PS et le dispositif IP de réseau local ou le dispositif de serveur local IPCable2Home dont l'adresse est transmise dans l'objet cabhCtpPingDestIp (le dispositif IP de réseau local cible) d'après le nombre de demandes de

sondage par écho défini par l'objet cabhCtpPingNumPkts et mémoriser le résultat dans l'objet cabhCtpPingAvgRTT. Quand la fonction d'utilitaire de sondage par écho du portail CTP est lancée, le dispositif PS DOIT déterminer les temps d'aller-retour minimal et maximal entre le dispositif PS et le dispositif IP de réseau local cible, pour l'ensemble des demandes de sondage par écho définies par l'objet cabhCtpPingNumPkts et mémoriser les valeurs dans les objets cabhCtpPingMinRTT et cabhCtpPingMaxRTT, respectivement.

Si une erreur de protocole ICMP se produit pendant l'exécution de l'utilitaire de sondage par écho, le dispositif PS DOIT incrémenter la valeur de l'objet cabhCtpPingNumIcmpError et journaliser l'erreur dans l'objet cabhCtpPingIcmpError. La dernière erreur ICMP qui se produit remplace la précédente par surécriture.

Le dispositif PS DOIT réinitialiser à la valeur 0 chacun des objets cabhCtpPingNumSent, cabhCtpPingNumRecv, cabhCtpPingAvgRTT, cabhCtpPingMaxRTT, cabhCtpPingMinRTT, cabhCtpPingNumIcmpError et cabhCtpPingIcmpError quand l'utilitaire de sondage par écho est lancé (c'est-à-dire quand la valeur de l'objet cabhCtpPingControl est réglée à start(1)).

Le temps RTT de l'utilitaire de sondage par écho est mesuré dans le dispositif PS comme la durée écoulée entre le moment où le dernier bit de chaque paquet de demande d'écho ICMP est transmis par l'utilitaire de sondage par écho du portail CTP, et le moment où le dernier bit du paquet correspondant de réponse d'écho ICMP est reçu.

Le dispositif PS DOIT permettre de régler l'adresse IP de destination de l'utilitaire de sondage par écho (objet cabhCtpPingDestIp) à toute adresse IPv4 valide de tout dispositif IP de réseau local ou dispositif de serveur local IPCable2Home accessible par une quelconque interface LAN PS exécutant l'utilitaire de sondage par écho du portail CTP.

Le dispositif PS NE DOIT PAS produire de paquets à la sortie d'une quelconque interface avec un réseau régional lors de l'exécution de la fonction d'utilitaire de sondage par écho.

Le dispositif PS NE DOIT PAS utiliser une quelconque adresse IP comme adresse IP d'origine de l'utilitaire de sondage par écho (objet cabhCtpPingSrcIp) à l'exception d'une adresse IP actuelle et valide d'interface PS WAN-Data (c'est-à-dire une valeur active de l'objet cabhCdpWanDataAddrIp) ou d'une adresse IP actuelle et valide d'interface PS/LAN. Si une valeur non valide est configurée pour l'objet cabhCtpPingSrcIp, le dispositif PS DOIT traiter l'exécution de l'essai comme un cas abandonné, régler à la valeur "abandonnée" l'objet d'état de l'utilitaire de sondage par écho – cabhCtpPingStatus – et signaler l'événement approprié (voir le Tableau B.1).

7 Utilitaires de préconfiguration

7.1 Introduction et aperçu général

L'élément de services de portail et les dispositifs IP de réseau local doivent être correctement initialisés et configurés afin d'échanger des informations significatives l'un avec l'autre et avec les éléments connectés au réseau câblé et au réseau Internet. Les utilitaires de préconfiguration IPCable2Home permettent à cette initialisation et à cette configuration de se produire de façon transparente et avec une intervention minimale de l'utilisateur. Ils permettent également au câblo-opérateur d'apporter de la valeur ajoutée aux abonnés au service de transmission de données en définissant les processus par lesquels ce câblo-opérateur peut faciliter et personnaliser l'initialisation et la configuration du dispositif PS et du dispositif IP de réseau local. Les trois utilitaires de préconfiguration définis afin d'accomplir cette tâche sont énumérés ci-dessous:

- fonction de portail DHCP par câble (CDP) dans l'élément de services de portail;
- utilitaire de configuration globale des services de portail (BPSC, *bulk portal services configuration*);
- client d'heure locale dans l'élément de services de portail.

7.1.1 Objectifs

Les objectifs des utilitaires de préconfiguration sont énumérés ci-dessous:

- permettre au dispositif PS d'acquérir une adresse réseau sur son interface avec un réseau régional à utiliser pour la gestion du dispositif PS;
- permettre au dispositif PS d'acquérir une ou plusieurs adresses réseau sur son interface avec un réseau régional, à utiliser pour l'échange de trafic entre dispositifs IP de réseau local et l'Internet ou entre dispositifs de serveur local IPCable2Home et l'Internet;
- permettre au dispositif PS de demander et d'acquérir des paramètres de configuration dans un fichier de configuration;
- permettre au dispositif PS d'acquérir l'heure locale à partir des services d'heure locale se trouvant dans le réseau de données du câblo-opérateur;
- permettre au dispositif PS d'attribuer des locations d'adresse réseau à des dispositifs IP de réseau local et à des dispositifs de serveur local IPCable2Home;
- permettre au dispositif PS d'attribuer des paramètres de configuration à des dispositifs IP de réseau local et à des dispositifs de serveur local IPCable2Home.

7.1.2 Hypothèses

Les hypothèses de fonctionnement des utilitaires de préconfiguration sont énumérées ci-dessous:

- les dispositifs IP de réseau local et les dispositifs de serveur local IPCable2Home implémentent un client du protocole DHCP comme défini par le document [RFC 2131];
- le système de préconfiguration du réseau câblé implémente un serveur DHCP comme défini par [RFC 2131];
- si le serveur DHCP du système de préconfiguration du réseau câblé prend en charge l'option DHCP 61 (option d'identificateur de client), l'interface IP avec le réseau WAN-Man et toutes les interfaces IP avec le réseau WAN-Data peuvent partager une adresse de commande MAC commune;
- les dispositifs IP de réseau local et les dispositifs de serveur local IPCable2Home peuvent prendre en charge diverses options DHCP et diverses extensions BOOTP de vendeur, autorisées par [RFC 2132];
- la configuration globale des services de portail sera réalisée par le téléchargement d'un fichier de configuration du dispositif PS contenant un ou plusieurs paramètres, au moyen du protocole trivial de transfert de fichiers (TFTP) [RFC 1350] ou du protocole de transfert d'hypertextes (HTTP) [RFC 2616] avec sécurité de la couche Transport (TLS, *transport layer security*) [RFC 2246];
- le serveur DHCP de la tête de réseau offrira à l'interface WAN-Man une option DHCP désignant un serveur temporel fonctionnant dans la tête de réseau.

7.2 Architecture de préconfiguration

7.2.1 Modes de préconfiguration

Trois modes de préconfiguration sont pris en charge. Ils sont désignés par les termes de *mode de préconfiguration DHCP (mode DHCP)*, *mode de préconfiguration SNMP (mode SNMP)* et *mode IPCable2Home inactif*. Ces trois modes de préconfiguration sont comparés dans le Tableau 7-1.

Tableau 7-1/J.192 – Modes de préconfiguration

	Mode DHCP	Mode SNMP	Mode IPCable2Home inactif
Champs et codes d'option DHCP	Reçoit les informations du fichier de configuration contenues dans les champs 'siaddr' et 'file'. Ne reçoit aucune option 122.	Ne reçoit aucun fichier d'informations de configuration. Reçoit des valeurs valides pour les sous-options 3, 6 et 10 de l'option 122.	Ne reçoit aucune information du fichier de configuration ni aucune option 122, ou reçoit une combinaison non valide d'informations du fichier de configuration et de sous-options de l'option 122.
Déclenchement du fichier de configuration du dispositif PS	Déclenché par la présence d'informations de serveur TFTP dans un message DHCP	Déclenché par NMS par message en protocole SNMP	PS ne reçoit aucun fichier de configuration
Exigence du fichier de configuration du dispositif PS	Le téléchargement du fichier de configuration du dispositif PS est requis	Le téléchargement du fichier de configuration du dispositif PS n'est pas requis	Le fichier de configuration du dispositif PS n'est pas requis

Le comportement spécifié des utilitaires de préconfiguration dépend du mode de préconfiguration dans lequel le dispositif PS fonctionne.

Le paragraphe 13, "Processus de préconfiguration", décrit la séquence d'événements pour les modes de préconfiguration DHCP et SNMP.

7.2.2 Description de l'architecture de préconfiguration

L'architecture de préconfiguration est illustrée dans la Figure 7-1. Les éléments de services de portail vont interagir avec les fonctions de serveur dans le réseau câblé à l'interface avec l'hybride HFC, ou avec les dispositifs de serveur local IPCable2Home afin de répondre aux directives de conception du système énumérées dans le § 7.3.2.

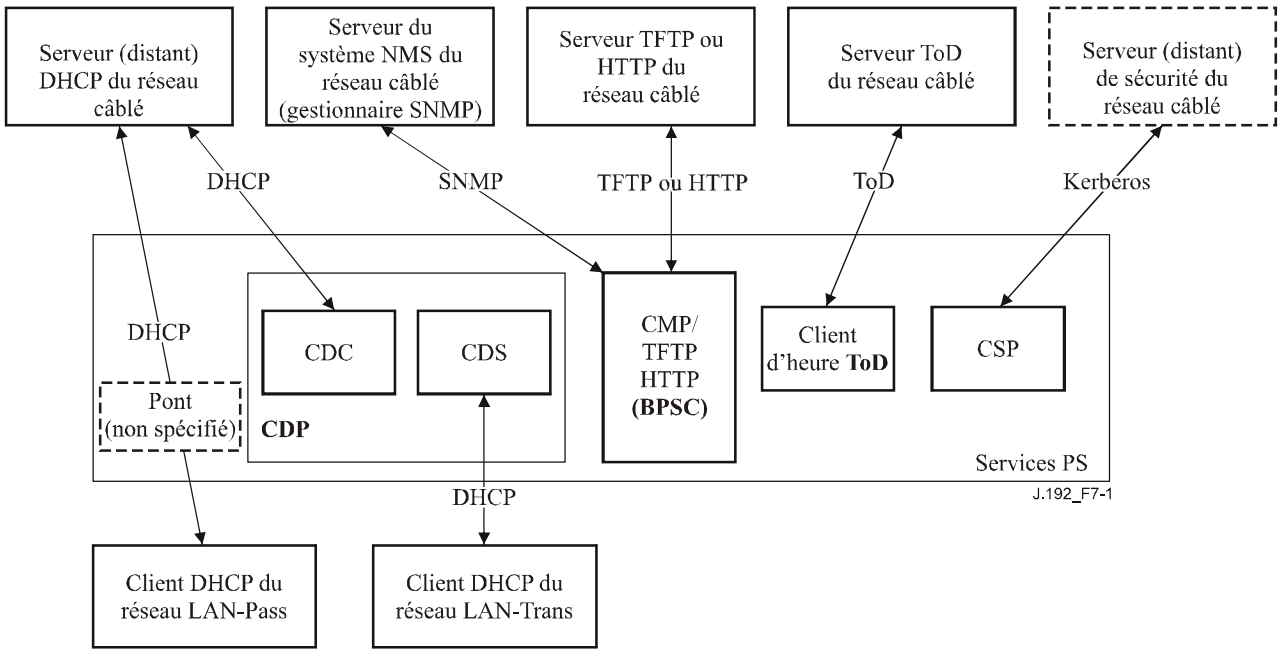


Figure 7-1/J.192 – Architecture de préconfiguration

7.3 Elément logique des services de portail – Portail DHCP par câble (CDP)

Le portail DHCP IPCable2Home (CDP) est un sous-élément de l'élément logique des services de portail. Le portail CDP a deux rôles principaux: l'acquisition des locations d'adresse réseau pour le dispositif PS et l'attribution des locations d'adresse réseau à des dispositifs IP de réseau local et à des dispositifs de serveur local IPCable2Home dans le réseau local. C'est un des trois utilitaires de préconfiguration présentés dans le § 7.1. Le présent paragraphe décrit les objectifs, les directives de conception du système, la description du système et les exigences se rapportant au portail CDP.

7.3.1 Objectifs du portail CDP

Les objectifs du portail CDP sont les suivants:

- permettre que les fonctions de client contenues dans le dispositif PS puissent communiquer avec les fonctions de serveur correspondantes dans le réseau de données par câble;
- fournir au dispositif PS des paramètres de configuration initiaux, lui donnant la capacité de continuer à se configurer par lui-même.

7.3.2 Directives de conception du système de portail CDP

Les directives de conception suivantes (Tableau 7-2) régissent les capacités définies pour le portail CDP:

Tableau 7-2/J.192 – Directives de conception du système de portail CDP

Numéro	Directives de conception du système de portail CDP
CDP 1	Les mécanismes d'adressage seront commandés par l'opérateur et offriront à celui-ci la connaissance des éléments IPCable2Home de réseau et des dispositifs IP de réseau local, ainsi que l'accessibilité à ces éléments et dispositifs.
CDP 2	Les processus d'acquisition et de gestion des adresses n'exigeront pas d'intervention humaine (en supposant qu'un compte d'utilisateur/de foyer a déjà été établi).
CDP 3	L'acquisition et la gestion des adresses seront échelonnables afin de prendre en charge l'augmentation attendue du nombre de dispositifs IP de réseau local.
CDP 4	Il est préférable que les adresses des dispositifs IP de réseau local restent les mêmes après des événements tels qu'un cycle d'alimentation ou un changement de fournisseur de services Internet.
CDP 5	Offrir un mécanisme permettant de surveiller et de contrôler le nombre de dispositifs IP de réseau local dans le secteur LAN-Trans.
CDP 6	Les communications résidentiels continueront à fonctionner comme prévu pendant les périodes de panne de serveur d'adresses de la tête de réseau. La prise en charge de l'adressage sera assurée pour les dispositifs IP de réseau local nouvellement ajoutés et pour les expirations d'adresse pendant les pannes de serveur d'adresses distant.
CDP 7	Les adresses IP seront conservées si possible (aussi bien les adresses acheminables mondialement que les adresses privées de gestion de réseau câblé).

7.3.3 Description du système de portail DHCP IPCable2Home

Le portail DHCP IPCable2Home (CDP) est l'entité logique qui est responsable des activités d'adressage. Les responsabilités du portail CDP en termes de demande d'adresse et d'attribution d'adresse sont les suivantes dans l'environnement IPCable2Home:

- l'attribution d'adresse IP, la maintenance d'adresse IP et la livraison des paramètres de configuration (par protocole DHCP) à des dispositifs IP de réseau local situés dans le secteur d'adresses du réseau LAN-Trans;

- l'acquisition d'une adresse IP de réseau WAN-Man et de zéro, une ou plusieurs adresses IP de réseau WAN-Data et des paramètres de configuration DHCP associés à l'élément de services de portail;
- fournir des informations au portail de nommage IPCable2Home (CNP) afin de prendre en charge des services de nom de serveur de dispositif IP de réseau local.

Le dispositif PS conserve deux adresses de matériel, dont l'une doit servir à acquérir une adresse IP aux fins de gestion et dont l'autre pourra servir à l'acquisition d'une ou de plusieurs adresse(s) IP pour des données. Afin d'empêcher la simulation d'une adresse matérielle, le dispositif PS ne permet pas la modification de l'une quelconque des deux adresses de matériel.

L'élément de services de portail exige une adresse IP dans le réseau local résidentiel pour son rôle de routeur dans le réseau local (voir § 8, "Traitement de paquet et conversion d'adresse"), de serveur DHCP (CDS) et de serveur DNS (voir § 9, "Résolution du nom"). Le dispositif PS reçoit les signaux issus d'une unique adresse IP du côté réseau local pour chacune de ces fonctionnalités. Il a besoin de communiquer cette adresse IP aux dispositifs IP du réseau local indiqués dans les champs d'option OFFER et ACK du protocole DHCP pour chacune de ces fonctionnalités de serveur distant. De façon à identifier de façon unique ces valeurs d'option, chacune de ces adresses de serveur distant est identifiée par différents objets de base MIB contenus dans le dispositif PS, dont la liste figure ci-dessous et dans le Tableau 7-2.

Adresse du routeur (passerelle par défaut)	cabhCdpServerRouter	Option 3
Adresse du serveur distant de noms de domaine (DNS)	cabhCdpServerDnsAddress	Option 6
Adresse du serveur de configuration dynamique du serveur local (DHCP) (serveur CDS)	cabhCdpServerDhcpAddress	Option 54

La valeur par défaut de l'objet cabhCdpServerRouter est 192.168.0.1. Le système NMS peut cependant régler l'objet cabhCdpServerRouter à une valeur différente.

La valeur de l'objet cabhcdpServerDhcpAddress est toujours la même que celle de l'objet cabhCdpServerRouter et le système NMS ne peut pas modifier cette valeur directement.

La valeur par défaut de l'objet cabhCdpServerDnsAddress est égale à celle de l'objet cabhCdpServerRouter. Cependant, le système NMS peut la porter à une valeur différente (p. ex. à l'adresse du serveur DNS dans le réseau de données du câblo-opérateur) de façon qu'un dispositif IP de réseau local puisse orienter ses requêtes DNS vers un serveur distant autre que le serveur DNS du dispositif PS.

Ainsi, le dispositif PS reçoit toujours l'adresse IP assignée à l'objet cabhCdpSeverRouter pour ses fonctionnalités de routeur du côté réseau local, de serveur distant de noms (DNS), et de serveur distant DHCP.

Comme représenté dans la Figure 7-2, les capacités du portail CDP sont intégrées dans deux éléments fonctionnels résidant dans le portail CDP:

- le serveur distant de protocole DHCP par câble (CDS);
- le client IPCable2Home du protocole DHCP (client CDC).

La Figure 7-2 décrit également l'interaction entre les composants du portail CDP et les secteurs d'adresses présentés dans le § 5. Le client CDC échange des messages DHCP avec le serveur DHCP se trouvant dans le réseau câblé (secteur d'adresses de réseau WAN-Man) afin d'acquérir une adresse IP et des options DHCP pour le dispositif PS, aux fins de la gestion. Le client CDC pourrait également échanger des messages DHCP avec le serveur DHCP se trouvant dans le réseau câblé

(secteur d'adresses de réseau WAN Data) afin d'acquérir zéro (0), une ou plusieurs adresse(s) IP au compte de dispositifs IP de réseau local situés dans le secteur LAN-Trans. Le serveur CDS échange des messages DHCP avec les dispositifs IP de réseau local situés dans le secteur LAN-Trans et attribue des adresses IP privées, accorde des connexions louées et pourrait fournir des options DHCP à des clients du protocole DHCP implantés dans ces dispositifs IP de réseau local.

Les dispositifs IP de réseau local situés dans le secteur LAN-Pass reçoivent leurs adresses IP, leurs connexions louées et leurs options DHCP directement du serveur DHCP implanté dans le réseau câblé. Le portail CDP dérive les messages DHCP entre le serveur DHCP implanté dans le réseau câblé et les dispositifs IP de réseau local implantés dans le secteur LAN-Pass.

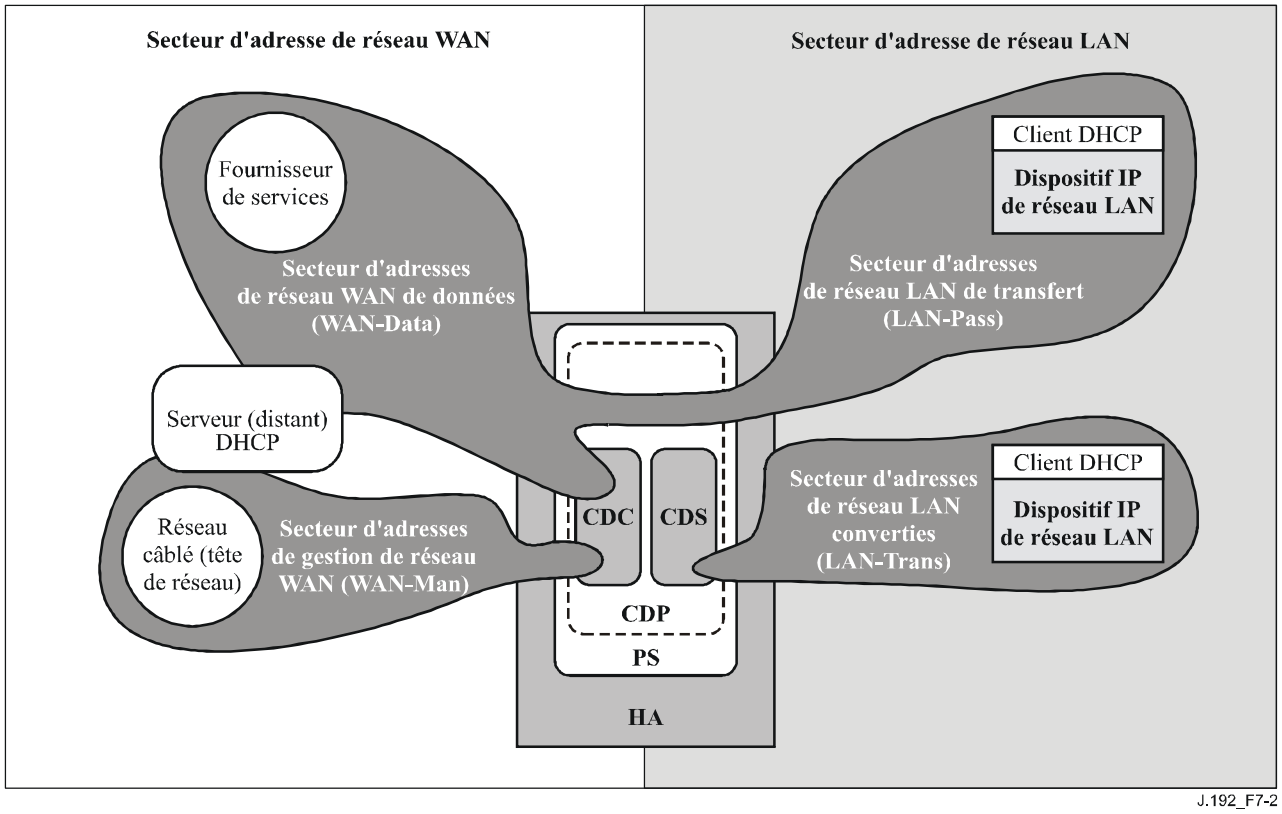


Figure 7-2/J.192 – Fonctions du portail CDP

Un dispositif PS intégré peut être configuré de façon à fonctionner dans l'un quelconque de quatre modes opératoires, comme décrit dans le § 5.5, sur la base de la valeur de l'objet esafePsCableHomeModeControl de base MIB eSAFE eDOCSIS [eDOCSIS1] (ePS seulement) et sur la base des valeurs des champs et options d'en-tête DHCP contenus dans le message ACK du DHCP reçu du serveur DHCP du câblo-opérateur. Si la valeur de l'objet esafePsCableHomeModeControl est mise à provSystem(2), le dispositif PS intégré est tenu d'essayer d'acquérir une location d'adresse IP de réseau WAN-Man du dispositif PS et d'agir sur les valeurs et options d'en-tête DHCP. Si la valeur de l'objet esafePsCableHomeModeControl est dormantCHMode(3), le dispositif PS intégré est tenu d'essayer d'acquérir une location d'adresse IP à utiliser pour sa fonction de conversion d'adresse et de portail de réseau (NAPT) (voir § 8, Traitement de paquet et conversion d'adresse) et est tenu de négliger les valeurs de champ et d'option d'en-tête DHCP qui sinon le configureraient de façon à fonctionner dans un mode autre que le mode CableHome inactif. Voir au § 7.3.3.2.4 une description complète du mode CableHome inactif. Si l'objet esafePsCableHomeModeControl est mis à la valeur disabled(1), le dispositif PS intégré n'essaie pas d'effectuer une préconfiguration et fonctionne en mode désactivé comme décrit dans le § 7.3.3.2.4.

Un dispositif PS autonome est toujours tenu d'essayer d'acquérir une location d'adresse IP de réseau WAN-Man de PS et est configuré de façon à fonctionner dans l'un quelconque de trois modes opératoires, sur la base des valeurs des champs et options d'en-tête DHCP. Un dispositif PS autonome ne peut pas être configuré de façon à fonctionner en mode désactivé. Voir le § 7.3.3.2.4 pour plus de détails.

7.3.3.1 Sous-élément du serveur DHCP (CDS)

Le serveur CDS est un sous-élément de l'élément logique de portail CDP du dispositif PS. C'est la fonction chargée d'attribuer des locations d'adresse réseau à des dispositifs IP de réseau local dans le secteur LAN-Trans. Il est également chargé de fournir aux dispositifs IP de réseau local des informations de configuration par codes d'option DHCP, comme spécifié dans [RFC 2132]. Le serveur CDS est tenu d'exécuter cette fonction, que le dispositif PS ait ou non une connexion WAN active.

7.3.3.1.1 Fonction de serveur CDS: objectifs

Les objectifs de la fonction de serveur CDS sont les suivants:

- attribuer des locations d'adresse réseau à des dispositifs IP de réseau local dans le secteur LAN-Trans conformément aux réglages de la base MIB du portail CDP et conformément à [RFC 2131];
- attribuer des informations de configuration conformément à [RFC 2132];
- répondre aux objectifs de fonctionnement en l'absence de connexion WAN en attribuant des locations d'adresse IP dans le secteur LAN-Trans et fournir des informations de configuration à des dispositifs IP de réseau local sur demande aussi longtemps que le dispositif PS est opérationnel, que le dispositif PS ait ou non une connexion WAN active;
- ne pas attribuer de locations d'adresse IP et ne pas fournir d'informations de configuration à des dispositifs IP de réseau local que le dispositif PS a été configuré de façon à traiter comme existant dans le secteur LAN-Pass.

7.3.3.1.2 Fonction de serveur CDS: directives de conception du système

Les directives de conception énumérées dans le Tableau 7-3 ont guidé la mise au point des spécifications de la fonction de serveur CDS.

Tableau 7-3/J.192 – Fonction de serveur distant de protocole DHCP par câble (CDS) – Directives de conception du système

Numéro	Directives de conception du système de fonction de serveur CDS
CDS 1	Permettre aux dispositifs IP de réseau local d'acquérir des locations d'adresse réseau et des informations de configuration pour le secteur LAN-Trans.
CDS 2	Le mécanisme d'attribution des adresses IP dans le secteur LAN-Trans et des informations de configuration fonctionnera, que le dispositif PS ait ou non une connexion WAN avec le réseau de transmission de données du câblo-opérateur.
CDS 3	Le mécanisme d'attribution des locations d'adresse IP dans le secteur LAN-Trans et des informations de configuration n'attribuera pas de locations d'adresse IP ou ne fournira pas d'informations de configuration pour les dispositifs IP de réseau local dans le secteur LAN-Pass.

7.3.3.1.3 Fonction de serveur CDS: description du système

Le serveur CDS est un serveur DHCP normalisé, comme défini dans [RFC 2132]. Ses responsabilités sont les suivantes:

- le serveur CDS attribue les adresses et délivre les paramètres de configuration DHCP aux dispositifs IP de réseau local recevant une adresse dans le secteur d'adresses du réseau LAN-Trans. Le serveur CDS apprend les options DHCP à partir du système NMS et offre ces options DHCP à des dispositifs IP de réseau local. Si des options DHCP n'ont pas été offertes par le système NMS (par exemple quand le dispositif PS s'amorce pendant une panne du câble), le serveur CDS se fonde sur les valeurs par défaut intégrées (DefVals) pour les options nécessaires;
- le serveur CDS est capable d'offrir des services d'adressage DHCP à des dispositifs IP de réseau local, indépendamment de l'état de connexité du réseau régional;
- le nombre d'adresses fournies par le serveur CDS à des dispositifs IP de réseau local est contrôlable par le système NMS. Le comportement du serveur CDS quand une limite réglable par le câblo-opérateur est dépassée est également configurable par le système NMS. Les actions possibles du serveur CDS quand la limite est dépassée sont les suivantes:
  1) attribuer une adresse IP de réseau LAN-Trans et traiter l'interconnexion WAN-LAN par conversion CAT comme cela se serait normalement produit si la limite n'avait pas été dépassée;
  2) ne pas attribuer d'adresse aux dispositifs IP de réseau local demandeurs. Un réglage à 0 du seuil d'adresses indique le seuil maximal possible pour la réserve d'adresses IP de réseau LAN-Trans définie par les valeurs "start" (début) (objet cabhCdpLanPoolStart) et "end" (fin) (objet cabhCdpLanPoolEnd) de la réserve;
- en l'absence d'informations sur l'heure locale à partir du serveur temporel (ToD, *time of day*), le serveur CDS fait appel à l'instant de début par défaut du service de portail: 00:00.0 (minuit) GMT le 1er janvier 1970, met à jour l'heure d'expiration pour toutes les connexions louées qui sont actives dans le secteur LAN-Trans afin de se resynchroniser avec les clients du protocole DHCP situés dans des dispositifs IP de réseau local, et conserve ces connexions louées sur la base de cet instant de début jusqu'à ce que le dispositif PS se synchronise avec le serveur temporel dans le réseau câblé;
- pendant le processus d'amorçage du dispositif PS, le serveur CDS reste inactif jusqu'à son activation par le dispositif PS;
- si le mode primaire de traitement de paquet du dispositif PS (objet cabhCapPrimaryMode) a été réglé au transfert et si le processus de préconfiguration du dispositif PS s'est achevé (ce qui est indiqué par l'objet cabhPsDevProvState à la valeur = pass(1)), alors le serveur CDS est désactivé.

Les dispositifs IP de réseau local peuvent recevoir des adresses qui résident dans le secteur LAN-Pass. Comme représenté dans la Figure 7-2, les demandes d'adresse LAN-Pass sont servies par l'infrastructure d'adressage du réseau régional, et non par le dispositif PS. Les processus d'adressage LAN-Pass interviendront quand le dispositif PS sera configuré de façon à fonctionner en mode de transfert ou en mode mixte de routage/acheminement (voir § 8.3.4.3, Exigences relatives au mode de transfert, pour plus de détails). Dans ces cas, les interactions DHCP surviendront directement entre dispositifs IP de réseau local et serveurs du réseau de données par câble. La présente Recommandation ne spécifie pas ce processus.

Dans l'ensemble de la présente Recommandation, les termes **Attribution dynamique** et **Attribution manuelle** sont utilisés comme défini dans [RFC 2132]. Les **options DHCP fournies par le serveur CDS**, objets cabhCdpServer dans la base MIB du portail CDP, sont des options DHCP qui peuvent être préconfigurées par le système NMS et qui sont offertes par le serveur CDS

à des dispositifs IP de réseau local munis d'une adresse LAN-Trans. Les options DHCP préconfigurées par le serveur CDS, objets cabhCdpServer, persistent après un cycle d'alimentation électrique du dispositif PS et le système NMS peut établir, lire, écrire et supprimer ces objets. Les options DHCP préconfigurées par le serveur CDS, objets cabhCdpServer, sont conservées pendant les périodes de panne du câble et ces objets sont offerts aux dispositifs IP de réseau local munis d'une adresse LAN-Trans pendant les périodes de panne du câble. Le stockage persistant par le client CDC des options DHCP est compatible avec [RFC 2132], section 2.1. Les valeurs par défaut des options DHCP préconfigurées par le serveur CDS – objet cabhCdpServer – sont définies (Tableau 7-4) et le système NMS peut réinitialiser les options DHCP fournies par le serveur CDS, objets cabhCdpServer et cabhCdpLanAddrTable, à leurs valeurs par défaut, par écriture dans l'objet de base MIB cabhCdpSetToFactory.

Les objets de seuil d'adresses du serveur CDS (objet cabhCdpLanTrans) contiennent les paramètres de commande d'événement utilisés par le serveur CDS afin de signaler au portail CMP l'ordre de produire une notification à destination du système de gestion de la tête de réseau, quand le nombre d'adresses LAN-Trans attribuées par le serveur CDS dépasse le seuil préétabli.

L'objet de décompte d'adresses (objet cabhCdpLanTransCurCount) est une valeur indiquant le nombre d'adresses LAN-Trans attribuées par le serveur CDS qui ont des connexions louées actives en protocole DHCP.

L'objet de seuil d'adresses (objet cabhCdpLanTransThreshold) est une valeur indiquant le moment où une notification sera produite à destination du système de gestion de la tête de réseau. La notification sera produite quand le serveur CDS attribuera une adresse au dispositif IP de réseau local qui provoque un dépassement du seuil (objet cabhCdpLanTransThreshold) de décompte d'adresses (objet cabhCdpLanTransCurCount).

L'action sur dépassement de seuil (objet cabhCdpLanTransAction) est celle qui est effectuée par le serveur CDS lorsque le décompte d'adresses (objet cabhCdpLanTransCurCount) dépasse le seuil d'adresses (objet cabhCdpLanTransThreshold). Si l'action sur dépassement de seuil (objet cabhCdpLanTransAction) permet des attributions d'adresses après le dépassement du décompte, la notification est produite chaque fois qu'une adresse est attribuée. Les actions définies sont:

a) attribuer une adresse LAN-Trans comme en cas normal;

b) ne pas attribuer d'adresse au prochain dispositif IP de réseau local demandeur.

Le décompte d'adresses (objet cabhCdpLanTransCurCount) continue d'être mis à jour pendant les périodes de panne du câble.

La base MIB du serveur CDS contient également les paramètres de début de réserve d'adresses (objet cabhCdpLanPoolStart) et de fin de réserve d'adresses (objet cabhCdpLanPoolEnd). Ces paramètres indiquent l'étendue des adresses qui, dans le secteur LAN-Trans, peuvent être attribuées par le serveur CDS à des dispositifs IP de réseau local.

La table d'adresses de réseau local du portail CDP (objet cabhCdpLanAddrTable) contient la liste des paramètres associés aux adresses attribuées aux dispositifs IP de réseau local ayant des adresses de réseau LAN-Trans. Ces paramètres sont les suivants:

- identificateurs de client [RFC 2132], section 9.14 (objet cabhCdpLanAddrClientID);
- adresse IP de réseau local attribuée au client (objet cabhCdpLanAddrIp);
- indication précisant si l'adresse a été attribuée manuellement (par le portail CMP) ou dynamiquement (par le portail CDP) (objet cabhCdpLanAddrMethod).

Le serveur CDS mémorise les informations d'identification du dispositif IP de réseau local contenues dans l'objet de base MIB cabhCdpLanAddrClientID. Le serveur CDS fait appel à la valeur transmise dans le champ "chaddr" du message DHCP REQUEST émis par le dispositif IP de réseau local à cette fin.

Le serveur CDS crée une entrée de table CDP (objet cabhCdpLanAddrTable) quand il attribue une adresse IP à un dispositif IP de réseau local. Le serveur CDS peut créer des entrées de table CDP (objet cabhCdpLanAddrTable) pendant les périodes de panne du câble.

La table de portail CDP (objet cabhCdpLanAddrTable) conserve une durée de location DHCP pour chaque dispositif IP de réseau local.

Les entrées de table de portail CDP préconfigurées par le système NMS (objet cabhCdpLanAddrTable) sont conservées pendant les périodes de panne du câble et persistent au-delà d'un cycle d'alimentation du dispositif PS.

7.3.3.1.4 Fonction de serveur CDS: exigences

Le dispositif PS DOIT être conforme aux exigences relatives au serveur figurant dans [RFC 2131], section 4.3.

Le dispositif PS DOIT prendre en charge l'attribution d'adresse dynamique et manuelle conformément au [RFC 2131], section 1.

L'attribution manuelle d'adresse IP par le dispositif PS DOIT être prise en charge au moyen des entrées de base MIB de portail CDP (objet cabhCdpLanAddrTable) créées par le système NMS ou par le fichier de configuration du dispositif PS.

Afin de prendre en charge l'attribution dynamique d'adresses IP, le dispositif PS DOIT être capable de créer, de modifier et de supprimer des entrées de table cabhCdpLanAddrTable pour les dispositifs munis d'une adresse LAN-Trans.

Les entrées de la table de gestion des adresses de réseau local préconfigurées par portail CDP (objet cabhCdpLanAddrTable) DOIVENT être conservées pendant une panne du câble et DOIVENT persister après un cycle d'alimentation électrique du dispositif PS. Le dispositif PS DOIT être capable d'offrir des services d'adressage par protocole DHCP à des dispositifs IP de réseau local activés par le dispositif PS, indépendamment de l'état de connexité du réseau régional.

Lors d'une réinitialisation ou d'un réamorçage du dispositif PS, celui-ci NE DOIT PAS échanger de messages DHCP avec les dispositifs IP de réseau local avant que le serveur CDS ait été activé par le dispositif PS.

Celui-ci DOIT activer le serveur CDS, c'est-à-dire que le dispositif PS DOIT commencer à répondre aux messages DISCOVER et REQUEST du protocole DHCP reçus par une quelconque interface PS/LAN dans l'une quelconque des conditions suivantes (voir également la Figure 13-2, Modes de préconfiguration IPCable2Home – Partie 1):

- quand le dispositif PS doit fonctionner en mode de préconfiguration DHCP, après que le client CDC a reçu une location d'adresse IP de l'interface PS WAN-Man et après que le dispositif PS a reçu et correctement traité un fichier de configuration du dispositif PS;
- quand le dispositif PS doit fonctionner en mode de préconfiguration SNMP, après que le client CDC a reçu une location d'adresse IP de l'interface PS WAN-Man, qu'il s'est authentifié auprès du serveur du centre de distribution de clés (KDC) et qu'il s'est correctement enrôlé auprès du système NMS;
- quand la première tentative du client CDC d'acquérir une location d'adresse IP de l'interface PS WAN-Man échoue;
- quand le dispositif PS doit fonctionner en mode de préconfiguration DHCP et que la première tentative de téléchargement ou de traitement du fichier de configuration du dispositif PS échoue;
- quand le dispositif PS doit fonctionner en mode de préconfiguration SNMP et que la tentative d'authentification auprès du serveur de centre KDC échoue;

- quand le dispositif PS doit fonctionner en mode de préconfiguration SNMP et est appelé à télécharger un fichier de configuration du dispositif PS avant que le fonctionnement du serveur CDS soit lancé, et que la première tentative de téléchargement ou de traitement du fichier de configuration du dispositif PS échoue.

Le dispositif PS DOIT attribuer – à chaque dispositif IP de réseau local situé dans le secteur LAN-Trans qui demande une adresse IP par protocole DHCP – une adresse IP unique, extraite de la réserve d'adresses commençant par l'objet cabhCdpLanPoolStart et se terminant par l'objet cabhCdpLanPoolEnd, si le nombre d'adresses IP déjà attribuées par le serveur CDS est inférieur à la valeur de l'objet cabhCdpLanTransThreshold.

Si la valeur de l'objet cabhCdpLanTransThreshold est 0, le dispositif PS DOIT traiter le seuil comme s'il avait été affecté de la plus grande valeur possible afin de désigner la taille actuelle de la réserve d'adresses IP de réseau LAN-Trans (définie par les valeurs de début (objet cabhCdpLanPoolStart) et de fin (objet cabhCdpLanPoolEnd) de la réserve d'adresses IP de réseau LAN-Trans).

Le dispositif PS DOIT conserver le paramètre de décompte d'adresses (objet cabhCdpLanTransCurCount) indiquant le nombre de locations d'adresse de réseau LAN-Trans accordées à des dispositifs IP de réseau local.

Le dispositif PS DOIT augmenter le décompte d'adresses chaque fois qu'une location d'adresse LAN-Trans est accordée à un dispositif IP de réseau local et DOIT diminuer le décompte d'adresses chaque fois qu'une adresse LAN-Trans est libérée ou qu'une location d'adresse LAN-Trans arrive à expiration.

Le dispositif PS DOIT comparer le paramètre de décompte d'adresses (objet cabhCdpLanTransCurCount) au paramètre de seuil d'adresses (objet cabhCdpLanTransThreshold) après attribution d'une adresse LAN-Trans. Si le paramètre de décompte d'adresses (objet cabhCdpLanTransCurCount) dépasse le paramètre de seuil d'adresses (objet cabhCdpLanTransThreshold), le dispositif PS DOIT produire une notification conformément au mécanisme de signalisation des événements défini dans le § 6.3.3.2, Fonction de signalisation d'événement de portail CMP et dans l'Annexe B. Pendant que le paramètre de décompte d'adresses (objet cabhCdpLanTransCurCount) dépasse le paramètre de seuil d'adresses (objet cabhCdpLanTransThreshold), le dispositif PS DOIT être capable d'effectuer les actions suivantes sur dépassement de seuil en réponse au prochain message DISCOVER émis par le réseau local en protocole DHCP: attribuer une adresse LAN-Trans comme en cas normal ou ne pas attribuer d'adresse.

Si l'objet cabhCdpLanTranCurCount a une valeur égale ou supérieure à celle de l'objet cabhCdpLanTransThreshold et si un dispositif IP de réseau local demande une location additionnelle d'adresse IP, l'action spécifiquement effectuée par le dispositif PS DOIT être conforme à l'indication donnée par le paramètre d'action sur dépassement de seuil (objet cabhCdpLanTransAction) qui a été préconfiguré.

Le dispositif PS NE DOIT attribuer des adresses IP et livrer les paramètres de configuration DHCP énumérés dans le Tableau 7-4, pour lesquels le serveur CDS a une valeur valide, qu'à des dispositifs IP de réseau local recevant une adresse dans le secteur d'adresses du réseau LAN-Trans.

Si le câblo-opérateur préconfigure des valeurs pour une rangée dans l'objet cabhCdpLanAddrTable, le dispositif PS (serveur CDS) DOIT offrir (c'est-à-dire tenter d'attribuer) une location pour l'adresse IP cabhCdpLanAddrIp préconfigurée, au dispositif IP de réseau local dont l'adresse matérielle correspond à l'identificateur cabhCdpLanAddrClientID préconfiguré, en réponse à un message DHCP DISCOVER reçu de ce dispositif IP de réseau local.

Quand le serveur CDS attribue une location active pour une adresse IP à un dispositif IP de réseau local, le dispositif PS DOIT supprimer cette adresse de la réserve d'adresses IP disponibles pour attribution à des dispositifs IP de réseau local.

Si le serveur CDS reçoit, d'un dispositif IP de réseau local, une demande de location qu'il ne peut pas satisfaire en raison de l'indisponibilité d'adresses dans la réserve d'adresses IP (définie par les objets cabhCdpLanPoolStart et CabhCdpLanPoolEnd), le dispositif PS DOIT signaler l'événement conformément à l'Annexe B et au mécanisme de signalisation des événements défini dans le § 6.3.3.2, Fonction de signalisation d'événement de portail CMP.

Le dispositif PS DOIT mémoriser la valeur transmise dans le champ "chaddr" du message DHCP REQUEST émis par le dispositif IP de réseau local quand une location active est créée pour le dispositif IP de réseau local.

Le dispositif PS DOIT prendre en charge tous les objets de base MIB du portail CDP, y compris tous les objets contenus dans la table cabhCdpLanAddrTable, les objets cabhCdpLanPool, les objets cabhCdpServer et les objets cabhCdpLanTrans.

La fonction de serveur CDS du dispositif PS DOIT prendre en charge les options DHCP indiquées comme étant obligatoires dans la colonne "Prise en charge du protocole CDS" du Tableau 7-4, "Options DHCP du serveur CDS".

Le serveur CDS DOIT inclure, dans les messages OFFER et ACK du protocole DHCP qu'il envoie à ses clients du protocole DHCP, la sous-option 101 de l'option DHCP de code 43 contenant la chaîne "CableHome1.1LAN-Trans" (sans espaces ni guillemets) en tant qu'information de sous-option, *seulement* en réponse aux messages DISCOVER et REQUEST du protocole DHCP qui comprennent l'option DHCP de code 60 contenant la valeur de chaîne "CableHome1.1BP" (sans espaces ni guillemets).

Le serveur CDS NE DOIT PAS inclure la sous-option 101 de l'option DHCP de code 43 dans les messages OFFER et ACK du protocole DHCP qu'il envoie à tout client du protocole DHCP qui n'a pas fourni la valeur de chaîne "*CableHome1.1BP*" dans l'option DHCP de code 60 contenue dans ses messages DISCOVER et REQUEST du protocole DHCP.

La fonction de serveur CDS du dispositif PS DOIT prendre en charge la fourniture des valeurs par défaut indiquées dans la colonne "Valeurs par défaut fixées à l'usine du serveur CDS" du Tableau 7-4, "Options DHCP du serveur CDS", si l'option DHCP n'a pas été préconfigurée avec d'autres valeurs.

Si le mode primaire de traitement de paquet du dispositif PS (objet cabhCapPrimaryMode) a été réglé à "transfert" et que le processus de préconfiguration du dispositif PS soit achevé (ce qui est indiqué par l'objet cabhPsDevProvState à la valeur = pass(1)), alors la fonction de serveur CDS du dispositif PS DOIT être désactivée.

La fonction de serveur CDS du dispositif PS NE DOIT PAS répondre à des messages DHCP qui sont reçus par une quelconque interface avec un réseau régional, ni émettre de messages DHCP à partir d'une quelconque interface avec un réseau régional.

La fonction de serveur CDS du dispositif PS NE DOIT PAS livrer de quelconque option DHCP avec valeur "néant" à un quelconque dispositif IP de réseau local.

Le serveur CDS NE DOIT PAS offrir de location pour l'adresse IP 192.168.0.1, c'est-à-dire que le serveur CDS NE DOIT PAS transmettre de message OFFER ou ACK du protocole DHCP avec la valeur 192.168.0.1 dans le champ "yiaddr".

Une distinction est faite quand le dispositif PS est dans l'état de préconfiguration où l'objet cabhPsDevProvState est égal à inProgress(2). Dans cet état, quand le dispositif PS fournit une location DHCP à un ou plusieurs client(s) d'équipement CPE de réseau local, il DOIT régler

l'option 51, Durée de location d'adresse IP, à 60 au lieu de 3600 comme spécifié dans le Tableau 7-4.

Tableau 7-4/J.192 – Options DHCP du serveur CDS

Numéro d'option	Fonction de l'option	Prise en charge du protocole par le serveur CDS (M = obligatoire ou O = facultative)	Valeurs par défaut fixées à l'usine du serveur CDS	Nom de l'objet de base MIB
0	Bourrage	M	N/A	N/A
255	Fin	M	N/A	N/A
1	Masque de sous-réseau	M	255.255.255.0	cabhCdpServerSubnetMask
2	Décalage horaire	M	0	cabhCdpServerTimeOffset
3	Option de routeur	M	192.168.0.1	cabhCdpServerRouter
6	Serveur distant de noms de domaine	M	192.168.0.1	cabhCdpServerDnsAddress
7	Serveur de journalisation	M	0.0.0.0	cabhCdpServerSyslogAddress
12	Nom du serveur local	M	N/A	N/A
15	Nom de domaine	M	Chaîne vide	cabhCdpServerDomainName
23	Temps par défaut de recherche de relais	M	64	cabhCdpServerTTL
26	Unité MTU d'interface	M	N/A	cabhCdpServerInterfaceMTU
43	Informations propres au vendeur	M	Choisies par le vendeur	cabhCdpServerVendorSpecific
43.101	Informations propres au vendeur sous-option 101	M (Note)	Chaîne (sans espaces) : "CableHome 1.1 LAN-Trans"	N/A
50	Adresse IP demandée	M	N/A	N/A
51	Durée de location d'adresse IP	M	3600 secondes	cabhCdpServerLeaseTime
54	Identificateur de serveur distant	M	192.168.0.1	cabhCdpServerDhcpAddress
55	Liste de demande de paramètres	M	N/A	N/A
60	Identificateur de classe de vendeur	M	N/A	N/A
61	Identificateur de client	O	N/A	N/A
NOTE – Le serveur CDS est tenu d'inclure la sous-option 101 de l'option DHCP de code 43, contenant la chaîne "CableHome 1.1 LAN-Trans" (sans espaces) dans les messages OFFER et ACK du protocole DHCP qu'il envoie seulement aux dispositifs IP de réseau local conformes au modèle IPCable2Home, cette conformité étant indiquée par la présence de la chaîne IPCable2Home1.1BP dans les messages DISCOVER et REQUEST du protocole DHCP.				

7.3.3.2 Fonction de client du protocole DHCP (client CDC) dans le portail CDP

7.3.3.2.1 Fonction de client CDC: objectifs

Les objectifs de la fonction de client CDC du portail CDP sont les suivants:

- acquérir une location d'adresse IP pour la pile de services de portail IP utilisée pour la messagerie de gestion et le transfert de fichiers entre les serveurs du réseau du câblo-opérateur et le dispositif PS;
- acquérir des informations de configuration à partir du serveur DHCP du réseau du câblo-opérateur;
- déterminer le mode de préconfiguration dans lequel le dispositif PS doit fonctionner;
- acquérir une ou plusieurs location(s) d'adresse IP pour mappage sur des dispositifs IP de réseau local dans le secteur LAN-Trans.

7.3.3.2.2 Fonction de client CDC: directives de conception du système

Les directives énumérées dans le Tableau 7-5 ont servi à orienter la spécification de la fonction de client CDC:

Tableau 7-5/J.192 – Fonction de client IPCable2Home du protocole DHCP (client CDC) – Directives de conception du système

Numéro	Directives de conception du système de fonction de client CDC
CDC 1	Permettre au dispositif PS d'acquérir une location d'adresse réseau et des informations de configuration pour son interface avec le réseau WAN-Man.
CDC 2	Permettre au dispositif PS d'acquérir une ou plusieurs locations d'adresse réseau et des informations de configuration pour son interface avec le réseau WAN-Data.
CDC 3	Le mécanisme d'attribution de locations d'adresse IP et d'informations de configuration dans le secteur LAN-Trans n'attribuera pas de locations d'adresse IP ni ne fournira d'informations de configuration aux dispositifs IP de réseau local situés dans le secteur LAN-Pass.

7.3.3.2.3 Fonction de client CDC: description du système

Le client CDC est un client normal du protocole DHCP comme défini dans [RFC 2131] et ses responsabilités sont les suivantes:

- le client CDC envoie des demandes à des serveurs DHCP de tête de réseau pour l'acquisition d'adresses dans le réseau WAN-Man et peut envoyer des demandes à des serveurs DHCP de tête de réseau pour l'acquisition d'adresses dans les secteurs d'adresses de réseau WAN-Data. Par ailleurs, le client CDC comprend un certain nombre des paramètres de configuration DHCP et agit sur eux;
- le client CDC effectue une détermination du mode de préconfiguration dans lequel les services de portail doivent fonctionner, sur la base des informations reçues dans le message ACKNOWLEDGE du protocole DHCP envoyé par son serveur DHCP;
- le client CDC prend en charge l'acquisition d'une seule adresse IP de réseau WAN-Man et de zéro, une ou plusieurs adresses IP de réseau WAN-Data;
- le client CDC prend en charge l'option d'identificateur de classe du vendeur (option DHCP 60), l'option d'informations propres au vendeur (option DHCP 43) et l'option d'identificateur de client (option DHCP 61);

- par défaut, le client CDC acquerra une seule adresse IP pour usage simultané par les interfaces IP de réseau WAN-Man et de réseau WAN-Data. Afin de minimiser les changements à apporter aux serveurs DHCP de tête de réseau existants, l'utilisation d'un identificateur de client (option DHCP 61) par le client CDC n'est pas requise dans ce cas par défaut;
- le client CDC contenu dans un dispositif PS autonome émet une demande de renouvellement de location DHCP quand il détecte que la liaison par réseau régional entre lui-même et le câblo-modem est perdue puis rétablie. Le dispositif PS autonome peut utiliser l'événement de perte de la liaison par réseau régional entre lui-même et le câblo-modem et de récupération du synchronisme comme un signal que le câblo-modem a subi une réinitialisation. Etant donné que le câblo-modem perd, quand il est réinitialisé, toutes les informations de réexpédition d'entrée dans le protocole de résolution d'adresse (ARP, Address Resolution Protocol) pour les adresses de commande MAC du dispositif PS autonome qu'il possédait avant la réinitialisation, il est nécessaire de disposer d'un mécanisme permettant au câblo-modem de ré-acquérir toutes les adresses de commande MAC du dispositif PS autonome qui doivent recevoir des trames de l'interface radioélectrique via le câblo-modem. Le dispositif PS autonome utilisera donc ces informations de perte et de rétablissement de liaison afin de lancer un renouvellement DHCP pour toutes les locations d'adresse IP qu'il a actuellement acquises via DHCP et qui sont encore valides. Ce message de renouvellement DHCP permettra au câblo-modem d'acquérir les adresses de commande MAC du dispositif PS autonome et de rétablir la réexpédition d'adresses MAC qu'il a besoin d'exécuter pour les trames qui sont, à l'interface radioélectrique, destinées au dispositif PS autonome.

Le portail CDP prend en charge diverses options DHCP et extensions BOOTP de vendeur, autorisées par [RFC 2132].

Le client CDC détermine le mode de préconfiguration dans lequel le dispositif PS doit fonctionner sur la base des informations reçues du serveur DHCP dans le message ACK du protocole DHCP, comme présenté dans le § 5.5, "Modes de fonctionnement IPCable2Home". Le mode de préconfiguration d'un dispositif PS intégré (ePS, embedded PS) peut également être configuré par l'intermédiaire d'un câblo-modem conforme à la spécification eDOCSIS, par réglage de la valeur de l'objet de base MIB esafePsCableHomeModeControl [Rec. UIT-T J.126]. Si l'objet esafePsCableHomeModeControl est mis à provSystem(2), le dispositif ePS est tenu de lancer le processus de préconfiguration, et le client CDC détermine le mode de préconfiguration. Si l'objet esafePsCableHomeModeControl est mis à la valeur disabledMode(1) ou dormantCHMode(3), le client CDC ne participe pas à la détermination du mode de préconfiguration ou de fonctionnement.

Fonctionnement en mode de préconfiguration DHCP

Le dispositif PS fonctionne en mode de préconfiguration DHCP s'il reçoit un nom de fichier valide pour le fichier de configuration du dispositif PS dans le champ "*file*" et une adresse IP valide dans le champ "*siaddr*" du message ACK du protocole DHCP et *ne reçoit pas* les sous-options 3, 6 ou 10 de l'option DHCP 122.

Le comportement du dispositif PS lorsqu'il fonctionne en mode de préconfiguration DHCP est résumé ci-dessous:

- le dispositif PS exige qu'un fichier de configuration du dispositif PS soit téléchargé à partir d'un serveur de fichiers dans le réseau câblé;
- le dispositif PS utilise par défaut les versions SNMPv1 et SNMPv2c pour la messagerie de gestion;
- le dispositif PS utilise par défaut la table docsDevNmAccessTable de la base MIB de dispositif DOCSIS [RFC 2669] afin de contrôler l'accès à la base de données PS par des bases MIB spécifiées;

- le dispositif PS peut être configuré de façon à utiliser la fonction de sécurité de la couche Transport (TLS, *transport layer security*) [RFC 2246] afin d'authentifier et de chiffrer le fichier de configuration du dispositif PS (voir § 11.9, "Sécurité du fichier de configuration du dispositif PS en mode de préconfiguration DHCP");
- le dispositif PS peut être configuré de façon à fonctionner en mode de coexistence de la version SNMPv3, au moyen de la gestion de clé par codage Diffie-Helman [RFC 2786], (voir § 6.3.3.1.4.2.2).

Fonctionnement en mode de préconfiguration SNMP

Le dispositif PS fonctionne en mode de préconfiguration SNMP s'il reçoit l'option DHCP 122 avec les champs de sous-option 3, 6 et 10, *ne reçoit pas* de nom de fichier valide dans le champ "*file*" et *ne reçoit pas* d'adresse IP valide dans le champ "*siaddr*" du message ACK du protocole DHCP.

Le comportement du dispositif PS lorsqu'il fonctionne en mode de préconfiguration SNMP est résumé ci-dessous:

- le dispositif PS n'est pas tenu de télécharger un fichier de configuration du dispositif PS à partir du serveur de fichiers dans le réseau câblé. Le dispositif PS peut être déclenché afin de télécharger un fichier de configuration du dispositif PS à tout instant mais il fonctionnera au moyen des paramètres par défaut fixées à l'usine sans téléchargement d'un fichier de configuration PS;
- un temporisateur configurable (cabhPsDevPreconfigurationTimer) commande la durée pendant laquelle le dispositif PS attendra d'être déclenché afin d'importer par téléchargement un fichier de configuration PS après avoir terminé l'authentification avec le centre KDC et avoir émis un message INFORM d'enrôlement de préconfiguration SNMP. La valeur de l'objet cabhPsDevProvState passera de inProgress(2) à pass(1) après que la durée spécifiée par la valeur de l'objet cabhPsDevPreconfigurationTimer s'est écoulée, si le dispositif PS n'est pas déclenché afin d'importer par téléchargement un fichier de configuration. Si le dispositif PS est déclenché par le gestionnaire SNMP de façon à importer par téléchargement un fichier de configuration PS avant que la durée spécifiée par le temporisateur de préconfiguration se soit écoulée, la valeur de l'objet cabhPsDevProvState ne passera pas à pass(1) avant que le dispositif PS n'ait correctement importé par téléchargement et terminé le traitement du fichier de configuration PS.
- le dispositif PS utilise par défaut la prise en charge *non* activée du mode de coexistence de la version SNMPv3 avec les versions SNMPv1 et SNMPv2 (voir § 11.4, Messagerie de gestion sécurisée envoyée au dispositif PS);
- le dispositif PS utilise par défaut le modèle de sécurité fondé sur l'utilisateur du protocole SNMPv3 [RFC 3414] et le modèle de contrôle d'accès fondé sur le point de vue du protocole SNMPv3 [RFC 3415] afin de contrôler l'accès à la base de données PS par bases MIB spécifiées (voir § 11.4);
- le dispositif PS fait appel à l'échange de messages par serveur Kerberos avec un serveur de centre de distribution de clés (KDC, *key distribution centre*) dont l'adresse IP est fournie aux services de portail dans la sous-option 51 de l'option DHCP 177 et utilise un détecteur de processus AP afin d'authentifier les messages SNMPv3 (voir § 11.4.4.2, Algorithmes de sécurité pour le protocole SNMPv3 en mode de préconfiguration SNMP);
- le dispositif PS peut être configuré de façon à recevoir et à traiter les messages SNMPv1 et SNMPv2c ainsi que les messages SNMPv3.

Mode IPCable2Home inactif

Le dispositif PS fonctionne en mode IPCable2Home inactif s'il ne reçoit ni la combinaison du champ "*file*", du champ "*siaddr*" ou des sous-options de l'option DHCP de code 122 afin de le configurer en mode de préconfiguration DHCP, ni la combinaison de ces champs et sous-options

afin de le configurer en mode de préconfiguration SNMP. Un dispositif PS intégré peut également être configuré de façon à fonctionner en mode CableHome inactif par l'intermédiaire de la base MIB du câblo-modem intégré conforme à la spécification eDOCSIS [Rec. UIT-T J.126]. Si la valeur de l'objet esafePsCableHomeModeControl de la base MIB eSAFE conforme à eDOCSIS est: dormantCHMode(3), le dispositif PS intégré est tenu de fonctionner en mode CableHome inactif, quelles que soient les valeurs des champs DHCP "file" et "siaddr" ou de l'option DHCP 122 contenus dans les messages DHCP reçus du serveur DHCP du câblo-opérateur.

Quand le dispositif PS doit fonctionner en mode IPCable2Home inactif, son comportement est tenu d'être comme décrit dans le § 7.3.3.2.4, y compris ce qui suit. Ce mode de fonctionnement est conçu afin de permettre au dispositif PS de fonctionner et d'exécuter des fonctions de passerelle résidentielle quand il est connecté à un réseau de données par câble qui ne prend pas encore en charge les systèmes de préconfiguration et de gestion IPCable2Home:

- ignorer tout message SNMP reçu par une quelconque interface avec un réseau régional;
- désactiver la fonction de client TFTP;
- désactiver la signalisation des événements par serveur SYSLOG;
- fermer le temporisateur de préconfiguration;
- activer les fonctionnalités CNP, CAP, USFS et CDS.

Le dispositif PS est tenu d'inclure certains champs d'option DHCP dans les messages DISCOVER et REQUEST du protocole DHCP qu'il envoie à des serveurs DHCP du réseau câblé. L'option d'identificateur de classe du vendeur (option DHCP 60) définit une classe de dispositif CableLabs. Dans la présente Recommandation, l'option d'identificateur de classe du vendeur contiendra la chaîne "CableHome1.1" afin d'identifier un élément logique de services de portail (PS) conforme, chaque fois que le client CDC demandera une adresse de secteur WAN-Man ou WAN-Data.

L'option d'informations propres au vendeur (option DHCP 43) identifie également le type de dispositif et ses capacités. Elle décrit le type de composant qui formule la requête (intégré ou autonome, CM ou PS), les composants qui sont contenus dans le dispositif (CM, MTA, PS, etc.) et le numéro de série du dispositif. Elle permet également d'indiquer des paramètres propres au dispositif. L'option 43 du protocole DHCP et ses sous-options sont définies dans le § 7.3.3.2.4.

Les détails des exigences relatives à la prise en charge des options DHCP 60 et 43 sont reproduits dans les Tableaux 7-6 et 7-7. Des détails relatifs à d'autres options DHCP facultatives et obligatoires sont présentés dans le Tableau 7-8.

Le paramètre de décompte d'adresses IP de réseau WAN-Data de la base MIB du portail CDP (objet cabhCdpWanDataIpAddrCount) est le nombre de locations d'adresse IP que le client CDC est tenu d'essayer d'acquérir pour le côté réseau régional des mappages de conversion NAT et NAPT. La valeur par défaut de l'objet cabhCdpWanDataIpAddrCount est zéro, ce qui signifie que, par défaut, le client CDC va acquérir seulement une adresse IP de réseau WAN-Man.

7.3.3.2.3.1 Option 61 du client DHCP intégré

L'élément de services de portail peut avoir une ou plusieurs adresses IP de réseau régional associées à une ou à plusieurs interfaces de couche Liaison de données (p. ex. MAC). Le client CDC ne peut donc pas se reposer seulement sur une adresse de commande MAC comme unique valeur d'identificateur de client.

La présente Recommandation permet l'utilisation de l'option d'identificateur de client (option DHCP 61), [RFC 2132] section 9.14, afin d'identifier de façon univoque l'interface logique de réseau régional qui est associée à une adresse IP particulière.

Le dispositif PS est tenu d'avoir deux adresses de matériel: l'une servant à identifier de façon univoque l'interface logique avec un réseau régional qui est associée à l'adresse IP de réseau WAN-Man (adresse matérielle de réseau WAN-Man) et l'autre servant à identifier de façon

univoque l'interface logique avec un réseau régional qui est associée à des adresses IP de réseau WAN-Data (adresse matérielle de réseau WAN-Data).

7.3.3.2.3.2 Modes des adresses de réseau régional

Afin d'activer la compatibilité avec autant de systèmes de préconfiguration de câblo-opérateur que possible, le client CDC prendra en charge les modes configurables suivants des adresses de réseau régional.

Mode 0 d'adresse WAN

L'élément de services de portail utilise une seule adresse IP de réseau régional, acquise par protocole DHCP au moyen de l'adresse matérielle du réseau WAN-Man. L'élément de services de portail a une seule interface IP WAN-Man et zéro interface IP WAN-Data. Ce mode d'adressage n'est applicable que quand le mode primaire de traitement de paquet du dispositif PS (objet cabhCapPrimaryMode) est réglé à "Transfert" (voir § 8.3.2). Le serveur DHCP de la tête de réseau du câblo-opérateur n'a normalement besoin d'aucune modification logicielle afin de prendre en charge ce mode d'adressage. En mode 0 d'adresse de réseau régional, la valeur de l'objet cabhCdpWanDataIpAddrCount est zéro.

Mode 1 d'adresse de réseau régional

L'élément de services de portail utilise une seule adresse IP de réseau régional, acquise par protocole DHCP au moyen de l'adresse matérielle de réseau WAN-Man. L'élément de services de portail a une seule interface IP WAN-Man et une seule interface IP WAN-Data. Ces deux interfaces se partagent une adresse IP commune. Ce mode d'adressage n'est applicable que quand le mode primaire de traitement de paquet du dispositif PS (objet cabhCapPrimaryMode) est réglé à "conversion NAPT". Le serveur DHCP de la tête de réseau du câblo-opérateur n'a normalement besoin d'aucune modification logicielle afin de prendre en charge ce mode d'adressage. En mode 1 d'adresse de réseau régional, la valeur de l'objet cabhCdpWanDataIpAddrCount est zéro.

Mode 2 d'adresse de réseau régional

L'élément de services de portail acquiert une adresse IP de réseau WAN-Man au moyen de l'unique adresse matérielle de réseau WAN-Man. Il est ensuite configuré par le système NMS de façon à demander une ou plusieurs adresse(s) IP unique(s) de réseau WAN-Data. L'élément de services de portail possédera une seule interface IP WAN-Man et une ou plusieurs interface(s) IP WAN-Data. Toutes les adresses IP de réseau WAN-Data se partageront une adresse matérielle commune qui sera unique par rapport à l'adresse matérielle du réseau WAN-Man. Les (au moins deux) interfaces (une interface WAN-Man et une ou plusieurs interface(s) WAN-Data) possèdent chacune leur propre adresse IP non partagée. Le portail CDP est configuré par le câblo-opérateur de façon à fonctionner en mode 2 d'adresse de réseau régional par écriture d'une valeur différente de zéro dans l'objet cabhCdpWanDataIpAddrCount, au moyen du fichier de configuration du dispositif PS ou d'une requête SNMP de mise à jour (SET). Ce mode d'adressage est applicable quand le mode primaire de traitement de paquet du dispositif PS (objet cabhCapPrimaryMode) est réglé à NAPT ou NAT. Le serveur DHCP de la tête de réseau du câblo-opérateur peut avoir besoin d'une modification logicielle afin de prendre en charge les identificateurs de client (option DHCP 61) de façon qu'il puisse attribuer de multiples adresses IP à l'adresse matérielle unique du réseau WAN-Data.

Il y a quatre scénarios possibles pour les adresses IP de réseau WAN-Data:

1) le dispositif PS est configuré de façon à demander zéro adresse IP de réseau WAN-Data. Aucun identificateur de client du réseau WAN-Data n'est nécessaire;

2) le dispositif PS est configuré de façon à demander une ou plusieurs adresses IP de réseau WAN-Data et il n'y a aucune entrée d'objet cabhCdpWanDataAddrClientId, configurée par opérateur, dans la base MIB du portail CDP. Le dispositif PS est tenu de produire automatiquement autant d'identificateurs uniques de client du réseau WAN-Data qu'indiqué par la valeur de l'objet cabhCdpWanDataIpAddrCount;

3) le dispositif PS est configuré de façon à demander une ou plusieurs adresses IP de réseau WAN-Data et il y a au moins autant d'entrées configurées par opérateur dans l'objet cabhCdpWanDataAddrClientId qu'indiqué par la valeur de l'objet cabhCdpWanDataIpAddrCount, c'est-à-dire que l'opérateur a préconfiguré assez de valeurs d'identificateur de client de réseau WAN-Data. Le dispositif PS ne produit automatiquement aucun identificateur de client;

4) le dispositif PS est configuré de façon à demander une ou plusieurs adresses IP de réseau WAN-Data et il y a moins d'entrées configurées par opérateur dans l'objet cabhCdpWanDataAddrClientId qu'indiqué par la valeur de l'objet cabhCdpWanDataIpAddrCount, c'est-à-dire que l'opérateur a préconfiguré un certain nombre, mais insuffisant, de valeurs d'identificateur de client de réseau WAN-Data. Le dispositif PS est tenu de produire automatiquement assez d'identificateurs uniques de client du réseau WAN-Data supplémentaires pour rendre le nombre total d'identificateurs uniques de client du réseau WAN-Data égal à la valeur de l'objet cabhCdpWanDataIpAddrCount.

Si le câblo-opérateur souhaite que le dispositif PS obtienne une ou plusieurs adresses IP de réseau WAN-Data qui soient distinctes de l'adresse IP du réseau WAN-Man, la procédure est la suivante.

Dans tous les modes d'adressage de réseau régional, le dispositif PS demande d'abord une adresse IP de réseau WAN-Man au moyen de l'adresse matérielle de ce réseau.

La procédure décrite ci-dessous implique que le dispositif PS a déjà acquis une adresse IP de réseau WAN-Man:

1) le câblo-opérateur préconfigure facultativement le dispositif PS avec des identificateurs de client uniques et spécifiques, par écriture de valeurs d'entrées de l'objet cabhCdpWanDataAddrClientId dans la table cabhCdpWanDataAddrTable de la base MIB du portail CDP, au moyen du fichier de configuration du dispositif PS ou de message(s) SNMP de requête de mise à jour (SET);

2) le câblo-opérateur configure le portail CDP de façon à fonctionner en mode 2 d'adresse de réseau régional par écriture, dans l'objet cabhCdpWanDataIpAddrCount, d'une valeur différente de zéro au moyen du fichier de configuration du dispositif PS ou du message SNMP de demande de mise à jour (set);

3) après que le portail CDP a été configuré de façon à fonctionner en mode 2 d'adresse de réseau régional comme décrit au cours de l'étape 2, le dispositif PS vérifie si des valeurs d'identificateur de client ont été préconfigurées par le système NMS comme décrit au cours de l'étape 1. Si un nombre de valeurs d'identificateur de client supérieur ou égal à la valeur de l'objet cabhCdpWanDataIpAddrCount a été préconfiguré, le dispositif PS fait appel à ces valeurs dans l'option DHCP 61 lorsqu'il formule une demande d'adresse(s) IP de réseau WAN-Data. Si des valeurs d'identificateur de client n'ont pas été préconfigurées, c'est-à-dire si les entrées de l'objet cabhCdpWanDataAddrClientId n'existent pas ou si le nombre de valeurs d'identificateur de client préconfigurées est inférieur à la valeur de l'objet cabhCdpWanDataIpAddrCount, le dispositif PS produit un certain nombre de valeurs uniques d'identificateur de client de telle sorte que, en combinaison avec les identificateurs de client préconfigurés, le nombre total d'identificateurs uniques de client a une valeur égale la valeur de l'objet cabhCdpWanDataIpAddrCount. Le dispositif PS produit des valeurs d'identificateur de client au moyen de la seule adresse matérielle de réseau WAN-Data pour la première adresse IP demandée de réseau WAN-Data et par concaténation de l'adresse matérielle de réseau WAN-Data avec un champ de comptage de

8 bits de longueur pour la deuxième adresse IP de réseau WAN-Data et pour toutes les suivantes. Si aucun identificateur de client n'a été préconfiguré par le système NMS, la première valeur du champ de comptage de 8 bits est 0x02 (indiquant la deuxième adresse IP de réseau WAN-Data demandée), la deuxième valeur du champ de comptage est 0x03 et ainsi de suite.

Exemple si aucun identificateur de client n'a été préconfiguré par le système NMS:

adresse matérielle indiquée pour le réseau WAN-Data: 0xCDCDCDCDCDCD

identificateur de client produit par le dispositif PS pour la première adresse IP demandée de réseau WAN-Data: 0xCDCDCDCDCDCD

identificateur de client produit par le dispositif PS pour la deuxième adresse IP demandée de réseau WAN-Data: 0xCDCDCDCDCDCD02

identificateur de client produit par le dispositif PS pour la troisième adresse IP demandée de réseau WAN-Data: 0xCDCDCDCDCDCD03

identificateur de client produit par le dispositif PS pour la nième adresse IP demandée de réseau WAN-Data: 0xCDCDCDCDCDCDn ($n \leq 0xFF$).

Si certains identificateurs de client ont été préconfigurés par le système NMS mais que leur nombre soit inférieur à la valeur de l'objet cabhCdpWanDataIpAddrCount, le dispositif PS produit autant d'identificateurs de client que nécessaire pour rendre le nombre total d'identificateurs de client égal à la valeur de l'objet cabhCdpWanDataIpAddrCount. Le dispositif PS produira ces valeurs additionnelles d'identificateurs de client en adjoignant une valeur de comptage sur 8 bits à l'adresse matérielle de réseau WAN-Data, à partir de 0x02, à moins que cette valeur ne fasse double emploi avec un identificateur de client préconfiguré. Si les identificateurs de client préconfigurés par le système NMS suivent le même format (adresse matérielle avec valeur de comptage sur 8 bits), le dispositif PS est tenu d'utiliser une unique valeur de comptage de façon à ne pas faire double emploi avec un identificateur de client préconfiguré.

Exemple dans le cas où des identificateurs de client ont été préconfigurés par le système NMS (trois valeurs d'identificateur de client préconfigurées, objet cabhCdpWanDataIpAddrCount à la valeur = 5):

adresse matérielle indiquée de réseau WAN-Data: 0xCDCDCDCDCDCD

premier identificateur de client préconfiguré pour la première adresse IP de réseau WAN-Data: 0x0A0A0A0A0A1A

deuxième identificateur de client préconfiguré pour la deuxième adresse IP de réseau WAN-Data: 0x0A0A0A0A0A2A

troisième identificateur de client préconfiguré pour la troisième adresse IP de réseau WAN-Data: 0x0A0A0A0A0A3A

premier identificateur de client produit par le dispositif PS pour la quatrième adresse IP demandée de réseau WAN-Data: 0xCDCDCDCDCDCD02

deuxième identificateur de client produit par le dispositif PS pour la cinquième adresse IP demandée de réseau WAN-Data: 0xCDCDCDCDCDCD03

4) le dispositif PS ajoute les valeurs d'identificateur de client qu'il produit en tant qu'entrées de l'objet cabhCdpWanDataAddrClientId jusqu'à la fin de la table cabhCdpWanDataAddrTable;

5) le dispositif PS (client CDC) demande (en répétant le processus de découverte du protocole DHCP selon les besoins) autant d'adresses IP uniques de réseau WAN-Data que spécifié par la valeur de l'objet cabhCdpWanDataIpAddrCount, au moyen de l'adresse matérielle de réseau WAN-Data contenue dans le champ "chaddr" du message DHCP et au moyen de la ou des valeurs d'identificateur de client extraites de l'étape 3 dans l'option

DHCP 61, en commençant par la première entrée d'objet cabhCdpWanDataAddrClientId dans la table cabhCdpWanDataAddrTable. Le client CDC n'est pas autorisé à demander plus d'adresses IP de réseau WAN-Data que la valeur de l'objet cabhCdpWanDataIpAddrCount, même si le nombre d'identificateurs de client préconfigurés est supérieur à la valeur de la table cabhCdpWanDataAddrTable.

7.3.3.2.4 Exigences relatives au client CDC

Le dispositif PS DOIT implémenter une fonction de client du protocole DHCP conformément aux exigences relatives aux clients figurant dans [RFC 2131].

Dans les deux configurations du dispositif PS (intégré et autonome), le dispositif PS DOIT implémenter deux adresses uniques de matériel d'interface avec un réseau régional: l'adresse matérielle de l'interface PS WAN-Man et l'adresse matérielle de l'interface PS WAN-Data. La valeur numérique de l'adresse matérielle de l'interface PS WAN-Data DOIT suivre séquentiellement la valeur numérique de l'adresse matérielle de l'interface PS WAN-Man. Les adresses matérielles des interfaces PS WAN-Man et PS WAN-Data DOIVENT persister une fois qu'elles ont été réglées en usine. Le dispositif PS NE DOIT PAS permettre la modification de ses adresses matérielles d'interface PS WAN-Man et PS WAN-Data réglées en usine.

Dans les deux configurations du dispositif PS (intégré et autonome), l'élément de services de portail DOIT avoir des adresses matérielles d'interface avec un réseau régional qui soient distinctes de l'adresse matérielle du câblo-modem.

Le dispositif PS DOIT diffuser le message DHCP DISCOVER conformément aux exigences relatives au client figurant dans [RFC 2131] et essayer d'acquérir une location d'adresse IP de l'interface PS WAN-Man pendant le processus d'amorçage du dispositif PS.

Le dispositif PS DOIT régler l'objet cabhPsDevProvState à la valeur inProgress (2) quand le dispositif PS diffuse le message DHCP DISCOVER pour la première fois après un réamorçage ou une réinitialisation du dispositif PS. Celui-ci ignore les champs et options d'en-tête DHCP qui ont servi à déterminer le mode de préconfiguration et n'est pas tenu de régler l'objet cabhPsDevProvState à la valeur inProgress (2) quand il renouvelle sa location d'adresse IP par protocole DHCP.

A la suite du processus de renouvellement de sa location d'adresse IP, le dispositif PS met l'objet d'état de préconfiguration (cabhPsDevProvState) à la valeur pass(1) ou à la valeur fail(2). Quand il renouvelle sa ou ses locations d'adresse IP de réseau WAN-Man ou WAN-Data, le dispositif PS DOIT mettre à jour son horloge système et les objets associés de base MIB (cabhPsDevDateTime) sur la base de la valeur de l'option 2 du DHCP (décalage horaire) dans le message ACK du DHCP si la valeur de l'objet cabhCdpTimeOffsetSelection est useDhcpOption2(1), OU sur la base de la valeur de l'objet cabhCdpSnmpSetTimeOffset si la valeur de l'objet cabhCdpTimeOffsetSelection est useSnmpSetOffset(2), et avec le réglage d'une heure d'été dans la période correspondante si la valeur de l'objet cabhCdpDaylightSavingTimeEnable est enabled(1). Quand il renouvelle sa ou ses locations d'adresse IP de réseau WAN-Man ou WAN-Data, le dispositif PS DOIT mettre à jour ses informations de location, y compris la mise à jour des valeurs des objets cabhCdpWanDataAddrLeaseCreateTime et cabhCdpWanDataAddrLeaseExpireTime selon le cas, sur la base de la valeur de l'option DHCP 51 (Durée de location d'adresse IP). Quand il renouvelle sa ou ses locations d'adresse IP de résesau WAN-Man ou WAN-Data, le dispositif PS DOIT ignorer les sous-options 3, 6 et 10 de l'option DHCP 122, ainsi que les champs "file" et "siaddr" de l'en-tête DHCP.

Le dispositif PS DOIT utiliser l'adresse matérielle de l'interface PS WAN-Man indiquée dans le champ *"chaddr"* et dans l'option DHCP 61 des messages DISCOVER et REQUEST du protocole DHCP, lorsqu'il demande une adresse IP de réseau WAN-Man à partir du serveur DHCP de tête de réseau.

Si la valeur de l'objet cabhCdpWanDataIpAddrCount est zéro, le dispositif PS DOIT utiliser l'adresse IP du réseau WAN-Man pour les interfaces PS WAN-Man et PS WAN-Data.

Si la valeur de l'objet cabhCdpWanDataIpAddrCount est supérieure à zéro, le dispositif PS DOIT demander, à partir du serveur DHCP de la tête de réseau, le nombre d'adresse(s) IP unique(s) de réseau WAN-Data qui est indiqué par la valeur de l'objet cabhCdpWanDataIpAddrCount.

Le dispositif PS (client CDC) NE DOIT PAS essayer d'acquérir plus d'adresses IP de réseau WAN-Data qu'indiqué par la valeur de l'objet cabhCdpWanDataIpAddrCount.

Le dispositif PS DOIT utiliser un unique identificateur cabhCdpWanDataAddrClientId dans l'option DHCP 61 pour chaque adresse IP de réseau WAN-Data demandée à partir du serveur DHCP de tête de réseau.

Le dispositif PS DOIT utiliser l'adresse matérielle de réseau WAN-Data comme valeur contenue dans le champ *"chaddr"* du message DHCP pour chaque adresse IP de réseau WAN-Data demandée au serveur DHCP de tête de réseau.

Le dispositif PS autonome DOIT lancer un renouvellement DHCP pour toutes les locations d'adresse IP qu'il a actuellement acquises via DHCP et qui sont encore valides, chaque fois qu'il apprend qu'il y a eu une perte, suivie d'un rétablissement, de la liaison par réseau régional entre le dispositif PS autonome et le câblo-modem. Ce message de renouvellement DHCP permettra au câblo-modem d'acquérir les adresses de commande MAC du dispositif PS autonome et de rétablir la réexpédition des informations de commande MAC dont il a besoin afin d'exécuter les trames de l'interface radioélectrique qui sont destinées au dispositif PS autonome.

L'on part du principe que, dans le cas de la plupart des dispositifs PS intégrés, quand le câblo-modem subit une réinitialisation, le dispositif PS intégré subit également une réinitialisation de façon à éviter tout état d'incohérence entre les deux dispositifs. Le dispositif PS autonome DOIT lancer un renouvellement DHCP pour toutes les locations d'adresse IP qu'il a actuellement acquises via DHCP et qui sont encore valides, chaque fois qu'il apprend qu'il y a eu une perte de liaison suivie d'un rétablissement de la liaison par réseau régional entre le dispositif PS autonome et le câblo-modem.

Quand le dispositif PS (client CDC) demande des adresses IP de réseau WAN-Data au serveur DHCP de tête de réseau, le dispositif PS DOIT utiliser les entrées d'identificateur cabhCdpWanDataAddrClientId pour l'option DHCP 61 dans l'ordre d'apparition de ces entrées dans la table cabhCdpWanDataAddrTable, en commençant par la première entrée.

Si une valeur différente de zéro est configurée pour l'objet cabhCdpWanDataIpAddrCount et si le nombre d'entrées de l'objet cabhCdpWanDataAddrClientId est inférieur à la valeur de l'objet cabhCdpWanDataIpAddrCount, le dispositif PS DOIT produire autant d'identificateurs uniques de client du réseau WAN-Data que nécessaire pour rendre le nombre total d'entrées de l'objet cabhCdpWanDataAddrClientId égal à la valeur de l'objet cabhCdpWanDataIpAddrCount et le dispositif PS DOIT ajouter chaque entrée ainsi produite à la fin de la table cabhCdpWanDataAddrTable.

Si le dispositif PS produit des identificateurs de client du réseau WAN-Data, la première entrée d'identificateur cabhCdpWanDataAddrClientId contenue dans la table cabhCdpWanDataAddrTable DOIT être l'adresse matérielle du réseau WAN-Data.

Si le dispositif PS produit des identificateurs de client du réseau WAN-Data, toute entrée d'identificateur cabhCdpWanDataAddrClientId produite par le dispositif PS, autre que la première entrée de la table cabhCdpWanDataAddrTable DOIT être l'adresse matérielle du réseau WAN-Data assortie d'une valeur finale de comptage sur 8 bits commençant par 0x02, à moins que cette valeur n'existe déjà en tant qu'entrée d'identificateur cabhCdpWanDataAddrClientId, auquel cas le dispositif PS DOIT produire l'identificateur de client sous la forme de l'adresse matérielle du réseau WAN-Data assortie de la prochaine valeur disponible de comptage sur 8 bits.

Le dispositif PS DOIT implémenter l'option d'informations propres au vendeur (option DHCP 43) comme spécifié dans les Tableaux 7-7 et 7-8. Les détails de l'option DHCP 43 et de ses sous-options sont encore définis ci-dessous. Les définitions des sous-options de l'option DHCP 43 DOIVENT être conformes aux exigences imposées par [RFC 2132].

L'option commence par un octet de type ayant la valeur du nombre 43, suivi par un octet de longueur. L'octet de longueur est suivi par le nombre d'octets de données égale à la valeur de l'octet de longueur. La valeur de l'octet de longueur n'inclut pas les deux octets spécifiant le balisage et la longueur.

L'option DHCP 43 est une option composite. Le contenu de l'option 43 se compose d'une ou de plusieurs sous-options. Les sous-options de l'option DHCP 43 prises en charge sont les suivantes: 1, 2, 3, 4, 5, 6, 11, 12, 13, et 14. Une sous-option commence par un octet de balisage contenant le code de sous-option, suivi d'un octet de longueur qui indique le nombre total d'octets de données. La valeur de l'octet de longueur n'inclut pas lui-même ou l'octet de balisage. L'octet de longueur est suivi par des octets de "longueur" des données de sous-option.

Le codage de chacune des sous-options de l'option 43 est défini ci-dessous. Voir les Tableaux 7-7 et 7-8 pour la fonction prévue de chaque sous-option.

Le dispositif PS DOIT coder l'option DHCP 43 dans sa sous-option 1 par le nombre d'octets égal à la valeur de l'octet de longueur de cette sous-option, avec chaque octet codant une sous-option requise.

Le dispositif PS DOIT coder chacune des sous-options 2, 3, 4, 5, 6, 12, 13 et 14 de l'option DHCP 43 comme une chaîne de caractères composée de caractères from le jeu de caractères ASCII de terminal virtuel de réseau (NVT, *network virtual terminal*), sans caractère NULL final.

Un dispositif PS autonome DOIT envoyer la sous-option de l'option 43 du DHCP 2 contenant la chaîne de caractères "SPS" (sans les guillemets).

Un dispositif PS intégré DOIT envoyer la sous-option de l'option 43 du DHCP 2 contenant la chaîne de caractères "EPS" (sans les guillemets).

Un dispositif PS autonome DOIT envoyer la sous-option de l'option 43 du DHCP 3 contenant la chaîne de caractères "SPS" (sans les guillemets).

Un dispositif PS intégré DOIT envoyer la sous-option de l'option 43 du DHCP 3 contenant une liste, à séparation par des caractères de deux-points, de tous les types de dispositif contenus dans le dispositif complet, comprenant au minimum la chaîne de caractères séparés par un deux-points "ECM:EPS" (sans les guillemets).

Si le dispositif PS est en train de demander une location d'adresse IP de réseau WAN-Man de dispositif PS, il DOIT envoyer la sous-option 11 de l'option 43 du DHCP contenant la valeur 0x01 codée comme un nombre binaire, dans ses messages DISCOVER et REQUEST du protocole DHCP.

Si le dispositif PS est en train de demander une location d'adresse IP de réseau WAN-Data de dispositif PS, il DOIT envoyer la sous-option 11 de l'option 43 du DHCP, contenant la valeur 0x02 codée comme un nombre binaire, dans ses messages DISCOVER et REQUEST du protocole DHCP.

Le Tableau 7-6 résume la façon dont le dispositif PS est tenu de régler les valeurs de la sous-option 11 de l'option DHCP 43 pour ses interfaces avec le réseau régional.

Tableau 7-6/J.192 – Valeurs de la sous-option 11 de l'option 43 du protocole DHCP

Identificateur d'élément	Description et commentaires
PS WAN-Man = 0x01	Identifie la demande d'adresse de secteur WAN-Man.
PS WAN-Data = 0x02	Identifie la demande d'adresse de secteur WAN-Data

La limite de longueur de chacune des sous-options 4, 5, 6, 12, 13 et 14 est de 255 octets. Ainsi la longueur totale de l'option 43 pourrait dépasser 255 octets. Si le nombre total d'octets contenus dans toutes les sous-options de l'option 43 du DHCP, dépasse 255 octets, le dispositif PS DOIT suivre le document RFC 3396 afin de subdiviser l'option en multiples options plus petites.

Le dispositif PS DOIT implémenter l'option d'identificateur de classe de vendeur (option DHCP 60) comme spécifié dans les Tableaux 7-7 et 7-8.

Dans le cas d'un dispositif PS intégré avec un câblo-modem, celui-ci et l'élément de services de portail envoient chacun des demandes DHCP distinctes. Le Tableau 7-7 décrit comment le dispositif PS DOIT régler le contenu des options 60 et 43 pour le dispositif PS quand l'élément de services de portail est intégré avec un câblo-modem et que des adresses de secteurs PS WAN-Man et PS WAN-Data distinctes sont demandées.

Tableau 7-7/J.192 – Options DHCP des demandes d'adresse WAN-Man et WAN-Data dans le cas d'un dispositif PS intégré

Options de demande DHCP	Valeur	Description
Demande DHCP d'adresse de réseau WAN-Man pour services de portail intégrés		
Option d'équipement CPE 60	"CableHome1.1"	
Option d'équipement CPE 43, sous-option 1	Demander un vecteur de sous-option	Liste des sous-options (dans l'option 43) à renvoyer par le serveur. Aucune n'est définie.
Option d'équipement CPE 43, sous-option 2	"EPS"	Dispositif PS intégré
Option d'équipement CPE 43, sous-option 3	"ECM:EPS"	Liste des dispositifs intégrés (CM intégré et PS intégré)
Option d'équipement CPE 43, sous-option 4	p. ex."123456"	Numéro de série du CM/PS
Option d'équipement CPE 43, sous-option 5	p. ex. "v3.2.1"	Numéro de version matérielle du dispositif CM/PS
Option d'équipement CPE 43, sous-option 6	p. ex. "1.0.2"	Numéro de version logicielle du dispositif CM/PS
Option d'équipement CPE 43, sous-option 11	Secteur PS WAN-Man (0x01)	Définit qu'une adresse est actuellement demandée dans le secteur PS WAN-Man
Option d'équipement CPE 43, sous-option 12	p. ex. "ABC Inc. CM-PS123..."	Description du système CM/PS à partir de l'objet sysDescr
Option d'équipement CPE 43, sous-option 13	p. ex. "CM-PS123-1.0.2...."	Révision de la micrologique du système CM/PS à partir de l'objet docsDevSwCurrentVers
Option d'équipement CPE 43, sous-option 14	p. ex. "1.2.3..."	Version du fichier de politique de pare-feu à partir de l'objet cabhSec2FirewallPolicyCurrent Version

Tableau 7-7/J.192 – Options DHCP des demandes d'adresse WAN-Man et WAN-Data dans le cas d'un dispositif PS intégré

Options de demande DHCP	Valeur	Description
Demande DHCP d'adresse de réseau WAN-Data pour services de portail intégrés		
Option d'équipement CPE 60,	"CableHome1.1"	
Option d'équipement CPE 43, sous-option 1	Demander un vecteur de sous-option	Liste des sous-options (dans l'option 43) à renvoyer par le serveur. Aucune n'est définie.
Option d'équipement CPE 43, sous-option 2	"EPS"	Dispositif PS intégré
Option d'équipement CPE 43, sous-option 3	"ECM:EPS"	Liste des dispositifs intégrés (CM intégré et PS intégré)
Option d'équipement CPE 43, sous-option 4	p. ex."123456"	Numéro de série du CM/PS
Option d'équipement CPE 43, sous-option 11	Secteur PS WAN-Data (0x02)	Définit qu'une adresse est actuellement demandée dans le secteur PS WAN-Data

Le Tableau 7-8 décrit le réglage que le dispositif PS DOIT effectuer dans le contenu des options 60 et 43, quand le dispositif PS est autonome.

Tableau 7-8/J.192 – Options DHCP des demandes d'adresse WAN-Man et WAN-Data dans le cas d'un dispositif PS autonome

Options de demande DHCP	Valeur	Description
Demande DHCP d'adresse de réseau WAN-Man pour dispositif PS autonome		
Option d'équipement CPE 60	"CableHome1.1"	
Option d'équipement CPE 43, sous-option 1	Demander un vecteur de sous-option	Liste des sous-options (dans l'option 43) à renvoyer par le serveur. Aucune n'est définie.
Option d'équipement CPE 43, sous-option 2	"SPS"	Dispositif PS autonome
Option d'équipement CPE 43, sous-option 3	"SPS"	Liste des dispositifs intégrés (dispositif PS autonome seulement)
Option d'équipement CPE 43, sous-option 4	p. ex. "123456"	Numéro de série du dispositif
Option d'équipement CPE 43, sous-option 5	p. ex. "v3.2.1"	Numéro de version matérielle du système CM/PS
Option d'équipement CPE 43, sous-option 6	p. ex. "1.0.2"	Numéro de version logicielle du système CM/PS
Option d'équipement CPE 43, sous-option 11	Secteur PS WAN-Man (0x01)	Définit qu'une adresse est actuellement demandée dans le secteur PS WAN-Man
Option d'équipement CPE 43, sous-option 12	p. ex. "ABC Inc. CM-PS123..."	Description du système CM/PS à partir de l'objet sysDescr

Tableau 7-8/J.192 – Options DHCP des demandes d'adresse WAN-Man et WAN-Data dans le cas d'un dispositif PS autonome

Options de demande DHCP	Valeur	Description
Option d'équipement CPE 43, sous-option 13	p. ex. "CM-PS123-1.0.2..."	Révision de la micrologique de CM/PS à partir de l'objet docsDevSwCurrentVers
Option d'équipement CPE 43, sous-option 14	p. ex. "1.2.3..."	Version du fichier de politique de pare-feu à partir de l'objet cabhSec2FirewallPolicyCurrentVersion
Demande DHCP d'adresse de réseau WAN-Data pour dispositif PS autonome		
Option d'équipement CPE 60	"CableHome1.1"	
Option d'équipement CPE 43, sous-option 1	Demander un vecteur de sous-option	Liste des sous-options (dans l'option 43) à renvoyer par le serveur. Aucune n'est définie.
Option d'équipement CPE 43, sous-option 2	"SPS"	Dispositif PS autonome
Option d'équipement CPE 43, sous-option 3	"SPS"	Liste des dispositifs intégrés (dispositif PS autonome seulement)
Option d'équipement CPE 43, sous-option 4	p. ex. "123456"	Numéro de série du dispositif
Option d'équipement CPE 43, sous-option 11	Secteur PS WAN-Data (0x02)	Définit qu'une adresse est actuellement demandée dans le secteur PS WAN-Data

Une description détaillée du contenu de l'objet sysDescr des services de portail figure dans le § 6.3.3.1.4, "Exigences relatives à la fonction d'agent SNMP".

Le dispositif PS DOIT prendre en charge les options DHCP indiquées comme étant obligatoires dans la colonne *Prise en charge du protocole par le client CDC* du Tableau 7-9 ci-après, qui énumère les options DHCP dont la prise en charge par le client CDC est obligatoire ou facultative.

Tableau 7-9/J.192 – Options DHCP de client CDC

Numéro d'option	Fonction de l'option	Prise en charge du protocole par le client CDC (M = obligatoire)
0	Bourrage	M
255	Fin	M
1	Masque de sous-réseau	M
2	Option de décalage horaire	M
3	Option de routeur	M
4	Option de serveur temporel	M
6	Serveur distant de noms de domaine	M
7	Serveur de journalisation (syslog)	M
12	Nom du serveur local	M
15	Nom de domaine	M
23	Temps par défaut de recherche de relais	M
26	Unité MTU d'interface	M

Tableau 7-9/J.192 – Options DHCP de client CDC

Numéro d'option	Fonction de l'option	Prise en charge du protocole par le client CDC (M = obligatoire)
43	Informations propres au vendeur	M
50	Adresse IP demandée	M
10	Durée de location d'adresse IP	M
54	Identificateur de serveur distant	M
55	Liste de demande de paramètres	M
60	Identificateur de classe de vendeur	M
61	Identificateur de client	M
122	Sous-option 3 – Adresse d'entité SNMP du fournisseur de services	M
122	Sous-option 6 – Nom du secteur Kerberos du secteur de préconfiguration	M
122	Sous-option 10 – Adresse IP du serveur Kerberos	M

Le dispositif PS DOIT inclure, dans les messages DISCOVER et REQUEST du protocole DHCP envoyés au serveur DHCP du réseau câblé, les options DHCP énumérées comme étant obligatoires dans le Tableau 7-10.

Tableau 7-10/J.192 – Options DHCP de client CDC contenues dans les messages DISCOVER et REQUEST

Numéro d'option	Fonction de l'option	Inclusion du protocole par le client CDC (M = obligatoire)
255	Fin	M
43	Informations propres au vendeur	M
50	Adresse IP demandée	M (message REQUEST du DHCP seulement)
55	Liste de demande de paramètres	M
60	Identificateur de classe de vendeur	M
61	Identificateur de client	M

Le dispositif PS DOIT demander les options DHCP énumérées comme étant obligatoires dans le Tableau 7-11, au moyen de l'option DHCP 55 (liste de demande de paramètres) [RFC 2132] émise dans les messages DISCOVER et REQUEST du protocole DHCP.

Tableau 7-11/J.192 – Options DHCP de client CDC demandée dans l'option 55

Numéro d'option	Fonction de l'option	Inclusion du protocole par le client CDC (M = obligatoire)
1	Masque de sous-réseau	M
2	Option de décalage horaire	M
3	Option de routeur	M
4	Option de serveur temporel	M
6	Serveur distant de noms de domaine	M
7	Serveur de journalisation (syslog)	M
15	Nom de domaine	M
23	Temps par défaut de recherche de relais	M
26	Unité MTU d'interface	M
10	Durée de location d'adresse IP	M
54	Identificateur de serveur distant	M
122	Option de configuration de client compatible avec le modèle PacketCable	M

La liste suivante énumère les actions que le dispositif PS est tenu d'effectuer si l'une quelconque des options DHCP demandées dans l'option DHCP 55 (énumérées dans le Tableau 7-11) est absente du message DHCP OFFER qu'il reçoit du serveur DHCP.

1) Si l'option DHCP 1 (Masque de sous-réseau) n'est pas présente dans le message DHCP d'offre de location que le dispositif PS a reçu du serveur DHCP, la réponse est incomplète et le dispositif PS DOIT produire l'identificateur d'événement 68000301 et relancer le processus de préconfiguration en commençant par diffuser un message DHCP DISCOVER par l'intermédiaire de son interface avec le réseau régional.

2) Si l'option DHCP 2 (Décalage horaire) n'est pas présente dans le message DHCP d'offre de location que le dispositif PS a reçu du serveur DHCP, l'offre de location n'est pas considérée comme incomplète et le dispositif PS est autorisé à accepter la location.

3) Si l'option DHCP 3 (Routeur) n'est pas présente dans le message DHCP d'offre de location que le dispositif PS a reçu du serveur DHCP, l'offre de location n'est pas considérée comme incomplète et le dispositif PS est autorisé à accepter la location.

4) Si l'option DHCP 4 (Serveur de marqueurs temporels) n'est pas présente dans le message DHCP d'offre de location que le dispositif PS a reçu du serveur DHCP, la réponse est incomplète et le dispositif PS DOIT produire l'identificateur d'événement 68000301 et relancer le processus de préconfiguration en commençant par diffuser un message DHCP DISCOVER par l'intermédiaire de son interface avec le réseau régional.

5) Si l'option DHCP 6 (Serveur de noms de domaine) n'est pas présente dans le message DHCP d'offre de location que le dispositif PS a reçu du serveur DHCP, la réponse est incomplète et le dispositif PS DOIT produire l'identificateur d'événement 68000301 et relancer le processus de préconfiguration en commençant par diffuser un message DHCP DISCOVER par l'intermédiaire de son interface avec le réseau régional.

6) Si l'option DHCP 7 (Serveur de journalisation) n'est pas présente dans le message DHCP d'offre de location que le dispositif PS a reçu du serveur DHCP, l'offre de location n'est pas considérée comme incomplète et le dispositif PS est autorisé à accepter la location.

7) Si l'option DHCP 15 (Nom de domaine) n'est pas présente dans le message DHCP d'offre de location que le dispositif PS a reçu du serveur DHCP, l'offre de location n'est pas considérée comme incomplète et le dispositif PS est autorisé à accepter la location.

8) Si l'option DHCP 23 (Temps de recherche de relais IP par défaut) n'est pas présente dans le message DHCP d'offre de location que le dispositif PS a reçu du serveur DHCP, l'offre de location n'est pas considérée comme incomplète et le dispositif PS est autorisé à accepter la location.

9) Si l'option DHCP 26 (Unité MTU d'interface) n'est pas présente dans le message DHCP d'offre de location que le dispositif PS a reçu du serveur DHCP, l'offre de location n'est pas considérée comme incomplète et le dispositif PS est autorisé à accepter la location.

10) Si l'option DHCP 51 (Durée de location d'adresse IP) n'est pas présente dans le message DHCP d'offre de location que le dispositif PS a reçu du serveur DHCP, la réponse est incomplète et le dispositif PS DOIT produire l'identificateur d'événement 68000301 et relancer le processus de préconfiguration en commençant par diffuser un message DHCP DISCOVER par l'intermédiaire de son interface avec le réseau régional.

11) Si l'option DHCP 54 (Identificateur de serveur distant) n'est pas présente dans le message DHCP d'offre de location que le dispositif PS a reçu du serveur DHCP, l'offre de location n'est pas considérée comme incomplète et le dispositif PS est autorisé à accepter la location.

12) Si l'option DHCP 122 (Option de configuration de client CableLabs) n'est pas présente dans le message DHCP d'offre de location que le dispositif PS a reçu du serveur DHCP, l'offre de location n'est pas considérée comme incomplète et le dispositif PS est autorisé à accepter la location.

Si le dispositif PS ne reçoit pas d'offre de location complète après avoir épuisé la valeur maximale du nombre de réessais, le dispositif PS DOIT fonctionner en mode inactif comme décrit au § 7.3.3.2.4.

Le dispositif PS DOIT prendre en charge une adresse de gestionnaire d'entité SNMP de fournisseur de services (sous-option 3 de l'option DHCP 122) configurée comme une adresse IPv4. Le format de la sous-option 3 de l'option DHCP 122 est décrit dans [RFC 3495].

Le dispositif PS DOIT prendre en charge un nom du secteur Kerberos (option DHCP 122, sous-option 6). Un nom du secteur Kerberos est requis par le dispositif PS afin d'autoriser une exploration par service DNS en vue de trouver l'adresse de l'entité de centre de distribution de clés (KDC) du fournisseur de services. Le format de la sous-option 6 de l'option DHCP 122 est décrit dans [RFC 3495].

Le dispositif PS DOIT prendre en charge une adresse IP de serveur de centre de distribution de clés (KDC) (option DHCP 122, sous-option 10). La sous-option d'adresse IP du serveur de centre KDC informe le dispositif PS de l'adresse réseau d'un ou de plusieurs serveurs de centre de distribution de clés.

Le codage de la sous-option d'adresse du serveur de centre KDC est décrit dans [RFC 3634].

Chaque fois que la première interface PS WAN-Data ne possède pas de location DHCP en cours, cette première interface PS WAN-Data DOIT avoir par défaut les paramètres IP suivants:

– adresse IP "de repli" de réseau WAN-Data: 192.168.100.5

– masque de réseau: 255.255.255.0

– passerelle par défaut: 192.168.100.1

La finalité de l'adresse IP "de repli" d'un réseau WAN-Data est de permettre l'accès à l'adresse IP de diagnostic du câblo-modem (192.168.100.1) à partir d'un dispositif IP de réseau local chaque fois qu'il n'y a pas d'adresse IP normale de réseau WAN-Data disponible dans ce dispositif PS. L'adresse IP "de repli" de réseau WAN-Data NE DOIT être utilisée qu'en tant que partie d'adresse IP de

réseau régional du nuplet de conversion dynamique NAT ou NAPT d'un mappage d'adresse de conversion C-NAT ou C-NAPT, selon le cas, vers l'adresse IP de diagnostic du câblo-modem (192.168.100.1). Le dispositif PS DOIT revenir par défaut à l'adresse IP "de repli" du réseau WAN-Data immédiatement après la mise sous tension et chaque fois que des locations actuelles d'adresse IP de réseau WAN-Data arrivent à expiration de sorte qu'aucune adresse IP de réseau WAN-Data ne demeure active, de manière à offrir un accès permanent aux capacités de diagnostic du câblo-modem. Le dispositif PS NE DOIT PAS utiliser l'adresse IP "de repli" de réseau WAN-Data quand il est configuré de façon à fonctionner en mode primaire de traitement de paquet par transfert.

Le dispositif PS NE DOIT PAS utiliser l'adresse IP "de repli" de réseau WAN-Data pour de quelconques mappages de conversion C-NAT ou C-NAPT quand le dispositif PS possède une location actuelle d'adresse IP de réseau WAN-Data. Si un serveur DHCP situé à l'interface PS WAN offre aux services de portail (client CDC) une location pour l'adresse IP 192.168.100.5, c'est-à-dire la même adresse que l'adresse IP "de repli" de réseau WAN-Data, le dispositif PS (client CDC) PEUT accepter cette location et utiliser cette adresse comme adresse IP de réseau WAN-Data pour un mappage de conversion C-NAT ou C-NAPT.

Même en utilisant l'adresse IP par défaut de réseau WAN-Data 192.168.100.5, le dispositif PS DOIT continuer à exécuter un message DHCP DISCOVER toutes les 10 secondes jusqu'à ce qu'une location DHCP valide soit accordée à cette interface PS WAN-Data (ou à l'interface avec le réseau WAN-Man si les réseaux WAN-Man et WAN-data se partagent une seule adresse IP).

Quand un dispositif PS va acquérir une adresse IP de gestion de réseau régional pour son interface WAN-Man, le dispositif PS DOIT toujours insérer son adresse matérielle de réseau régional dans le champ d'identificateur de client (option DHCP 61) du message DHCP DISCOVER.

Si, pendant sa tentative d'acquérir une location pour l'adresse IP de l'interface PS WAN-Man, le client CDC ne reçoit aucun message DHCP OFFER, le dispositif PS DOIT journaliser l'identificateur d'événement ID 68000100 dans le journal local et rediffuser un message DHCP DISCOVER (c'est-à-dire relancer la séquence de préconfiguration si cette condition d'échec apparaît) – en répétant jusqu'à 5 fois cette tentative d'acquisition de location DHCP. Si le client CDC, lors de sa cinquième tentative d'acquisition d'une location d'adresse IP de l'interface PS WAN-Man, ne reçoit aucun message DHCP OFFER, le dispositif PS DOIT utiliser l'adresse IP "de repli" de réseau régional, le masque de réseau et la passerelle par défaut comme décrit ci-dessus et continuer à essayer d'acquérir une adresse IP valide de réseau WAN-Man en diffusant le message DHCP DISCOVER à la sortie de son interface avec le réseau régional toutes les 10 secondes jusqu'à ce qu'une location DHCP valide soit accordée pour l'adresse IP de réseau WAN-Man.

Lorsqu'un dispositif PS fonctionnant en mode 2 d'adresse de réseau régional (comme décrit au § 7.3.3.2) va acquérir une adresse IP de réseau WAN-Data pour une interface avec un réseau WAN-Data qui utilisera une adresse IP distincte de l'interface avec le réseau WAN-Man, le dispositif PS DOIT inclure l'option d'identificateur de client (cabhCdpWanDataAddrClientId) dans le message DISCOVER du DHCP. Afin de permettre ces identificateurs uniques de client de réseau WAN-Data, le client CDC DOIT autoriser le système NMS à créer des entrées cabhCdpWanDataAddrClientId dans la table cabhCdpWanDataAddrTable.

Si un dispositif PS doit fonctionner en mode 2 d'adresse de réseau régional (comme décrit au § 7.3.3.2), ce dispositif PS DOIT essayer d'obtenir une adresse IP, via DHCP, pour chaque identificateur unique de client (cabhCdpWanDataAddrClientId) dans la table cabhCdpWanDataAddrTable, jusqu'à la limite définie par cabhCdpWanDataIpAddrCount.

Le dispositif PS DOIT continuer à retransmettre le message DISCOVER du DHCP diffusé en implémentant un algorithme randomisé d'attente exponentielle de données, cohérent avec celui qui est décrit dans [RFC 2131], avant d'acquérir une location d'adresse IP valide d'interface PS WAN-Man et/ou PS WAN-Data, selon les besoins.

Si le dispositif PS (CDC) réussit à acquérir l'adresse IP de réseau WAN-Man (c'est-à-dire qu'il reçoit un acquittement ACK d'un serveur DHCP via l'interface PS WAN-Man) à sa première tentative, et si ce dispositif PS doit fonctionner en mode de préconfiguration DHCP, ce dispositif PS DOIT essayer une synchronisation d'heure locale avec le serveur distant d'heure locale (ToD) en émettant une demande d'heure ToD comme décrit au § 7.5.4, avant d'essayer d'importer par téléchargement le fichier de configuration PS.

Si le dispositif PS (CDC) ne réussit pas à acquérir l'adresse IP de réseau WAN-Man (c'est-à-dire que la requête DHCP arrive à expiration conformément au [RFC 2131]) à sa première tentative, ce dispositif PS DOIT déclencher le serveur CDS (c'est-à-dire lancer le fonctionnement du serveur CDS), de façon que le serveur CDS puisse desservir les requêtes DHCP issues de dispositifs IP de réseau local dans le secteur LAN-Trans.

La fonction de client CDC du dispositif PS ne DOIT répondre qu'aux messages DHCP qui sont reçus par l'intermédiaire d'une interface avec le réseau régional et ne DOIT envoyer de tels messages que par une telle interface.

Lorsque la location DHCP d'adresse de réseau WAN-Man arrive à expiration, le dispositif PS DOIT effacer toutes les entrées de rangée de la table cabhCdpWanDnsServerTable.

Modes opératoires de préconfiguration de dispositif PS

Le présent paragraphe définit les exigences du dispositif PS pour le fonctionnement dans les modes présentés dans le § 5.5.

Si un dispositif PS est intégré en tant qu'élément eSAFE avec un câblo-modem conforme à eDOCSIS [eDOCSIS1] et si l'objet de base MIB esafePsCableHomeModeControl conforme à eDOCSIS est mis à la valeur provSystem(2), alors ce dispositif PS intégré DOIT essayer d'acquérir une location d'adresse IP de réseau WAN-Man de dispositif PS, et adhérer aux exigences pour le mode de préconfiguration DHCP, le mode de préconfiguration SNMP, ou le mode CableHome inactif comme décrit ci-dessous. Des exigences additionnelles pour le fonctionnement d'un dispositif PS intégré sur la base de la valeur de l'objet esafePsCableHomeModeControl sont définies ci-dessous.

Mode de préconfiguration DHCP

Si le client CDC reçoit, pendant le processus d'acquisition d'une location pour l'adresse IP de l'interface PS WAN-Man, une adresse IP valide contenue dans le champ 'siaddr' du message ACK du protocole DHCP [RFC 2131] reçu du serveur DHCP dans le réseau câblé, et un nom de fichier valide dans le champ 'file' et ne reçoit pas -dans l'option DHCP 122- la sous-option 3, la sous-option 6 ou la sous-option 10 (combinaison valide 1), le dispositif PS DOIT régler l'objet cabhPsDevProvMode à la valeur dhcpmode(1) et essayer de synchroniser l'heure locale avec le serveur temporel ToD comme décrit dans le § 7.5.4, "Fonction de client d'heure locale: exigences". Selon la valeur des champs 'siaddr' et 'file' de l'en-tête de message DHCP, le dispositif PS peut être tenu d'essayer d'importer par téléchargement un fichier de configuration. Voir le § 7.4.4.2, Exigences relatives au déclenchement de configuration BPSC.

Mode de préconfiguration SNMP

Si, pendant le processus d'acquisition d'une location pour l'adresse IP de l'interface PS WAN-Man, le client CDC reçoit un message DHCP ACK provenant du serveur DHCP dans le réseau câblé contenant l'option DHCP 122 avec une adresse IP valide (adresse de gestionnaire SNMP) dans la sous-option 3, contenant un nom valide du secteur Kerberos dans la sous-option 6 et contenant une adresse IP valide (adresse IP du serveur Kerberos) dans la sous-option 10 mais ne reçoit pas d'adresse IP valide dans le champ 'siaddr' et ni de nom de fichier valide dans le champ 'file' (combinaison valide 2), le dispositif PS DOIT régler l'objet cabhPsDevProvMode à la valeur snmpmode(2) et DOIT mettre en fonctionnement le serveur CDS puis essayer de synchroniser l'heure locale avec le serveur temporel ToD et se légitimer auprès du serveur de centre KDC comme

décrit dans le § 11.3.4, "Infrastructure d'authentification: exigences". Le dispositif PS fonctionnant en mode de préconfiguration SNMP peut aussi être configuré de façon à essayer d'importer par téléchargement un fichier de configuration. Voir le § 7.4.4.2, Exigences relatives au déclenchement de configuration BPSC.

Mode CableHome inactif

Si le client CDC reçoit, pendant le processus d'acquisition d'une location pour l'adresse IP de l'interface PS WAN-Man, dans l'option DHCP 122 du message ACK en protocole DHCP reçu du serveur DHCP dans le réseau câblé, une combinaison quelconque des sous-options 3, 6 et 10, d'un champ 'siaddr' et d'un champ 'file' autre que les deux combinaisons valides décrites ci-dessus, ce dispositif PS a reçu une configuration DHCP non valide et DOIT journaliser l'identificateur d'événement 68000301 (voir le Tableau B.1, Evénements définis pour CableHome) puis effectuer ce qui suit dans l'hypothèse qu'il est connecté par câblo-modem à un réseau de données par câble qui ne prend pas en charge la préconfiguration CableHome (mode CableHome inactif):

- désactiver l'agent SNMP (portail CMP) pour l'accès à l'interface avec un réseau régional. Laisser l'agent SNMP activé pour les messages reçus par l'intermédiaire de l'interface avec un réseau local (c'est-à-dire pour les messages SNMP adressés à l'interface PS routeur-serveur);
- désactiver le client du protocole TFTP;
- désactiver la signalisation des événements par serveur SYSLOG;
- accepter la location d'adresse IP offerte (équipement CPE) et l'utiliser comme adresse d'interface PS WAN-Data dans la table de mappage du portail CAP, y compris l'attribution de cette adresse à l'objet cabhCdpWanDataAddrIp et l'insertion des autres entrées de la table d'adresses IP de réseau WAN-Data du portail CDP (objet cabhCdpWanDataAddrTable). Le dispositif PS fonctionnera sans adresse IP de réseau WAN-Man, ce qui est différent de chacun des modes d'adresse de réseau régional décrits dans le § 7.3.3.2.3.2;
- fermer le temporisateur de préconfiguration;
- mettre la valeur de l'objet cabhPsDevProvMode à dormantCHmode(3);
- mettre la valeur de l'objet cabhPsDevProvState à fail(3);
- activer le serveur CDS;
- activer le portail CAP et la fonctionnalité de commutation USFS;
- activer le portail CNP;
- activer le pare-feu;
- fonctionner avec les paramètres qui ont déjà été préconfigurés, y compris ceux qui ont été extraits des valeurs d'objets de base MIB persistants. Le dispositif PS fonctionnant en mode IPCable2Home inactif NE DOIT PAS réinitialiser ses objets de base MIB aux réglages par défaut fixées à l'usine.

Un dispositif PS intégré peut également être configuré de façon à fonctionner en mode CableHome inactif par l'intermédiaire de l'objet esafePsCableHomeModeControl de la base MIB eSAFE conforme à eDOCSIS [eDOCSIS1]. Si l'objet esafePsCableHomeModeControl du câblo-modem intégré conforme à eDOCSIS est mis à dormantCHMode(3), le dispositif ePS est tenu d'essayer d'acquérir une location d'adresse IP et de fonctionner en mode CableHome inactif comme décrit ci-dessus, quelles que soient les valeurs des champs DHCP 'siaddr' et 'file', en présence ou en absence de l'option DHCP 122 et de ses sous-options dans les messages DHCP OFFER et ACK. Voir le Tableau 7-12.

Mode désactivé

Lorsqu'un dispositif PS intégré est configuré de façon à fonctionner en mode désactivé par l'intermédiaire la base MIB eSAFE du modèle eDOCSIS (esafePsCableHomeModeControl = disabledMode(1)) [eDOCSIS1], alors le dispositif PS intégré DOIT faire ce qui suit:

- libérer sa location d'adresse IP de réseau WAN-Man et toutes éventuelles locations d'adresse IP de réseau WAN-Data qu'il pourrait posséder dans un cas comme dans l'autre, ou arrêter d'essayer d'acquérir une location d'adresse IP de réseau WAN-Man ou WAN-Data en rejetant sans NE PASification les messages OFFER, ACK, ou autres messages DHCP;
- agir comme un pont transparent comme défini dans la référence [ISO/CEI 10038], entre le secteur de réseau WAN-Data et le secteur de réseau LAN-Pass, y compris le routage transparent de tous les types de trame dont les spécifications DOCSIS [DOCSIS1], [DOCSIS9] exigent le passage par un câblo-modem;
- NE PAS exécuter d'éventuelles fonctions de routage transparent par conversion C-NAT ou C-NAPT ;
- désactiver la fonctionnalité de serveur distant DHCP (CDS), de serveur distant HTTP, d'agent SNMP, et de serveur DNS (portail CNP);
- désactiver le pare-feu;
- abandonner tous les paquets envoyés à l'adresse du routeur-serveur du PS (cabhCdpServerRouter) ou à l'adresse IP "notoire" de réseau local 192.168.0.1 du PS;
- donner priorité au traitement de commutation de réexpédition sélective en amont (USFS), par rapport aux décisions de routage de réseau local à réseau régional.

La seule façon de configurer un dispositif PS de façon à fonctionner en mode désactivé consiste à régler à disabled(1) la valeur d'un objet esafePsCableHomeModeControl de base MIB eSAFE de câblo-modem eDOCSIS. Le mode désactivé ne s'applique pas à un dispositif PS autonome car il n'est pas intégré comme un objet eSAFE dans un câblo-modem eDOCSIS.

Le dispositif PS intégré peut être extrait du mode désactivé en réglant à provSystem(2) ou à dormantCHMode(3) la valeur de l'objet esafePsCableHomeModeControl de la base MIB eSAFE du câblo-modem intégré [eDOCSIS1].

Lorsque le dispositif PS est administrativement changé (extrait) à partir du mode désactivé, ce dispositif PS DOIT régler tous les objets de base MIB CableHome à leur valeur par défaut réglée à l'usine.

Le Tableau 7-12 définit les actions que le dispositif PS intégré est tenu d'effectuer quand l'objet esafePsCableHomeModeControl de la base MIB eSAFE conforme à eDOCSIS [eDOCSIS1] est activé, pour chaque mode de fonctionnement du dispositif PS. Le dispositif ePS DOIT effectuer les actions énumérées dans le Tableau 7-12 s'il doit fonctionner dans les mode énumérés dans la première colonne, intitulée 'Mode actuel de l'ePS'; et l'objet esafePsCableHomeModeControl de la base MIB eSAFE conforme à eDOCSIS est réglé comme indiqué dans la deuxième colonne, intitulée 'esafePsCableHomeModeControl'. Noter que le mode actuel du dispositif ePS, indiqué dans la première colonne du Tableau 7-12, est pris en compte dans l'objet de base MIB eDOCSIS esafePsCableHomeModeStatus.

Tableau 7-12/J.192 – Actions requises de l'ePS pour les réglages de l'objet esafePsCableHomeModeControl

Mode actuel de l'ePS	Objet esafePsCableHomeModeControl	Actions requises de l'ePS
Mode désactivé	disabledMode(1)	Aucune action requise
Mode inactif CableHome	disabledMode(1)	Effectuer les actions énumérées dans les Mode désactivé § ci-dessus
Mode CableHome	disabledMode(1)	Effectuer les actions énumérées dans le paragraphe ci-dessus concernant le mode désactivé
Mode désactivé	provSystem(2)	Relancer le processus de préconfiguration en commençant par diffuser le message DHCP DISCOVER par l'intermédiaire de l'interface avec le réseau régional
Mode inactif CableHome	provSystem(2)	Relancer le processus de préconfiguration en commençant par diffuser le message DHCP DISCOVER par l'intermédiaire de l'interface avec le réseau régional
Mode CableHome	provSystem(2)	Relancer le processus de préconfiguration en commençant par diffuser le message DHCP DISCOVER par l'intermédiaire de l'interface avec le réseau régional
Mode désactivé	dormantCHMode(3)	– Relancer le processus de préconfiguration en commençant par diffuser le message DHCP DISCOVER par l'intermédiaire de l'interface avec le réseau régional – Ne pas inclure les sous-options 2 à 14 de l'option 43 du DHCP dans les messages DHCP DISCOVER / REQUEST – Ne pas inclure 'CableHome1.0' ou 'CableHome1.1' comme valeur d'option 60 du DHCP – Ne pas inclure l'option DHCP 122 dans la liste de demande de paramètres de l'option DHCP 55 – Ignorer les champs d'en-tête DHCP 'file' et 'siaddr' dans les messages DHCP OFFER et ACK: ne pas importer par téléchargement de fichier de configuration et ne pas fonctionner en mode de préconfiguration DHCP ni en mode de préconfiguration SNMP, quelles que soient les valeurs des champs DHCP 'file' et 'siaddr' et celles des options DHCP. – Effectuer les actions énumérées dans le paragraphe ci-dessus concernant le mode inactif CableHome

Tableau 7-12/J.192 – Actions requises de l'ePS pour les réglages de l'objet esafePsCableHomeModeControl

Mode actuel de l'ePS	Objet esafePsCableHomeModeControl	Actions requises de l'ePS
Mode inactif CableHome	dormantCHMode(3)	Aucune action requise
Mode CableHome	dormantCHMode(3)	– Relancer le processus de préconfiguration en commençant par diffuser le message DHCP DISCOVER par l'intermédiaire de l'interface avec le réseau régional – Ne pas inclure les sous-options 2 à 14 de l'option 43 du DHCP dans les messages DHCP DISCOVER / REQUEST – Ne pas inclure 'CableHome1.0' ou 'CableHome1.1' comme valeur d'option 60 du DHCP – Ne pas inclure l'option DHCP 122 dans la liste de demande de paramètres de l'option DHCP 55 – Ignorer les champs d'en-tête DHCP 'file' et 'siaddr' dans les messages DHCP OFFER et ACK: ne pas importer par téléchargement de fichier de configuration et ne pas fonctionner en mode de préconfiguration DHCP ni en mode de préconfiguration SNMP, quelles que soient les valeurs des champs DHCP 'file' et 'siaddr' et celles des options DHCP. – Effectuer les actions énumérées dans le paragraphe ci-dessus concernant le mode inactif CableHome

7.4 Fonction de services de portail – Configuration globale des services de portail (BPSC)

7.4.1 Objectifs de la fonction de configuration globale des services de portail

Les principaux objectifs de la fonction BPSC sont de demander, de recevoir et de traiter les paramètres de configuration du dispositif PS et du pare-feu.

7.4.2 Fonction de configuration globale des services de portail: directives de conception du système

Les directives identifiées dans le Tableau 7-13 ont guidé la spécification des capacités pour la fonction de configuration globale des services de portail:

Tableau 7-13/J.192 – Configuration globale des services de portail: directives de conception du système

Numéro	Directives
BPSC 1	Offrir un mécanisme permettant au dispositif PS de télécharger et de traiter les fichiers de configuration de dispositif PS et de pare-feu.

7.4.3 Fonction de configuration globale des services de portail: description du système

La configuration globale des services de portail est normalement effectuée pendant la préconfiguration de l'élément de services de portail, par le traitement des réglages de configuration contenus dans un fichier de configuration. Cependant, ce processus peut être lancé à tout moment. Dans le présent paragraphe, le terme "fichier de configuration" signifie soit le fichier de configuration du dispositif PS ou le fichier de configuration du pare-feu. Les exigences spécifiques concernant l'un ou l'autre type de fichier de configuration seront étiquetées avec la valeur appropriée, c'est-à-dire "Fichier de configuration du dispositif PS" ou "Fichier de configuration du pare-feu". L'utilitaire de configuration globale des services de portail comporte les composants suivants:

- le format du fichier de configuration;
- les modes de déclenchement du processus de téléchargement;
- les moyens d'authentifier le fichier;
- les moyens de signaler en retour l'état du téléchargement du fichier de configuration et d'autres considérations.

La configuration globale des services de portail (BPSC, *bulk PS configuration*) est un utilitaire que les opérateurs peuvent utiliser afin de changer en bloc les réglages de configuration du dispositif PS et du pare-feu, au moyen d'un fichier de configuration. En principe, le fichier de configuration contiendra de nombreux réglages, car la principale utilité des fichiers de configuration est la capacité de changer un certain nombre de réglages de configuration avec le minimum d'intervention de la part du câblo-opérateur. Cependant, on suppose que le fichier de configuration du pare-feu ne va servir qu'à des réglages propres au pare-feu.

Le processus de configuration globale des services de portail peut se comporter de la même façon que des mises à jour (SET) SNMP successives, exécutées manuellement par un opérateur. Le fichier de configuration est un utilitaire destiné à rendre les opérateurs plus productifs et moins enclins à commettre des erreurs lors de grands changements de configuration.

Il est significatif de noter qu'un dispositif PS fonctionnant en mode de préconfiguration SNMP n'a pas besoin d'avoir un fichier de configuration du dispositif PS chargé avant de pouvoir fonctionner. On suppose qu'un dispositif PS fonctionnant en mode de préconfiguration SNMP va s'auto-initialiser à un état connu et qu'un dispositif PS pourrait fonctionner pendant toute sa durée de vie sans avoir de fichier de configuration du dispositif PS chargé. Cependant, un dispositif PS acceptera et traitera un fichier de configuration du dispositif PS lorsqu'on lui en fournira un.

7.4.4 Fonction de configuration globale des services de portail: exigences

Un dispositif PS fonctionnant en mode de préconfiguration DHCP DOIT télécharger et traiter un fichier de configuration du dispositif PS.

Un dispositif PS fonctionnant en mode de préconfiguration SNMP DOIT être capable de fonctionner sans fichier de configuration du dispositif PS, mais DOIT être capable de télécharger et de traiter un fichier de configuration du dispositif PS s'il est déclenché comme décrit dans le § 7.3.3.2. Le dispositif PS n'est pas tenu de télécharger un fichier de configuration du pare-feu en mode de préconfiguration DHCP ou SNMP.

Les réglages d'objet de base MIB transmis dans le fichier de configuration du dispositif PS ont priorité sur les réglages d'objet de base MIB existants et DOIVENT les remplacer par surécriture.

7.4.4.1 Format du fichier de configuration: exigences

Les données de configuration du dispositif PS ou du pare-feu DOIVENT être contenues dans un fichier qui est téléchargé par protocole TFTP ou HTTPS. Le fichier de configuration DOIT contenir un certain nombre de réglages de configuration (1 par paramètre), chacun étant de la forme "Type-Longueur-Valeur (TLV)". Les définitions de ces termes sont présentées dans le Tableau 7-14.

Tableau 7-14/J.192 – Définitions des éléments TLV

Type	Identificateur d'un seul octet qui définit le paramètre
Longueur	Champ de deux octets spécifiant la longueur du champ de valeur (non compris les champs Type et Longueur)
Valeur	Ensemble d'octets de longueur définie par le terme 'longueur', contenant la valeur propre au paramètre

Les réglages de configuration DOIVENT se suivre directement dans le fichier, qui est un flux d'octets (sans marqueurs d'enregistrement). Le dispositif PS DOIT être capable de traiter et de recevoir correctement un fichier de configuration qui est complété par bourrage de façon à avoir un nombre entier de mots de 32 bits et DOIT être capable de recevoir et de traiter correctement un fichier de configuration qui n'est pas complété par bourrage à un nombre entier de mots de 32 bits. Voir au § 7.4.4.1.1 une définition du bourrage. Les réglages de configuration sont subdivisés en trois types:

- réglages de configuration qui sont tenus d'être présents;
- réglages de configuration additionnels ou facultatifs, spécifiés par le modèle IPCable2Home, qui PEUVENT être présents;
- réglages de configuration propres au vendeur.

Un fichier de configuration de dispositif PS peut contenir de nombreux paramètres différents, mais les seuls paramètres qui DOIVENT être inclus dans le fichier de configuration de dispositif PS sont la vérification de l'intégrité du message (MIC, *message integrity check*) PS (de type 53) et le marqueur de fin de données (de type 255). Un fichier de configuration de pare-feu PEUT contenir de nombreux paramètres TLV différents de type 28 pour configurer le pare-feu, mais le seul paramètre qui DOIT être inclus dans le fichier de configuration de pare-feu est le marqueur de fin de données (Type 255). Si le fichier de configuration de pare-feu contient une vérification de l'intégrité de message du dispositif PS (MIC) (Type 53), celui-ci DOIT l'ignorer.

Afin de permettre une gestion uniforme du dispositif PS, celui-ci DOIT prendre en charge un fichier de configuration dont la longueur peut atteindre 64 K octets.

Chaque élément de services de portail DOIT prendre en charge les types de paramètre de configuration 0, 9, 10, 21, 28, 32, 33, 34, 38, 43, 53 et 255, qui sont décrits dans le présent paragraphe. Chaque paramètre TLV contenu dans le fichier de configuration du pare-feu décrit un attribut du pare-feu. Etant donné que le pare-feu IPCable2Home est configuré par l'accès à la base MIB de sécurité IPCable2Home (voir § 11.6.4, "Pare-feu: exigences"), un fichier de configuration du pare-feu comprend normalement les réglages de configuration par TLV de type 28, qui contiennent des objets de base MIB en protocole SNMP. Des informations de configuration de pare-feu propres au vendeur sont autorisées pour transmission aux services de portail dans le fichier de configuration du pare-feu au moyen du type de réglage de configuration propre au vendeur 43 (TLV-43). Si le fichier de configuration ne contient pas les attributs requis, le dispositif PS DOIT rejeter le fichier.

La longueur de la valeur contenue dans le champ de longueur concernant tout paramètre de configuration inclus dans un fichier de configuration IPCable2Home DOIT être de 2 octets.

La valeur du champ de longueur pour chaque type figurant dans les descriptions d'élément TLV du présent paragraphe est la longueur réelle en octets du champ de valeur.

7.4.4.1.1 Réglage de configuration du bourrage

Cet élément n'a aucun champ de longueur ou de valeur et n'est utilisé qu'après le marqueur de fin de données pour compléter le fichier à un nombre entier de mots de 32 bits.

Type	Longueur	Valeur
0	---	---

7.4.4.1.2 Nom de fichier de mise à jour logicielle

Nom du fichier de mise à jour logicielle pour le dispositif IPCable2Home. Le nom du fichier est un nom de chemin de répertoire entièrement qualifié. Le fichier est censé résider dans un serveur TFTP identifié dans une option de réglage de configuration.

Type	Longueur	Valeur
9	Variable	Nom du fichier

7.4.4.1.3 Contrôle d'accès en écriture du protocole SNMP

Cet objet permet de désactiver l'accès SNMP de mise à jour (SET) à des objets individuels de base MIB. Chaque instance de cet objet commande l'accès à tous les objets de base MIB inscriptibles dont les préfixes d'identificateur d'objet (OID) correspondent. Cet objet peut être répété afin de désactiver l'accès à un nombre quelconque d'objets de base MIB.

Type	Longueur	Valeur
10	n	Préfixe d'identificateur OID plus fanion de commande

Où n est la longueur du codage ASN.1 conforme aux règles de codage de base [Rec. UIT-T X.690 | ISO/CEI 8825-1] du préfixe de l'identificateur d'objet (OID) plus un octet pour le fanion de commande.

Le fanion de commande peut prendre les valeurs suivantes:

- 0 – accès en écriture autorisé
- 1 – accès en écriture interdit

Tout préfixe d'identificateur OID peut être utilisé. L'identificateur OID vide 0.0 peut servir à contrôler l'accès à tous les objets de base MIB. (L'identificateur OID 1.3.6.1 possédera le même effet.)

Quand des instances multiples de cet objet sont présentes et se superposent, le plus long (le plus spécifique) préfixe a priorité.

L'on peut donc avoir, par exemple:

someTable: accès en écriture interdit

someTable.1.3: accès en écriture autorisé

Cet exemple interdit l'accès à tous les objets contenus dans la table someTable à l'exception de ceux de la table someTable.1.3.

7.4.4.1.4 Serveur TFTP de mise à jour logicielle

Adresse IP du serveur TFTP dans lequel réside le fichier de mise à jour logicielle pour le dispositif IPCable2Home.

Type	Longueur	Valeur
21	4	ip1, ip2, ip3, ip4

7.4.4.1.5 Objet de base MIB du protocole SNMP avec extension de longueur – Première phase

Cet objet permet de régler les objets de base MIB en protocole SNMP via le processus d'enregistrement en protocole TFTP avant les messages SET du SNMP effectués avec le nuplet TLV-28, dont la fonction consiste à n'inclure que les messages SET du SNMP qui doivent se produire avant d'autres messages SET du SNMP afin d'assurer un fonctionnement correct, tels que les objets SetToFactory (p. ex., cabhPsDevSetToFactory) qui effacent les objets de base MIB permanents. Les messages SET du SNMP non prioritaires sont censés être inclus dans le nuplet TLV-28.

La valeur de ce paramètre est une variable d'association du SNMP (VarBind) comme défini dans [RFC 3416]. Le paramètre VarBind est codé conformément aux règles de codage de base de la notation ASN.1, exactement comme ce serait le cas s'il faisait partie d'une unité PDU de requête SET du SNMP.

Type	Longueur	Valeur
27	Variable	Variable d'association

Le dispositif PS DOIT traiter la variable d'association contenue dans un nuplet TLV de type 27 comme si elle faisait partie d'une requête SET du SNMP, avec les précautions suivantes:

- il DOIT traiter la requête comme étant entièrement autorisée (il ne peut pas la refuser pour absence de privilège);
- les dispositions de commande d'écriture du SNMP ne s'appliquent pas;
- aucune réponse du SNMP n'est produite par le dispositif PS;
- cet objet PEUT être répété avec différents paramètres VarBind afin de mettre à jour ("SET") l'association d'un certain nombre d'objets de base MIB. Tous les messages SET du SNMP d'un fichier de configuration qui apparaissent dans des nuplets TLV de type 27 DOIVENT être traités comme s'ils étaient simultanés. Chaque paramètre VarBind DOIT être limité à 65535 octets;
- cet objet DOIT être traité avant tout nuplet TLV de type 28 présent dans le fichier de configuration soit traité.

7.4.4.1.6 Objet de base MIB en protocole SNMP avec extension de longueur

Cet objet permet de régler des objets arbitraires de base MIB en protocole SNMP par le processus d'enregistrement TFTP, où la valeur est une variable d'association (VarBind) du protocole SNMP, comme défini dans [RFC 3416]. La valeur VarBind est codée conformément aux règles de codage de base en notation ASN.1, exactement comme si elle faisait partie d'une requête SNMP de mise à jour (Set).

Type	Longueur	Valeur
28	Variable	variable d'association

Le dispositif PS DOIT traiter la variable d'association, contenue dans un nuplet TLV de type 28, comme si elle faisait partie d'une requête SNMP de mise à jour (Set) avec les précautions suivantes:

- il DOIT traiter la requête comme étant entièrement autorisée (il ne peut pas la refuser pour absence de privilège);
- les dispositions de commande en écriture SNMP (voir le paragraphe précédent) ne s'appliquent pas;

- aucune réponse SNMP n'est produite par le dispositif PS;
- cet objet PEUT être répété avec différentes valeurs VarBind afin de mettre à jour (Set) un certain nombre d'objets de base MIB. Toutes les mises à jour SNMP (Set) contenues dans un fichier de configuration, qui apparaissent à l'intérieur de nuplets TLV de type 28, DOIVENT être traitées comme si elles étaient simultanées. Chaque valeur VarBind DOIT être limitée à 65 535 octets.

7.4.4.1.7 Certificat de vérification de code de constructeur

Certificat de vérification de code de constructeur (M-CVC) pour le téléchargement sécurisé de logiciel. Voir § 11.8.4.4.2, "Initialisation du réseau".

Type	Longueur	Valeur
32	Variable	Certificat CVC du constructeur (notation ASN.1 codée en règles DER)

7.4.4.1.8 Certificat de vérification de code de cosignataire

Certificat de vérification de code de cosignataire (C-CVC) pour le téléchargement sécurisé de logiciel. Voir § 11.8.4.4.2, "Initialisation du réseau".

Type	Longueur	Valeur
33	Variable	Certificat CVC de cosignataire (notation ASN.1 codée en règles DER)

7.4.4.1.9 Valeur de démarrage SNMPv3

(Voir § C.1.2.8, DOCSIS 1.1 – RFI Specification, SP-RFIv1.1-I09-020830.)

Les éléments de services de portail conformes DOIVENT comprendre le nuplet TLV suivant avec ses sous-éléments et être capables d'ouvrir l'accès SNMPv3 aux services de portail, que ceux-ci fonctionnent en mode d'accès NmAccess ou en mode de coexistence (voir § 6.3.3, "Description du système de portail CMP" et § 6.3.3.1.4.2, "Exigences relatives au mode de gestion de réseau").

Type	Longueur	Valeur
34	n	Composite

Jusqu'à cinq de ces objets peuvent être inclus dans le fichier de configuration. Chacun de ces objets provoque l'adjonction d'une nouvelle rangée dans les tables usmDHKickstartTable et usmUserTable et la production d'un nombre public d'agent pour ces rangées.

7.4.4.1.9.1 Nom de sécurité de démarrage SNMPv3

Type	Longueur	Valeur
34.1	2-16	Nom de sécurité codé en caractères UTF8

Pour le jeu de caractères ASCII, les codages UTF8 et ASCII sont identiques. Normalement, ce codage sera spécifié comme étant un des utilisateurs du modèle USM intégré dans le système IPCable2Home, p. ex. "CHAdministrator".

Le nom de sécurité n'est PAS terminé par zéro, ce qui est signalé dans la table usmDHKickStartTable comme étant un nom usmDHKickStartSecurityName et dans la table usmUserTable comme étant un nom usmUserName et un nom usmUserSecurityName.

7.4.4.1.9.2 Nombre public de gestionnaire de démarrage SNMPv3

Type	Longueur	Valeur
34.2	n	Nombre public à codage de Diffie-Helman du gestionnaire, exprimé comme une chaîne d'octets.

Ce nombre est le nombre public à codage de Diffie-Helman déduit d'un nombre aléatoire produit de façon privée (par le gestionnaire ou par l'opérateur) et transformé conformément à [RFC 2786]. Ce nombre est signalé dans la table usmDHKickStartTable comme faisant partie de l'objet usmKickstartMgrPublic. Quand il est combiné avec l'objet signalé dans la même rangée comme faisant partie de l'objet usmKickstartMyPublic, ce nombre peut servir à calculer les clés dans la rangée correspondante de la table usmUserTable.

7.4.4.1.10 Récepteur de notification SNMP

Type	Longueur	Valeur
38	n	Composite

Cet élément de fichier de configuration du dispositif PS spécifie une station de gestion de réseau qui va recevoir des notifications à partir du dispositif PS quand celui-ci est en mode de gestion de réseau par "coexistence". Ce nuplet TLV (38) comporte plusieurs sous-champs TLV à l'intérieur de l'élément de fichier de configuration par nuplets TLV. Jusqu'à 10 de ces éléments peuvent être inclus dans le fichier de configuration du dispositif PS. Le paragraphe 6.3.3.1.4.6, "Mappage des champs de nuplet TLV contenus dans des rangées créées de table SNMPv3", donne des détails sur la façon dont cet élément du fichier de configuration est mappé dans les tables fonctionnelles SNMPv3.

Tous les champs à octets multiples de ce sous-TLV DOIVENT être placés dans l'ordre des octets du réseau.

7.4.4.1.10.1 Sous-TLV 38.1 – Adresse IP du récepteur de préinterruptions

Adresse IPv4 du récepteur de préinterruptions, en binaire.

Type	Longueur	Valeur
38.1	4	Adresse IP

7.4.4.1.10.2 Sous-TLV 38.2 – Numéro de port UDP du récepteur de préinterruptions

Numéro de port UDP du récepteur de préinterruptions, en binaire.

Type	Longueur	Valeur
38.2	2	Port UDP

Si ce sous-TLV n'est pas présent dans un fichier de configuration, la valeur par défaut 162 est utilisée.

7.4.4.1.10.3 Sous-TLV 38.3 – Type de préinterruption émis par le dispositif PS (Note 2)

Type de préinterruption.

Type	Longueur	Valeur
38.3	2	Type de préinterruption

Le dispositif PS DOIT prendre en charge les valeurs suivantes de type de préinterruption:

1 = message TRAP du protocole SNMPv1 dans un paquet SNMPv1

2 = message TRAP du protocole SNMPv2c dans un paquet SNMPv2c

3 = message INFORM du protocole SNMP dans un paquet SNMPv2c

4 = message TRAP du protocole SNMPv2c dans un paquet SNMPv3

5 = message INFORM du protocole SNMP dans un paquet SNMPv3

7.4.4.1.10.4 Sous-TLV 38.4 – Temporisation

Temporisation, en milliseconds, utilisée pour envoyer les messages INFORM du protocole SNMP.

Type	Longueur	Valeur
38.4	2	0-65 535

7.4.4.1.10.5 Sous-TLV 38.5 – Réessais

Nombre de réessais d'envoi d'un message INFORM, après l'avoir envoyé une première fois.

Type	Longueur	Valeur
38.5	2	0-65 535

7.4.4.1.10.6 Sous-TLV 38.6 – Paramètres de filtrage de notification

Type	Longueur	Valeur
38.6	n	OID de filtre

Où n est la longueur de l'identificateur d'objet à codage ASN.1.

Il s'agit d'un identificateur d'objet (OID) de filtre formaté en notation ASN.1, de valeur snmpTrapOID, qui identifie les notifications à envoyer au récepteur de notification. Cette notification sera envoyée avec tout ce qu'elle recouvre.

Si ce sous-TLV n'est pas présent, le récepteur de notification doit recevoir toutes les notifications produites par l'agent SNMP.

7.4.4.1.10.7 Sous-TLV 38.7 – Nom de sécurité à utiliser lors de l'envoi d'une notification SNMPv3

Type	Longueur	Valeur
38.7	2-16	Nom de sécurité codé en format UTF8

Ce sous-TLV n'est pas requis pour les préinterruptions de type = 1, 2, ou 3. Le dispositif PS DOIT ignorer le sous-TLV 38.7 si le type de préinterruption contenu dans le sous-TLV 38.3 est 1, 2, ou 3. Si le sous-TLV 38.7 n'est pas fourni avec un préinterruption de type 4 ou 5, le dispositif PS DOIT envoyer la notification SNMPv3 avec le niveau de sécurité noAuthNoPriv au moyen du nom de sécurité "@PSconfig". (Note 2)

Nom de sécurité

Nom de sécurité SNMPv3 à utiliser lors de l'envoi d'une notification SNMPv3. Il n'est utilisé que si le type de préinterruption est réglé à 4 ou 5. Il DOIT s'agir d'un nom spécifié dans un nuplet TLV de fichier de configuration de type 34 en tant que partie de la procédure de démarrage DH (Diffie-Helman). Les notifications DOIVENT être envoyées au moyen des clés d'authentification et de confidentialité calculées par le dispositif PS pendant la procédure de démarrage DH.

Notes aux § 7.4.4.1.10.x:

NOTE 1 – Dès réception de l'un de ces éléments TLV, le dispositif PS DOIT créer des entrées dans les tables suivantes afin de provoquer la transmission de préinterruption recherchée: snmpNotifyTable, snmpTargetAddrTable, snmpTargetParamsTable, snmpNotifyFilterProfileTable, snmpNotifyFilterTable, snmpCommunityTable, usmUserTable, vacmSecurityToGroupTable, vacmAccessTable et vacmViewTreeFamilyTable

NOTE 2 – Type de préinterruption: la chaîne communautaire pour les préinterruptions dans les paquets SNMPv1 et v2 DOIT être "public". Le nom de sécurité dans les messages TRAP et INFORM des paquets SNMPv3 où aucun nom de sécurité n'a été spécifié DOIT être "@PSconfig", auquel cas le niveau de sécurité DOIT être NoAuthNoPriv.

NOTE 3 – Identificateur OID de filtre: le protocole SNMPv3 permet la spécification des identificateurs OID qui sont à envoyer à un récepteur de préinterruptions. L'identificateur OID de filtre situé dans l'élément de configuration spécifie l'identificateur OID de la racine d'un sous-arbre de filtre de préinterruption. Tous les messages TRAP ayant un OID de préinterruption contenu dans ce sous-arbre de filtre de préinterruption DOIVENT être envoyés au récepteur de préinterruptions.

NOTE 4 – Le fichier de configuration du dispositif PS est autorisé à contenir également des éléments TLV de base MIB (TLV-28) qui créent des entrées dans l'une quelconque des 10 tables énumérées dans la Note 1. Le dispositif PS DOIT ignorer les éléments TLV de base MIB qui utilisent les colonnes d'indice qui commencent par les caractères "@PSconfig".

7.4.4.1.11 Informations propres au vendeur

Si des informations propres au vendeur sont fournies aux services de portail, elles DOIVENT être codées dans le champ d'informations propres au vendeur (VSIF, *vendor-specific information field*) (code 43) au moyen du champ d'identificateur de vendeur afin de spécifier quels nuplets TLV s'appliquent à quels produits de vendeur. Un champ VSIF correctement formé contient un seul sous-TLV d'identificateur de vendeur (code 43.1) en tant que premier sous-TLV. Le dispositif PS DOIT rejeter le fichier de configuration PS si un quelconque nuplet TLV de champ VSIF (type 43) n'est pas correctement formé.

Un fichier de configuration PS peut avoir de multiples champs VSIF contenant différents sous-TLV ou le même sous-TLV d'identificateur de vendeur. Le dispositif PS ne traitera que les champs VSIF dont le sous-TLV d'identificateur de vendeur est concordant et il ignorera les champs VSIF dont les sous-TLV de vendeur ne concordent pas. Il est permis d'ajouter des sous-types propres au vendeur après le type 43.1.

Type	Longueur	Valeur
43	N	réglages propres au vendeur

Sous-TLV 43.1 – Type d'identificateur de vendeur

Identification de vendeur spécifiée par les trois octets de l'identificateur unique d'organisation (OUI, *organization unique identifier*) du vendeur PS.

Type	Longueur	Valeur
43.1	3	v1, v2, v3

7.4.4.1.12 Vérification d'intégrité de message PS (vérification MIC de PS)

Type	Longueur	Valeur
53	20	Hachage SHA sur 160 bits (20 octets)

Ce paramètre contient un hachage (vérification MIC de PS) calculé par l'algorithme de hachage sécurisé (SHA-1) défini dans le document NIST, FIPS PUB 180-1: Secure Hash Standard, avril 1995. Ce nuplet TLV n'est utilisé que dans le fichier de configuration, immédiatement avant le marqueur de fin de données.

7.4.4.1.13 Marqueur de fin de données

Marqueur spécial pour la fin des données. Il n'a aucun champ de longueur ou de valeur.

Type	Longueur	Valeur
255	---	---

7.4.4.2 Exigences relatives au déclenchement de configuration BPSC

Le transfert du fichier de configuration vers le dispositif PS à partir du serveur TFTP ou HTTPS situé dans le réseau de données par câble est lancé par un événement désigné par le terme de

déclencheur. Les exigences relatives au déclenchement du transfert d'un fichier de configuration du dispositif PS ou de configuration du pare-feu à partir d'un serveur TFTP ou HTTPS vers le dispositif PS sont données ci-après.

Le mode de déclenchement du téléchargement du fichier de configuration du dispositif PS dépend du mode de préconfiguration dans lequel le dispositif PS est en train de fonctionner. Le portail CMP DOIT lire la valeur de l'objet cabhPsDevProvMode (voir § 7.3.3.2.4) avant d'initialiser un téléchargement du fichier de configuration du dispositif PS. La méthode de déclenchement du téléchargement du fichier de configuration du pare-feu ne dépend pas du mode de préconfiguration.

7.4.4.2.1 Déclenchement du téléchargement du fichier de configuration du dispositif PS dans le mode de préconfiguration DHCP

Si le dispositif PS reçoit l'adresse du serveur TFTP ou HTTPS dans le champ 'siaddr' et le nom du fichier de configuration du dispositif PS dans le champ 'file' du message DHCP ACK, ET si la valeur de l'objet de base MIB cabhPsDevProvState = inProgress(2), le dispositif PS DOIT combiner l'adresse du serveur et le nom du fichier de configuration du dispositif PS de façon à former une valeur codée comme une adresse URL et DOIT écrire cette valeur dans l'objet cabhPsDevProvConfigFile de l'objet de base MIB PsDev. Le dispositif PS DOIT utiliser le format suivant pour la valeur, codée comme une adresse URL, de l'adresse IP du serveur TFTP et du nom du fichier de configuration du dispositif PS:

tftp://adresse_IPv4_du_serveur_TFTP/chemin_complet_du_fichier_deconfiguration_PS/Nom_du_fichier_de_configuration_PS

Le dispositif PS DOIT utiliser le format suivant pour la valeur, codée comme une adresse URL, de l'adresse IP du serveur HTTPS et du nom du fichier de configuration du dispositif PS:

https://adresse_IPv4_du_serveur_HTTPS/chemin_complet_du_fichier_de_configuration_PS/Nom_du_fichier_de_configuration_PS

Le téléchargement du fichier de configuration du dispositif PS, par un dispositif PS fonctionnant en mode de préconfiguration DHCP, est déclenché par la présence de l'emplacement du fichier de configuration du dispositif PS (adresse IP du serveur TFTP ou HTTPS) et par la présence de son nom dans le message DHCP envoyé aux services de portail (client CDC) par le serveur DHCP dans le réseau câblé. Voir § 7.3.3.2.4, "Exigences relatives au client CDC".

Si le dispositif PS doit fonctionner en mode de préconfiguration DHCP (ce qui est indiqué par la valeur de l'objet cabhPsDevProvMode), après réception par le dispositif PS (client CDC) d'un message DHCP ACK provenant du serveur DHCP dans le réseau câblé et que l'adresse IP dans le champ 'siaddr' ne corresponde pas à la première adresse IP dans l'option DHCP 72, ET si la valeur de l'objet de base MIB cabhPsDevProvState = inProgress(2), alors le dispositif PS DOIT envoyer une requête GET du protocole TFTP au serveur identifié dans le champ 'siaddr' du message DHCP afin de télécharger le fichier de configuration.

Si le dispositif PS doit fonctionner en mode de préconfiguration DHCP (ce qui est indiqué par la valeur de l'objet cabhPsDevProvMode) après réception par le dispositif PS (client CDC) d'un message DHCP ACK provenant du serveur DHCP dans le réseau câblé et que l'adresse IP dans le champ 'siaddr' corresponde à la première adresse IP dans l'option DHCP 72 et que l'objet de base MIB cabhPsDevTodSyncStatus ait une valeur égale à '1' (accès au serveur ToD réussi), alors le dispositif PS DOIT établir une session de sécurité TLS comme défini dans le § 11 et envoyer une requête GET du protocole http au serveur identifié dans le champ 'siaddr' du message DHCP, afin de télécharger le fichier de configuration.

Si le dispositif PS doit fonctionner en mode de préconfiguration DHCP (ce qui est indiqué par la valeur de l'objet cabhPsDevProvMode) après réception par le dispositif PS (client CDC) d'un message DHCP ACK provenant du serveur DHCP dans le réseau câblé et que l'adresse IP dans le champ 'siaddr' corresponde à la première adresse IP dans l'option DHCP 72 et que l'objet de base MIB cabhPsDevTodSyncStatus ait une valeur égale à '2' (échec d'accès au serveur ToD), le

dispositif PS DOIT attendre que l'objet de base MIB cabhPsDevTodSyncStatus ait une valeur égale à '1' (accès au serveur ToD réussi) avant d'établir une session de sécurité TLS comme défini dans le § 11 et d'envoyer une requête GET du protocole http au serveur identifié dans le champ 'siaddr' du message DHCP, afin de télécharger le fichier de configuration.

La modification de l'objet cabhPsDevProvConfigFile NE DOIT PAS déclencher le téléchargement, par un dispositif PS fonctionnant en mode de préconfiguration DHCP, d'un fichier de configuration. Un dispositif PS fonctionnant en mode de préconfiguration DHCP DOIT traiter l'objet cabhPsDevProvConfigFile comme étant en lecture seule.

7.4.4.2.2 Déclenchement du téléchargement du fichier de configuration du dispositif PS dans le mode de préconfiguration SNMP

Si le dispositif PS doit fonctionner en mode de préconfiguration SNMP (ce qui est indiqué par la valeur de l'objet cabhPsDevProvMode), le téléchargement du fichier de configuration du dispositif PS NE DOIT PAS survenir avant l'achèvement du processus d'établissement SNMPv3 (voir § 11.4, "Messagerie de gestion sécurisée envoyée au dispositif PS", pour des détails sur le processus d'établissement SNMP).

Si le dispositif PS doit fonctionner en mode de préconfiguration SNMP (ce qui est indiqué par la valeur de l'objet cabhPsdevProvMode), l'élément de services de portail NE DOIT PAS lancer un téléchargement du fichier de configuration du dispositif PS si l'objet de base MIB cabhPsDevTodSyncStatus a une valeur égale à '2' (échec d'accès au serveur ToD).

Si le dispositif PS doit fonctionner dans le mode de préconfiguration SNMP et si la durée écoulée depuis qu'il a envoyé le message INFORM d'enrôlement de préconfiguration décrit dans le Tableau 13-3, qui fait suite à l'authentification du centre KDC, est égale à la valeur de l'objet cabhPsDevPreconfigurationTimer ET si le dispositif PS n'a pas été déclenché de façon à importer par téléchargement un fichier de configuration PS, alors ce dispositif PS DOIT régler la valeur de l'objet cabhPsDevProvState à pass(1) et continuer le processus de préconfiguration pour le mode de préconfiguration SNMP comme décrit dans le § 13.4. Si le dispositif PS doit fonctionner dans le mode de préconfiguration SNMP et est déclenché de façon à importer par téléchargement un fichier de configuration PS quand la durée écoulée depuis qu'il a émis le message INFORM d'enrôlement de préconfiguration est inférieure à la valeur de l'objet cabhPsDevPreconfigurationTimer, alors le dispositif PS NE DOIT PAS régler la valeur de l'objet cabhPsDevProvState à pass(1) avant qu'il ait réussi à importer par téléchargement et à traiter le fichier de configuration PS spécifié. Si le dispositif PS doit fonctionner dans le mode de préconfiguration SNMP et a été déclenché de façon à importer par téléchargement un fichier de configuration PS, ce dispositif PS DOIT régler la valeur de l'objet cabhPsDevProvState à pass(1) quand il réussit à importer par téléchargement et à traiter le fichier de configuration PS.

Une fois que le dispositif PS, fonctionnant en mode de préconfiguration SNMP (ce qui est indiqué par la valeur de l'objet cabhPsDevProvMode), envoie une requête TFTP afin de télécharger un fichier de configuration du dispositif PS (sous réserve des conditions décrites dans d'autres exigences ci-dessous), le dispositif PS DOIT achever la phase de téléchargement. Quand le dispositif PS (portail CMP) a correctement téléchargé le fichier de configuration du dispositif PS demandé, il DOIT traiter ce fichier avant d'envoyer une requête TFTP afin de recevoir un autre fichier de configuration du dispositif PS.

Le dispositif PS DOIT essayer de télécharger et de traiter le fichier de configuration dont le nom et l'adresse sont spécifiés dans l'objet cabhPsDevProvConfigFile quand il reçoit une requête Set (mise à jour) du protocole SNMP pour l'objet cabhPsDevProvConfigFile, si les conditions suivantes sont vraies:

- le dispositif PS doit fonctionner en mode de préconfiguration SNMP;
- l'objet de base MIB cabhPsDevTodSyncStatus a une valeur égale à '1' (accès au serveur ToD réussi);

- cabhPsDevProvConfigFileStatus = idle(1).

Le format de l'objet cabhPsDevProvConfigFile DOIT être une adresse IP de serveur TFTP codée sous forme d'adresse URL et un nom de fichier de configuration.

Si le dispositif PS (portail CMP) fonctionnant en mode de préconfiguration SNMP reçoit une requête SNMP de mise à jour (Set) à partir du système NMS afin de mettre à jour la valeur des objets cabhPsDevProvConfigFile et cabhPsDevProvConfigFileStatus à la valeur = busy(2), ou si l'objet cabhPsDevProvConfigHash ne possède pas de valeur valide, alors le dispositif PS DOIT ignorer la requête de mise à jour.

7.4.4.2.3 Déclencheur du fichier de configuration du pare-feu

Le téléchargement du fichier de configuration du pare-feu est déclenché quand la valeur servant à mettre à jour (SET) l'objet cabhSec2FwPolicyFileURL MIB, soit par le fichier de configuration du dispositif PS ou par une requête SET (mise à jour) du protocole SNMP, est différente de la valeur de l'objet de base MIB cabhSec2FwPolicySuccessfulFileURL. Si la valeur servant à mettre à jour (SET) l'objet de base MIB cabhSec2FwPolicyFileURL, soit par le fichier de configuration du dispositif PS ou par une requête SET (mise à jour) du protocole SNMP, est la même que celle de l'objet de base MIB cabhSec2FwPolicySuccessfulFileURL, le téléchargement du fichier de configuration du pare-feu NE DOIT PAS être déclenché.

Quand une importation par téléchargement a été déclenchée, le dispositif PS DOIT utiliser le préfixe de la valeur de l'objet de base MIB cabhSecFwPolicyFileURL afin de déterminer s'il y a lieu d'utiliser une session de protocole TFTP (tftp://) ou TLS (https://) comme défini au § 11 pour l'importation par téléchargement du fichier de configuration du pare-feu.

7.4.4.2.4 Fonctionnement après déclenchement

Une fois déclenché, le dispositif PS DOIT utiliser un client TFTP selon [RFC 1350] et [RFC 2348] ou un client http selon [RFC 2616] afin de télécharger les fichiers de configuration.

Un mécanisme de signalisation est nécessaire de façon à informer l'entité gestionnaire du fait que le dispositif PS est actuellement en train de traiter un fichier de configuration. L'objet de base MIB cabhPsDevProvConfigFileStatus de la base MIB PsDev est défini de façon à jouer le rôle de ce mécanisme de signalisation.

Si un dispositif PS n'est pas déjà en train de demander, de télécharger, ou de traiter un fichier de configuration, il DOIT régler l'objet cabhPsDevProvConfigFileStatus à la valeur = idle(1). Quand le dispositif PS a envoyé une requête TFTP pour un fichier de configuration spécifié dans l'objet cabhPsDevProvConfigFile, il DOIT régler l'objet cabhPsDevProvConfigFileStatus à la valeur = busy(2). Quand le dispositif PS achève le traitement du fichier de configuration du dispositif PS, le dispositif PS DOIT régler l'objet cabhPsDevProvConfigFileStatus à la valeur = idle(1).

Une fois déclenché afin de télécharger un fichier de configuration, l'élément de services de portail DOIT continuer à essayer de télécharger le fichier de configuration spécifié à partir de l'emplacement spécifié jusqu'à ce que ce fichier de configuration ait été correctement téléchargé et que le hachage ait été correctement calculé comme décrit dans le § 7.4.4.3, "Exigences relatives à la vérification du fichier de configuration et à l'authentification du mode de préconfiguration SNMP". Le dispositif PS DOIT utiliser une temporisation adaptative pour les protocoles TFTP et HTTPS fondée sur un temps exponentiel d'attente de données binaires comme décrit ci-dessous, si la première tentative n'a pas réussi, jusqu'à ce que le dispositif PS reçoive correctement le fichier demandé provenant du serveur situé dans le réseau de données par câble:

- chaque réessai a lieu 2^n seconde(s) après la précédente tentative, où le compteur de réessais du fichier de configuration du dispositif PS ou du pare-feu a la valeur n = [1, 2, 3, 4, ou 5];

- n = 1 pour le premier réessai, puis est incrémenté d'une unité pour chaque nouvelle tentative jusqu'à ce que n = 5;
- si le dispositif PS n'obtient pas correctement le fichier de configuration du dispositif PS demandé après la tentative avec n = 5, n doit être réinitialisé à 1 et le dispositif PS doit relancer le processus d'acquisition de l'adresse IP du réseau WAN-Man par protocole DHCP;
- si le dispositif PS n'obtient pas correctement le fichier demandé de configuration du pare-feu après la tentative avec n = 5, n doit être réinitialisé à 1 et le dispositif PS DOIT continuer son fonctionnement normal, c'est-à-dire que le dispositif PS ne doit pas relancer le processus d'acquisition de l'adresse IP du réseau WAN-Man.

Le dispositif PS ne DOIT échanger de messages TFTP et HTTPS que par l'interface PS WAN-Man. Le dispositif PS DOIT ignorer tout fichier de configuration non reçu par l'interface PS WAN-Man.

Quand le téléchargement du fichier de configuration est achevé et que le fichier de configuration est correctement authentifié comme décrit dans le § 7.4.4.3, "Exigences relatives à la vérification du fichier de configuration et à l'authentification du mode de préconfiguration SNMP", le dispositif PS DOIT traiter les éléments TLV contenus dans le fichier comme défini ci-dessous. Voir, au § 7.4.4.4, "Exigences relatives au traitement du fichier de configuration et à la signalisation des états", des détails concernant le traitement des erreurs et la production d'événements au cours du traitement du fichier de configuration.

Le dispositif PS DOIT utiliser les paramètres extraits du fichier de configuration afin de mettre à jour (Set) les objets gérés dans la base de données PS. Ce processus est fonctionnellement équivalent à une opération de requête SET (mise à jour) du protocole SNMP, mais il ne dépend pas de l'utilisateur ou des autorisations d'accès fondées sur le point de vue. Le dispositif PS DOIT inconditionnellement mettre à jour dans la base de données PS les objets gérés correspondant à des identificateurs OID reconnus.

Le dispositif PS DOIT convertir les éléments TLV-27 du fichier de configuration en une seule unité PDU du protocole SNMP contenant (n) composants de base MIB d'identificateur OID ou d'instance et de valeur (paramètres 'VarBind' du protocole SNMP) et DOIT convertir les éléments TLV-28 du fichier de configuration en une seule unité PDU du protocole SNMP contenant (n) composants de base MIB d'identificateur OID ou d'instance et de valeur (paramètres 'VarBind' du protocole SNMP). Conformément au document [RFC 3416], l'unique unité PDU du protocole SNMP produite par un fichier de configuration TLV-27 sera traitée "comme si elle était simultanée", l'unique unité PDU du protocole SNMP produite par un fichier de configuration TLV-28 sera traitée "comme si elle était simultanée" et le dispositif PS DOIT avoir un comportement cohérent, sans tenir compte de l'ordre dans lequel les éléments TLV-28 ou TLV-27 apparaissent dans le fichier de configuration ou dans une unité PDU du protocole SNMP. L'exigence relative à l'unique unité PDU du protocole SNMP produite par un fichier de configuration est compatible avec les comportements des paquets d'unité PDU du protocole SNMP reçus à partir d'un gestionnaire SNMP: l'ordre des valeurs 'VarBind' des unités PDU du protocole SNMP n'a pas d'importance et aucune limite MAX n'est fixée pour ces unités. Une fois qu'une unique unité PDU du protocole SNMP est construite, le dispositif PS la traite et détermine l'acceptation/le rejet de la configuration des services de portail sur la base des règles de traitement du fichier de configuration, décrites dans le § 7.4.4.4, "Exigences relatives au traitement du fichier de configuration et à la signalisation des états". Lors du traitement de l'unité PDU du protocole SNMP, le dispositif PS DOIT prendre en charge l'objet CreateAndGo pour la création de rangée.

Le dispositif PS DOIT mettre à jour la longueur du fichier de configuration du dispositif PS dans l'objet de base MIB cabhPsDevProvConfigFileSize.

Le dispositif PS DOIT mettre à jour le nombre d'éléments TLV traités (c'est-à-dire ceux qui sont destinés à changer la configuration des services de portail selon leur propre champ de valeur) et le

nombre d'éléments TLV ignorés (c'est-à-dire ceux qui sont destinés à changer la configuration des services de portail selon leur propre champ de valeurs mais qui n'y réussissent pas) à partir d'un fichier de configuration du dispositif PS, dans les objets de base MIB cabhPsDevProvConfigTLVProcessed et cabhPsDevConfigTLVRejected, respectivement[1]. Les types de paramètre de configuration 255 (marqueur de fin de données), 53 (vérification MIC du dispositif PS), 0 (réglage de configuration du bourrage) et les paires de champs de type et longueur qui correspondent à des sous-champs TLV ne spécifient pas de valeurs dans les champs de valeur destinés à changer la configuration des services de portail et donc NE DOIVENT PAS être comptés dans les valeurs des objets cabhPsDevProvConfigTLVProcessed et cabhPsDevConfigTLVRejected.

7.4.4.3 Exigences relatives à la vérification du fichier de configuration et à l'authentification du mode de préconfiguration SNMP

L'algorithme servant à authentifier le fichier de configuration dépend du mode de préconfiguration dans lequel le dispositif PS doit fonctionner (voir § 5.5, "Modes de fonctionnement IPCable2Home"). Le dispositif PS prend en charge deux modes de préconfiguration: le mode de préconfiguration DHCP et le mode de préconfiguration SNMP. Deux méthodes d'authentification du fichier de configuration sont prises en charge dans le mode de préconfiguration DHCP, selon les informations reçues dans le champ 'siaddr' du message DHCP ACK.

Les paragraphes ci-après décrivent les algorithmes de sécurité et exigences nécessaires pour vérifier le hachage du fichier de configuration selon le mode de préconfiguration de l'élément de services de portail, lequel DOIT prendre en charge les deux algorithmes de sécurité spécifiés dans les § 7.4.4.3.1, "Vérification du fichier de configuration du dispositif PS en mode de préconfiguration DHCP" et 7.4.4.3.2, "Algorithme d'authentification du fichier de configuration du dispositif PS en mode de préconfiguration SNMP".

7.4.4.3.1 Vérification du fichier de configuration du dispositif PS en mode de préconfiguration DHCP

Lorsqu'il fonctionne en mode de préconfiguration DHCP, le dispositif PS utilise une vérification par hachage du fichier de configuration, ou authentifie le message dans lequel le fichier est transféré, selon la configuration du système de préconfiguration du câblo-opérateur.

Le dispositif PS DOIT effectuer la vérification suivante du fichier de configuration sur la base du hachage SHA-1:

1) quand le générateur de fichiers de configuration du système de préconfiguration crée un nouveau fichier de configuration du dispositif PS ou modifie un fichier existant, le générateur de fichiers de configuration va créer un hachage SHA-1 du contenu du fichier de configuration du dispositif PS, considéré comme une chaîne d'octets. Le marqueur de fin de données et tout bourrage lui faisant suite ne sont pas inclus dans le calcul de hachage;
2) le générateur de fichiers de configuration ajoute la valeur de hachage, calculée au cours de l'étape 1, au fichier de configuration du dispositif PS en tant que dernier réglage par nuplet TLV (immédiatement avant le marqueur de fin de données) au moyen d'un nuplet TLV de type 53. Le fichier de configuration du dispositif PS est alors mis à la disposition du serveur TFTP approprié;
3) l'élément de services de portail télécharge le fichier de configuration du dispositif PS;
4) le dispositif PS DOIT mettre à jour l'objet cabhPsDevProvConfigHash de base MIB avec la valeur de hachage à partir du hachage de TLV créé dans les étapes 1 et 2;

---

[1] Selon ces définitions, un élément TLV qui ne configure pas correctement le dispositif PS est compté deux fois: une fois par chacun des objets cabhPsDevProvConfigTLVProcessed et cabhPsDevProvConfigTLVRejected. Un élément TLV qui configure correctement le dispositif PS n'est compté que par l'objet cabhPsDevProvConfigTLVProcessed.

5) l'élément de services de portail DOIT calculer un hachage SHA-1 sur le contenu du fichier de configuration du dispositif PS à l'exception du hachage de TLV (servant à configurer l'objet cabhPsDevProvConfigHash MIB), du marqueur de fin de données et de tout bourrage qui suit. Si le hachage calculé et la valeur de l'objet cabhPsDevProvConfigHash de base MIB sont identiques, l'intégrité du fichier de configuration du dispositif PS est vérifiée et le fichier de configuration DOIT être traité; sinon, le fichier DOIT être rejeté.

7.4.4.3.2 Algorithme d'authentification du fichier de configuration du dispositif PS en mode de préconfiguration SNMP

La procédure de vérification du hachage du fichier de configuration du dispositif PS par l'élément de services de portail en mode de préconfiguration SNMP est reproduite ci-dessous:

1) quand le générateur de fichiers de configuration du système de préconfiguration crée un nouveau fichier de configuration du dispositif PS ou modifie un fichier existant, le générateur de fichiers de configuration crée un hachage SHA-1 du contenu entier du fichier de configuration du dispositif PS, considéré comme une chaîne d'octets. Le marqueur de fin de données et tout bourrage lui faisant suite ne sont pas inclus dans le calcul de hachage;
2) le système NMS envoie la valeur de hachage calculée au cours de l'étape 1 vers l'élément de services de portail par requête SET (mise à jour) du protocole SNMP. Le dispositif PS met à jour son objet cabhPsDevProvConfigHash de base MIB avec la nouvelle valeur;
3) le système NMS envoie le nom et l'emplacement du fichier de configuration du dispositif PS par requête SET (mise à jour) du protocole SNMP. Le dispositif PS met à jour son objet cabhPsDevProvConfigFile de base MIB avec la nouvelle valeur;
4) l'élément de services de portail télécharge le fichier nommé à partir du serveur TFTP configuré. Si le fichier de configuration du dispositif PS contient un nuplet TLV de type 53, le dispositif PS DOIT l'ignorer;
5) l'élément de services de portail DOIT calculer un hachage SHA-1 sur le contenu du fichier de configuration du dispositif PS à l'exception du nuplet TLV 53 s'il existe, du marqueur de fin de données et de tout bourrage qui suit. Si le hachage calculé et la valeur de l'objet cabhPsDevProvConfigHash de base MIB sont identiques, l'intégrité du fichier de configuration du dispositif PS est vérifiée et le fichier de configuration DOIT être traité; sinon, le fichier DOIT être rejeté.

7.4.4.3.3 Vérification du fichier de configuration du pare-feu

Le dispositif PS est tenu de vérifier le fichier de configuration du pare-feu comme décrit dans le présent paragraphe si ce fichier est offert en mode de préconfiguration SNMP ou en mode de préconfiguration DHCP sans l'utilisation du protocole HTTPS/TLS comme défini dans le § 11.9, "Sécurité du fichier de configuration du dispositif PS en mode de préconfiguration DHCP".

Si le fichier de configuration du pare-feu a été téléchargé sans l'utilisation du protocole http/TLS, le dispositif PS DOIT suivre la procédure définie aux étapes 1 à 5 ci-dessous afin de vérifier l'intégrité du fichier de configuration du pare-feu:

1) le générateur de fichiers de configuration du pare-feu va créer un hachage SHA-1 du contenu entier du fichier de configuration du pare-feu, considéré comme une chaîne d'octets;
2) le système de préconfiguration envoie la valeur de hachage calculée au cours de l'étape 1 à l'élément de services de portail d'une des deux façons suivantes:
   a) en modifiant l'objet cabhSec2FwPolicyFileHash de base MIB par un nuplet TLV de type 28 contenu dans le fichier de configuration du dispositif PS;
   b) en envoyant une requête Set (mise à jour) du protocole SNMP afin de mettre à jour l'objet cabhSec2FwPolicyHash de base MIB;

3) le système de préconfiguration envoie le nom et l'emplacement du fichier de configuration du pare-feu afin de déclencher le téléchargement du fichier de configuration du pare-feu d'une des deux façons suivantes:

   a) en modifiant l'objet cabhSec2FwPolicyFileURL de base MIB par un nuplet TLV de type 28 contenu dans le fichier de configuration du dispositif PS;

   b) en envoyant une requête Set (mise à jour) du protocole SNMP afin de mettre à jour l'objet cabhSec2FwPolicyURL de base MIB;

4) si l'objet cabhSecFwPolicyFileOperStatus n'a pas la valeur inProgress (1) et si la valeur servant à mettre à jour (Set) l'objet cabhSec2FwPolicyFileURL de base MIB est différente de la valeur de l'objet cabhSec2FwPolicySuccessfulFileURL de base MIB, alors l'élément de services de portail DOIT immédiatement télécharger le fichier nommé à partir du serveur configuré;

5) le dispositif PS DOIT calculer un hachage SHA-1 sur le contenu entier du fichier de configuration du pare-feu et comparer le hachage calculé au hachage représenté par la valeur de l'objet cabhSec2FwPolicyFileHash de base MIB. Si le hachage calculé et la valeur de l'objet cabhSec2FwPolicyFileHash de base MIB sont identiques, l'intégrité du fichier de configuration du pare-feu est vérifiée et le dispositif PS DOIT utiliser ce fichier de configuration du pare-feu afin de configurer le pare-feu; sinon le dispositif PS DOIT ignorer le fichier.

7.4.4.4 Exigences relatives au traitement du fichier de configuration et à la signalisation des états

Le dispositif PS DOIT signaler l'état et les conditions d'erreur du téléchargement du fichier de configuration au moyen du processus de signalisation des événements décrit dans le § 6.3.3.2, "Fonction de signalisation d'événement de portail CMP".

Le Tableau 7-15 identifie les modes de succès et d'échec qui pourraient être rencontrés lors du téléchargement et du traitement du fichier de configuration du dispositif PS, ainsi que l'action que le dispositif PS DOIT entreprendre quand il détecte ces modes.

Tableau 7-15/J.192 – Conditions de traitement du fichier de configuration

Condition	Action
TFTP échoué – requête Get envoyée, aucune réponse reçue	Signaler un événement (identificateur d'événement 68000500) et réessayer le transfert TFTP.
HTTPS échoué – requête Get envoyée, aucune réponse reçue ou échec de connexion au serveur HTTPS	Signaler un événement (identificateur d'événement 68002000) et réessayer le transfert HTTPS.
TFTP échoué – Fichier de configuration non trouvé	Signaler un événement (identificateur d'événement 68000600) et réessayer le transfert TFTP.
HTTPS échoué – Echec de la tentative de téléchargement du fichier de configuration et nombre maximal de réessais non dépassé	Signaler un événement (identificateur d'événement 68003000) et réessayer le transfert HTTPS.
TFTP échoué – Paquets dans le désordre	Signaler un événement (identificateur d'événement 68000700) et réessayer le transfert TFTP.
Téléchargement TFTP échoué – Echec de la tentative d'importation du fichier de configuration et nombre maximal admissible de réessais effectué	Signaler un événement (identificateur d'événement 68000900) et réinitialiser.
Téléchargement HTTPS échoué – Echec de la tentative d'importation du fichier de configuration et nombre maximal admissible de réessais effectué	Signaler un événement (identificateur d'événement 68003100) et réinitialiser.

Tableau 7-15/J.192 – Conditions de traitement du fichier de configuration

Condition	Action
Téléchargement du fichier de configuration réussi	Signaler un événement (identificateur d'événement 68001000 si le téléchargement a été effectué par TFTP (le protocole TLS n'a pas été utilisé) ou identificateur d'événement 68003200 si le téléchargement a été effectué par protocole HTTPS/TLS) et commencer la vérification ou l'authentification du fichier de configuration.
Echec de la vérification d'authentification du fichier de configuration	Signaler un événement (identificateur d'événement 68000800) et réinitialiser. Ne pas essayer de traiter le fichier.
Fichier de configuration est trop volumineux	Signaler un événement (identificateur d'événement 73040102) et réinitialiser. Ne pas essayer de traiter le fichier.
Absence de marqueur de fin de données	Signaler un événement (identificateur d'événement 73040102) et réinitialiser. Ne pas essayer de traiter le fichier.
Duplication de l'identificateur OID du nuplet TLV-27 ou TLV-28	Signaler un événement (identificateur d'événement 73040102), rejeter le fichier de configuration et réinitialiser. Sauvegarder toutes les valeurs d'objet qui existaient avant la tentative de traitement de ce mauvais fichier de configuration. Le dispositif PS n'est pas tenu de rétablir les objets de base MIB à la valeur qui leur avait été assignée avant la tentative de traitement du fichier de configuration si l'unique unité PDU SNMP créée à partir des paramètres TLV-27 a été activée. Voir le paragraphe relatif au fonctionnement après déclenchement.
Duplication des TLV-9, TLV-21, TLV-32, TLV-33 ou duplication des sous-TLV afin d'obtenir un seul nuplet TLV-34, TLV-38, TLV-43.	Signaler un événement (73040102), rejeter le fichier de configuration et réinitialiser. Sauvegarder tous les objets qui existaient avant la tentative de traitement de ce mauvais fichier de configuration.
Type reconnu mais mauvaise valeur, ou OID de TLV-27 ou TLV-28 valide mais mauvaise valeur de base MIB	Signaler un événement (identificateur d'événement 73040102), rejeter le fichier de configuration et réinitialiser. Sauvegarder toutes les valeurs d'objet qui existaient avant la tentative de traitement de ce mauvais fichier de configuration. Le dispositif PS n'est pas tenu de rétablir les objets de base MIB à la valeur qui leur avait été assignée avant la tentative de traitement du fichier de configuration si l'unique unité PDU SNMP créée à partir des paramètres TLV-27 a été activée. Voir le paragraphe relatif au fonctionnement après déclenchement.
Apparition d'un OID SNMP non reconnu	Ne pas tenir compte du TLV en cause et signaler un événement (identificateur d'événement 73040100). Continuer à traiter le fichier.
Champ de type non valide pour le dispositif PS	Ne pas tenir compte du TLV en cause et signaler un événement (identificateur d'événement 73040101). Continuer à traiter le fichier.

Voir dans l'Annexe B une liste d'événements y compris ceux qui sont énumérés dans le Tableau 7-15, ainsi que des informations sur la façon dont les événements sont rapportés.

7.4.4.4.1 Tentative infructueuse de téléchargement du fichier de configuration – Réessais par protocole TFTP ou HTTPS autorisés

Si le compteur de réessais du fichier de configuration du dispositif PS est inférieur à 5 et si la requête Get du protocole TFTP ou HTTPS arrive à expiration, ou si le fichier de configuration du dispositif PS n'est pas trouvé sur le serveur distant, ou si la requête Get du protocole TFTP ou HTTPS a échoué en raison de paquets dans le désordre, le dispositif PS DOIT mettre en fonctionnement le serveur CDS et le portail CNP, signaler l'événement approprié et réessayer de télécharger le fichier de configuration du dispositif PS conformément à l'algorithme de réessai décrit dans le § 7.4.4.2.4, "Fonctionnement après déclenchement".

Si le compteur de réessais du fichier de configuration du pare-feu est inférieur à 5 et si la requête Get du protocole TFTP ou http arrive à expiration, ou si le fichier de configuration du pare-feu n'est pas trouvé sur le serveur distant, ou si la requête Get du protocole TFTP ou http a échoué en raison de paquets dans le désordre, le dispositif PS DOIT continuer son fonctionnement normal, signaler l'événement approprié et réessayer de télécharger le fichier de configuration du pare-feu conformément à l'algorithme de réessai décrit dans le § 7.4.4.2.4, "Fonctionnement après déclenchement".

7.4.4.4.2 Tentative infructueuse de téléchargement du fichier de configuration – Réessais par protocole TFTP ou HTTPS épuisés

Si le compteur de réessais du fichier de configuration du dispositif PS est égal à 5 et si le dispositif PS n'a pas correctement téléchargé le fichier de configuration du dispositif PS, le dispositif PS DOIT signaler l'événement indiqué dans le Tableau 7-15, "Conditions de traitement du fichier de configuration", afin d'indiquer l'échec du processus de téléchargement du fichier de configuration du dispositif PS et libérer son adresse IP d'interface PS WAN-Man conformément au [RFC 2131] et relancer le processus d'acquisition de l'adresse IP du réseau WAN-Man par protocole DHCP.

Si le compteur de réessais du fichier de configuration du pare-feu est égal à 5 et si le dispositif PS n'a pas correctement téléchargé le fichier de configuration du dispositif PS, le dispositif PS DOIT signaler l'événement indiqué dans le Tableau 7-15, "Conditions de traitement du fichier de configuration", afin d'indiquer l'échec du processus de téléchargement du fichier de configuration du pare-feu et continuer son fonctionnement normal. Si le fichier de configuration du pare-feu n'est pas correctement téléchargé, le dispositif PS DOIT fonctionner comme il le faisait avant l'échec de la tentative de téléchargement du fichier de configuration du pare-feu.

7.4.4.4.3 Téléchargement réussi du fichier de configuration du dispositif PS

Un téléchargement réussi du fichier de configuration du dispositif PS est défini comme une réception complète et correcte par l'élément de services de portail du contenu du fichier de configuration du dispositif PS dans la période de temporisation du protocole TFTP et le calcul par le dispositif PS des valeurs de hachage pour le fichier de configuration du dispositif PS sans erreurs provenant de cette autorité calcul.

Si le dispositif PS télécharge correctement le fichier de configuration du dispositif PS, le dispositif PS DOIT remettre à zéro le compteur de réessais du fichier de configuration du dispositif PS et signaler l'événement indiqué par "Téléchargement TFTP réussi" dans la colonne 'Mode d'échec' du Tableau 7-15, "Conditions de traitement du fichier de configuration".

7.4.4.4.4 Echec du téléchargement du fichier de configuration du dispositif PS

En cas d'échec de la vérification du fichier de configuration du dispositif PS comme spécifié dans le § 7.4.4.3, "Exigences relatives à la vérification du fichier de configuration et à l'authentification du mode de préconfiguration SNMP", ou dans le § 11.9, "Sécurité du fichier de configuration du

dispositif PS en mode de préconfiguration DHCP", le dispositif PS DOIT arrêter le processus de préconfiguration, ignorer le fichier de configuration du dispositif PS, signaler l'événement approprié et relancer le processus d'acquisition d'adresse IP de réseau WAN-Man par protocole DHCP.

Si le fichier de configuration du dispositif PS ne contient aucun TLV marqueur de fin de données (TLV-255), aucun TLV de vérification MIC du dispositif PS (TLV-53), ou est trop volumineux pour être traité, le dispositif PS DOIT arrêter le processus de préconfiguration, ignorer le fichier de configuration du dispositif PS, signaler l'événement approprié et relancer le processus d'acquisition de l'adresse IP du réseau WAN-Man par protocole DHCP.

Si le fichier de configuration du dispositif PS contient des éléments en double TLV-27 ou TLV-28 ("en double" signifiant que deux ou plus de deux objets de base MIB en protocole SNMP ont un identificateur d'objet (OID) identique), le dispositif PS DOIT arrêter le processus de préconfiguration, ignorer le fichier de configuration du dispositif PS, signaler l'événement approprié et relancer le processus d'acquisition de l'adresse IP du réseau WAN-Man par protocole DHCP.

Si le fichier de configuration du dispositif PS contient un champ de type reconnu mais un mauvais champ de valeur ou un identificateur OID de TLV-27 ou TLV-28 valide mais une mauvaise valeur de base MIB, le dispositif PS DOIT arrêter le processus de préconfiguration, ignorer le fichier de configuration du dispositif PS, signaler l'événement approprié et relancer le processus d'acquisition de l'adresse IP du réseau WAN-Man par protocole DHCP.

Si le fichier de configuration du dispositif PS contient un champ de type reconnu ou un élément TLV-27 ou TLV-28 contenant un identificateur OID non reconnu, le dispositif PS DOIT ignorer ce TLV, signaler l'événement approprié et continuer le traitement du fichier de configuration du dispositif PS.

Si le dispositif PS effectue le traitement de l'unique unité PDU SNMP créée à partir du paramètre TLV-27 puis découvre des éléments TLV-28 en double ou avec une valeur erronée, ce dispositif PS n'est pas tenu de restaurer les objets de base MIB modifiés par le paramètre TLV-27 à leur valeur précédente, avant de rejeter le fichier de configuration, de signaler l'événement et de réinitialiser le dispositif PS.

7.4.4.4.5 Téléchargement rússi du fichieer de configuration du pare-feu

Un téléchargement réussi du fichier de configuration du pare-feu est défini comme une réception complète et correcte du fichier par l'élément de services de portail dans la période de temporisation TFTP ou HTTPS et après validation du fichier sans erreur comme défini par la procédure de vérification d'intégrité décrite dans le § 7.4.4.3, "Exigences relatives à la vérification du fichier de configuration et à l'authentification du mode de préconfiguration SNMP". Après que le dispositif PS a correctement téléchargé le fichier de configuration du pare-feu, le dispositif PS DOIT mettre à jour l'objet cabhSec2FwPolicySuccessfulFileURL de base MIB avec la même valeur que l'objet cabhSec2FwPolicyFileURL de base MIB.

Si le dispositif PS télécharge correctement le fichier de configuration du pare-feu, le dispositif PS DOIT réinitialiser le compteur de réessais du fichier de configuration du pare-feu à zéro et signaler l'ID d'événement 80013500 (voir le Tableau B.1, "Evénements définis pour IPCable2Home"). Après que le dispositif PS a correctement téléchargé et traité le fichier de configuration du pare-feu, celui-ci DOIT fonctionner comme configuré par le fichier téléchargé.

7.4.4.4.6 Echec du téléchargement du fichier de configuration du pare-feu

En cas d'échec de la vérification du fichier de configuration comme spécifié dans le § 7.4.4.3, "Exigences relatives à la vérification du fichier de configuration et à l'authentification du mode de préconfiguration SNMP", le dispositif PS DOIT continuer son fonctionnement normal, ignorer le fichier de configuration du pare-feu et signaler l'événement approprié, identifié dans le Tableau B.1, "Evénements définis pour IPCable2Home".

Si le fichier de configuration du pare-feu contient des éléments en double TLV-27 ou TLV-28 ("en double" signifiant que deux ou plus de deux objets de base MIB en protocole SNMP ont un identificateur d'objet identique (OID)), le dispositif PS DOIT continuer son fonctionnement normal, ignorer le fichier de configuration du pare-feu et signaler l'événement approprié, identifié dans le Tableau B.1, "Evénements définis pour IPCable2Home".

Si le fichier de configuration du pare-feu contient un champ de type reconnu mais un mauvais champ de valeur, ou une valeur d'identificateur de TLV-27 ou TLV-28 mais une mauvaise valeur de base MIB, le dispositif PS DOIT continuer son fonctionnement normal, ignorer le fichier de configuration du pare-feu et signaler l'événement approprié, identifié dans le Tableau B.1, "Evénements définis pour IPCable2Home".

Si le fichier de configuration du pare-feu contient un champ de type reconnu ou un élément TLV-28 contenant un identificateur OID non reconnu, le dispositif PS DOIT ignorer ce TLV, signaler l'événement approprié, identifié dans le Tableau B.1, "Evénements définis pour IPCable2Home" et continuer le traitement du fichier de configuration du pare-feu.

Si le téléchargement du fichier de configuration du pare-feu échoue pour une raison quelconque, le pare-feu DOIT fonctionner comme configuré avant l'échec de la tentative de téléchargement.

7.5 Fonction de services de portail – Client d'heure locale

7.5.1 Fonction de client d'heure locale: objectifs

L'objectif des fonctions de client d'heure locale du dispositif PS est d'acquérir l'heure locale à partir du serveur temporel dans le réseau du câblo-opérateur.

7.5.2 Fonction de client d'heure locale: directives de conception du système

Les directives identifiées dans le Tableau 7-16 ont guidé la spécification des capacités définies pour la fonction de client d'heure locale des services de portail:

Tableau 7-16/J.192 – Client d'heure locale: directives de conception du système

Numéro	Directives
ToD 1	Offrir un mécanisme permettant au dispositif PS de mettre en œuvre la synchronisation horaire avec la tête de réseau.

7.5.3 Fonction de client d'heure locale: description du système

L'élément de services de portail utilise un client d'heure locale conforme au document [RFC 868], afin de réaliser la synchronisation horaire avec un serveur temporel situé dans le réseau de transmission de données du câblo-opérateur. La synchronisation horaire est essentielle pour les fonctions de sécurité des services de portail ainsi que pour la messagerie de signalisation des événements.

Quand le client CDC du protocole DHCP demande une adresse IP – à partir du serveur DHCP situé dans le réseau de transmission de données du câblo-opérateur – pour l'interface avec le réseau WAN-Man, ce client du protocole DHCP va recevoir l'adresse IP du serveur temporel situé dans le réseau de transmission de données du câblo-opérateur, dans l'option 4 du protocole DHCP.

Une fois que la pile IP du réseau WAN-Man commence à utiliser l'adresse IP qu'elle a reçue du serveur DHCP situé dans le réseau de transmission de données du câblo-opérateur, le dispositif PS envoie une interrogation temporelle [RFC 868] au serveur temporel. Si celui-ci renvoie une réponse valide, le dispositif PS utilise, afin d'établir l'heure locale, l'heure UTC acquise du serveur temporel avec un certain décalage horaire apportant un ajustement par rapport à l'heure UTC en fonction du fuseau horaire dans lequel le dispositif PS est implanté.

Une source d'informations sur le décalage horaire est le serveur DHCP. Ces informations peuvent comprendre celles qui sont contenues dans l'option DHCP 2 (Option de décalage horaire) des messages DHCP OFFER et ACK. En variante, le câblo-opérateur peut préconfigurer le dispositif PS avec un décalage horaire par écriture d'une valeur de l'objet de base MIB de portail CDP [voir § E.2] cabhCdpSnmpSetTimeOffset. Un autre objet de base MIB de portail CDP, cabhCdpTimeOffsetSelection, permet au câblo-opérateur de configurer le dispositif PS de façon à utiliser soit le décalage horaire fourni dans l'option DHCP 2 ou le décalage horaire indiqué par l'objet cabhCdpSnmpSetTimeOffset. Un autre décalage horaire possible est l'ajustement d'heure d'été dans les régions qui l'observent. L'objet de base MIB de portail CDP cabhCdpDaylightSavingTimeEnable permet au câblo-opérateur de configurer le dispositif PS de façon à ajouter 1 h au décalage horaire afin de tenir compte de l'heure d'été. Voir la référence [§ E.2] pour les détails.

Une fois qu'il a acquis l'heure UTC à partir du serveur temporel avec la valeur appropriée du décalage horaire (déterminée par la valeur de l'objet cabhCdpTimeOffsetSelection), le dispositif PS va les combiner, va ajouter l'ajustement d'heure d'été le cas échéant (si l'objet cabhCdpDaylightSavingTimeEnable est réglé à la valeur enabled(1)), va mettre à jour la valeur en tant qu'heure actuelle dans l'objet de base MIB IPCable2Home cabhPsDevDateTime et va commencer à utiliser cette heure locale pour les marqueurs temporels des messages événementiels et pour les fonctions de sécurité.

7.5.4 Fonction de client d'heure locale: exigences

L'élément de services de portail DOIT implémenter un client d'heure locale.

Le client d'heure locale des services de portail DOIT être conforme au protocole horaire [RFC 868] et ne doit utiliser que le protocole UDP.

Lors d'une réinitialisation, avant que le dispositif PS se synchronise avec un serveur d'heure locale, l'élément de services de portail DOIT initialiser sa date à 00:00.0 (minuit) GMT du 1er janvier 1970.

Si le dispositif PS reçoit l'option 4 du protocole DHCP (option de serveur temporel) dans le message ACK du protocole DHCP, ce dispositif PS DOIT sauvegarder l'adresse IP du serveur temporel duquel le dispositif PS a accepté une réponse sous forme de valeur de l'objet cabhPsDevTimeServerAddr.

Un dispositif PS intégré DOIT utiliser la plus récente heure locale valide qui a été acquise à partir du serveur temporel ToD pour l'horloge locale du système, même si cela implique l'écrasement de l'heure système acquise par le câblo-modem ou l'écrasement de l'heure système initialement fixée à l'heure historique (00:00:00 (minuit) GMT, le 1er janvier 1970)).

Si la valeur de l'objet cabhPsDevTodSyncStatus est true(1), c'est-à-dire si l'heure locale a déjà été établie, il n'est pas nécessaire que le client d'heure locale émette une requête temporelle ToD.

Le dispositif PS ne DOIT envoyer et recevoir de messages ToD qu'au moyen de son interface avec le réseau WAN-Man.

Le dispositif PS DOIT utiliser la valeur de l'objet cabhPsDevDateTime pour toutes les fonctions nécessitant l'heure locale et dont la précision admissible peut n'être qu'à la seconde près.

Le processus d'acquisition IPCable2Home d'heure locale se compose de deux phases: la phase de tentative initiale de synchronisation avec l'heure locale (tentative initiale) et la phase de réessai de synchronisation avec l'heure locale (réessai). Si le dispositif PS réussit à synchroniser son heure locale avec le serveur distant d'heure locale pendant la phase de tentative initiale, il ne lance pas la phase de réessai. Le dispositif PS est tenu d'entrer dans la phase de tentative initiale et d'essayer la synchronisation avec un serveur distant d'heure locale dès réception d'un message d'acquittement ACK du DHCP, si la valeur de l'objet cabhPsDevTodSyncStatus est: false(2). Le paragraphe 7.5.4.1

décrit le comportement requis de tentative initiale pour le dispositif PS. Le paragraphe 7.5.4.2 décrit le comportement requis du dispositif PS si celui-ci est tenu de lancer la phase de réessai ToD.

7.5.4.1 Tentative initiale de synchronisation avec l'heure locales: exigences

Si le dispositif PS doit fonctionner en mode de préconfiguration DHCP ou de préconfiguration SNMP (cabhPsDevProvMode = dhcpmode(1) ou snmpmode(2)), le dispositif PS DOIT essayer de se synchroniser avec un serveur distant d'heure locale dont l'adresse lui a été transmise dans l'option DHCP 4 du message d'acquittement ACK du DHCP, conformément à [RFC 868]. Un dispositif PS fonctionnant en mode CableHome inactif n'est pas tenu d'essayer de se synchroniser avec un serveur distant d'heure locale.

Si le dispositif PS ne réussit pas à se synchroniser avec un serveur distant d'heure locale (ToD) à sa première tentative, ce dispositif PS DOIT essayer de se synchroniser avec le prochain serveur ToD dans l'ordre énuméré dans l'option DHCP 4, jusqu'à ce qu'il réussisse à se synchroniser avec un serveur OU jusqu'à ce qu'il ait effectué une tentative infructueuse avec chaque serveur ToD énuméré. Le dispositif PS DOIT signaler l'événement approprié (voir le Tableau B.1) pour chaque tentative infructueuse de synchronisation avec un serveur distant d'heure locale. Une tentative de synchronisation avec un serveur distant d'heure locale est un unique essai d'accès au port 37 d'un serveur distant d'heure locale, lancé par le dispositif PS comme décrit dans [RFC 868]. Une tentative infructueuse de synchronisation avec un serveur distant d'heure locale est telle que son résultat est que le dispositif PS NE reçoit PAS d'informations temporelles valides du serveur distant d'heure locale, ou telle qu'une tentative de résoudre l'adresse (IP) du serveur distant d'heure locale a comme résultat que le dispositif PS n'acquiert pas cette adresse.

Si le dispositif PS réussit à se synchroniser avec un serveur distant d'heure locale, il DOIT effectuer ce qui suit:

- mettre la valeur de l'objet cabhPsDevTodSyncStatus à: true(1);
- mettre la valeur de l'objet cabhCdpServeurTimeOffset à celle de l'option 2 du DHCP (décalage horaire) du message d'acquittement ACK du DHCP si la valeur de l'objet cabhCdpTimeOffsetSelection est: useDhcpOption2(1), ou à celle de l'objet cabhCdpSnmpSetTimeOffset si la valeur de l'objet cabhCdpTimeOffsetSection est: useSnmpSetOffet(2);
- mettre la valeur de l'objet cabhPsDevDateTime égale à l'heure UTC acquise à partir du serveur temporel, plus le décalage horaire de l'option 2 du DHCP contenue dans le message d'acquittement ACK du DHCP OU acquise à partir de la valeur de l'objet cabhCdpSnmpSetTimeOffset conformément à la valeur de l'objet cabhCdpTimeOffsetSelection, plus 1 h d'ajustement d'heure d'été pendant la période correspondante si la valeur de l'objet cabhCdpDaylightSavingTimeEnable est: enabled(1);
- mettre la valeur de l'objet cabhPsDevTimeServeurAddr à l'adresse IP du serveur distant d'heure locale avec lequel le dispositif PS a synchronisé son horloge;
- si la fonction de serveur CDS du dispositif PS possède des locations en cours d'adresse IP de réseau local, mettre à jour l'objet cabhCdpLanAddrCreateTime avec la valeur de l'objet cabhPsDevDateTime et régler la valeur de l'objet cabhCdpLanAddrExpireTime égale à cabhCdpLanAddrCreateTime plus la valeur de l'objet cabhCdpServeurLeaseTime, pour chaque location active;
- continuer par le processus de préconfiguration comme défini au § 13.

Si un dispositif PS intégré fonctionnant en mode de préconfiguration DHCP ne réussit pas à se synchroniser avec l'un quelconque des serveurs distants d'heure locale énumérés dans l'option DHCP 4 du message d'acquittement ACK du DHCP après avoir tenté de le faire une seule fois avec chaque serveur ToD énuméré, le dispositif PS intégré DOIT essayer d'acquérir l'horloge système du

câblo-modem. Le dispositif PS intégré fonctionnant dans le mode de préconfiguration SNMP n'est pas tenu d'essayer d'acquérir l'horloge système du câblo-modem.

Si le dispositif PS intégré fonctionnant en mode de préconfiguration DHCP ne réussit pas à se synchroniser avec l'un quelconque des serveurs distants d'heure locale à sa première tentative avec chacun d'eux et réussit à acquérir l'horloge système du câblo-modem, ce dispositif PS intégré DOIT effectuer ce qui suit:

- mettre la valeur de l'objet cabhPsDevTodSyncStatus à: false(2);
- mettre la valeur de l'objet cabhPsDevDateTime à l'horloge système du câblo-modem;
- si la fonction de serveur CDS du dispositif PS intégré possède des locations en cours d'adresse IP de réseau local, mettre à jour l'objet cabhCdpLanAddrCreateTime avec la valeur de l'objet cabhPsDevDateTime (heure du câblo-modem) et régler la valeur de l'objet cabhCdpLanAddrExpireTime égale à cabhCdpLanAddrCreateTime plus la valeur de l'objet cabhCdpServeurLeaseTime, pour chaque location active;
- lancer le processus de réessai de synchronisation avec l'heure locale défini au § 7.5.4.2 et continuer par le processus de préconfiguration défini au § 13.

Un dispositif PS intégré fonctionnant en mode de préconfiguration DHCP qui ne réussit pas à se synchroniser avec un quelconque serveur distant d'heure locale à sa première tentative avec chaque serveur et qui ne réussit pas à acquérir l'horloge système du câblo-modem, DOIT effectuer ce qui suit:

- mettre la valeur de l'objet cabhPsDevTodSyncStatus à: false(2);
- mettre la valeur de l'objet cabhPsDevDateTime à l'heure historique (00:00.0 (minuit) GMT, 1er janvier 1970);
- si sa fonction de serveur CDS possède des locations en cours d'adresse IP de réseau local, mettre à jour l'objet cabhCdpLanAddrCreateTime avec la valeur de l'objet cabhPsDevDateTime (heure historique) et régler la valeur de l'objet cabhCdpLanAddrExpireTime égale à cabhCdpLanAddrCreateTime plus la valeur de l'objet cabhCdpServeurLeaseTime, pour chaque location active;
- lancer le processus de réessai de synchronisation avec l'heure locale défini au § 7.5.4.2 et continuer par le processus de préconfiguration défini au § 13;
- signaler l'événement approprié (voir le Tableau B.1) pour chaque tentative infructueuse de synchronisation avec le serveur distant d'heure locale.

Un dispositif PS autonome fonctionnant en mode de préconfiguration DHCP qui ne réussit pas à se synchroniser avec un quelconque serveur distant d'heure locale à sa première tentative avec chacun de ces serveurs, DOIT effectuer ce qui suit:

- mettre la valeur de l'objet cabhPsDevTodSyncStatus à: false(2);
- mettre la valeur de l'objet cabhPsDevDateTime à l'heure historique (00:00.0 (minuit) GMT, 1er janvier 1970);
- si sa fonction de serveur CDS possède des locations en cours d'adresse IP de réseau local, mettre à jour l'objet cabhCdpLanAddrCreateTime avec la valeur de l'objet cabhPsDevDateTime (heure historique) et régler la valeur de l'objet cabhCdpLanAddrExpireTime égale à cabhCdpLanAddrCreateTime, plus la valeur de l'objet cabhCdpServeurLeaseTime, pour chaque location active;
- lancer le processus de réessai de synchronisation avec l'heure locale défini au § 7.5.4.2 ET continuer par le processus de préconfiguration défini au § 13;
- signaler l'événement approprié (voir le Tableau B.1) pour chaque tentative infructueuse de synchronisation avec le serveur distant d'heure locale.

Un dispositif PS fonctionnant dans le mode de préconfiguration SNMP qui ne réussit pas à se synchroniser avec un quelconque serveur distant d'heure locale énuméré dans l'option DHCP 4 du message d'acquittement ACK du DHCP à sa première tentative avec chacun de ces serveurs, DOIT lancer le processus de réessai de synchronisation avec l'heure locale défini au § 7.5.4.2. Un dispositif PS fonctionnant dans le mode de préconfiguration SNMP qui ne réussit pas à se synchroniser avec un quelconque serveur distant d'heure locale NE DOIT PAS continuer par le processus de préconfiguration défini au § 13. L'exigence que le dispositif PS signale un événement pour chaque tentative infructueuse de synchronisation avec un serveur distant d'heure locale s'applique au dispositif PS fonctionnant dans le mode de préconfiguration SNMP.

7.5.4.2 Réessai de synchronisation sur l'heure locale – Exigences

Si un dispositif PS fonctionnant en mode de préconfiguration DHCP ne réussit pas à se synchroniser avec un quelconque serveur distant d'heure locale énuméré dans l'option 4 du message d'acquittement ACK du DHCP et si cabhPsDevTodSyncStatus = false(2), ce dispositif PS DOIT continuer à essayer de se synchroniser avec les serveurs distants d'heure locale énumérés dans l'option 4 du message d'acquittement ACK du DHCP jusqu'à ce qu'il réussisse à signaler l'événement approprié (voir le Tableau B.1) pour chaque tentative infructueuse.

Tant que la valeur de l'objet cabhPsDevTodSyncStatus = false(2), un dispositif PS fonctionnant dans le mode de préconfiguration SNMP DOIT continuer à essayer de se synchroniser avec chacun des serveurs distants d'heure locale énumérés dans l'option 4 du message d'acquittement ACK du DHCP, pour un total de six tentatives (tentative initiale plus cinq réessais) et signaler l'événement approprié (voir le Tableau B.1) pour chaque tentative infructueuse.

Le client d'heure locale du dispositif PS NE DOIT PAS dépasser plus de trois requêtes d'heure locale ToD par serveur distant d'heure locale dans toute période de 5 minutes. Au minimum, un dispositif PS essayant de se synchroniser avec un serveur ToD DOIT émettre au moins 1 requête d'heure locale par période de 5 minutes.

Un dispositif PS fonctionnant dans le mode de préconfiguration SNMP qui ne réussit pas à se synchroniser avec un quelconque serveur distant d'heure locale après avoir essayé six fois avec chaque serveur ToD énuméré dans l'option 4 du message d'acquittement ACK du DHCP, DOIT effectuer ce qui suit:

- mettre la valeur de l'objet cabhPsDevTodSyncStatus à false(2);
- enregistrer l'identificateur d'événement 68000403 (voir l'Annexe B, Tableau B.1) conformément à la priorité configurée pour l'événement et conformément à la procédure définie au § 6.3.3.2, Fonction de signalisation d'événement de portail CMP;
- relancer le processus de préconfiguration en commençant par l'envoi d'un message DHCP DISCOVER;
- signaler l'événement approprié (voir le Tableau B.1) pour chaque tentative infructueuse de synchronisation avec le serveur distant d'heure locale.

7.6 Fonction de point extrême (BP) – Client du protocole DHCP

7.6.1 Fonction de point extrême de client du protocole DHCP: objectifs

L'objectif de la fonction de point extrême de client du protocole DHCP est d'acquérir une location d'adresse IP et des paramètres de configuration pour le point BP à partir du serveur DHCP du système.

7.6.2 Fonction de point extrême de client du protocole DHCP: directives de conception du système

Les directives énumérées dans le Tableau 7-17 ont guidé la spécification de la fonction de point extrême de client du protocole DHCP.

Tableau 7-17/J.192 – Fonction de point extrême de client du protocole DHCP: directives de conception du système

Numéro	Directives
BP DHC 1	Permettre au point BP d'acquérir une location d'adresse réseau et des informations de configuration.

7.6.3 Fonction de point extrême de client du protocole DHCP: description du système

La fonction de point extrême d'un client du protocole DHCP est chargée d'acquérir une location d'adresse IP à partir d'un serveur DHCP du système. Ce serveur pourrait être la fonction de serveur CDS du sous-élément de portail CDP du dispositif PS ou pourrait être un serveur DHCP situé dans le réseau de données du câblo-opérateur, selon la façon dont le mode de traitement des paquets dans le dispositif PS est configuré. Les fonctions de point extrême de client du protocole DHCP recueillent également des informations de configuration transmises dans les champs d'option DHCP à partir du serveur DHCP du système.

7.6.4 Fonction de point extrême de client du protocole DHCP: exigences

Le point BP DOIT implémenter une fonction de client du protocole DHCP conformément aux exigences relatives aux clients figurant dans [RFC 2131].

Lors d'une réinitialisation, le point BP DOIT envoyer un message DHCP DISCOVER diffusé afin d'acquérir une location d'adresse IP.

Le point BP DOIT prendre en charge les options et sous-options DHCP indiquées comme étant obligatoires (M) dans le Tableau 7-18.

Le point BP DOIT inclure les codes d'option DHCP ci-après dans chaque message DHCP DISCOVER et DHCP REQUEST qu'il envoie:

- Option DHCP de code 55: liste de demande de paramètres;
- Option DHCP de code 60: identificateur de classe de vendeur, avec la chaîne "CableHome1.1BP" (sans espaces ni guillemets);
- Option DHCP de code 255: fin.

Tableau 7-18/J.192 – Options DHCP requises par un client de point BP du protocole DHCP

Numéro d'option	Fonction de l'option	Prise en charge (M = obligatoire ou O = facultative)	Valeur par défaut fixée à l'usine
0	Bourrage	–	N/A
255	Fin	M	N/A
1	Masque de sous-réseau	M	N/A
2	Décalage horaire	O	0
3	Option de routeur	M	N/A
6	Serveur de noms de domaine	M	N/A
7	Serveur de journalisation	M	N/A
12	Nom du serveur local	O	N/A
15	Nom de domaine	M	Chaîne vide
23	Temps par défaut de recherche de relais	M	N/A
26	Unité MTU d'interface	M	N/A

Tableau 7-18/J.192 – Options DHCP requises par un client de point BP du protocole DHCP

Numéro d'option	Fonction de l'option	Prise en charge (M = obligatoire ou O = facultative)	Valeur par défaut fixée à l'usine
43	Informations propres au vendeur	M	Choisies par le vendeur
50	Adresse IP demandée	M	Valeur néant ou choisie par le vendeur
10	Durée de location d'adresse IP	M	N/A
54	Identificateur de serveur	M	N/A
55	Liste de demande de paramètres	M	N/A
60	Identificateur de classe de vendeur	M	"CableHome1.1BP"
61	Identificateur de client	O	N/A

8 Traitement de paquet et conversion d'adresse

8.1 Introduction/Aperçu général

8.1.1 Objectifs

Les objectifs clés qui régissent les capacités de traitement de paquet sont les suivants:

- offrir une fonctionnalité de conversion d'adresse facile sur le câble, offrant au câblo-opérateur la visibilité et la facilité de gestion des dispositifs domestiques tout en préservant les architectures d'acheminement fondées sur une ressource de réseau câblé;
- empêcher le trafic inutile sur le réseau câblé et sur le réseau domestique;
- conserver les adresses IP acheminables mondialement ainsi que les adresses de gestion privée de réseau câblé;
- faciliter l'acheminement du trafic IP domestique par attribution d'adresses de réseau à des dispositifs IP de réseau local de telle sorte qu'ils résident dans le même sous-réseau logique.

8.1.2 Hypothèses

- On suppose que, quand des serveurs de préconfiguration de câblo-opérateur offrent de multiples adresses IP acheminables mondialement à des dispositifs domestiques clients, ces adresses ne vont pas nécessairement résider dans le même sous-réseau.
- Le changement de fournisseur de services Internet est censé n'intervenir qu'assez rarement, à un rythme similaire à celui du changement de transporteur primaire à longue distance par un abonné résidentiel.

8.2 Architecture

Le présent paragraphe décrit les concepts clés régissant la fonctionnalité de traitement de paquet et de conversion d'adresses dans l'environnement IPCable2Home.

8.3 Elément logique des services de portail – Portail d'adressage IPCable2Home (CAP)

Le portail d'adressage IPCable2Home (CAP) est un sous-élément logique de l'élément logique de services de portail. Ses fonctions consistent à acheminer le trafic entre le réseau local et le réseau

régional, à acheminer le trafic de réseau local à réseau local, et à exécuter des fonctions de conversion d'adresse et de port.

8.3.1 Objectifs du portail CAP

Les objectifs du portail CAP sont énumérés ci-dessous et dans le § 8.1.1:

- acheminer des paquets IP entre dispositifs IP de réseau local et entre dispositifs IP de réseau local et passerelle par défaut des services de portail sur le réseau régional;
- offrir une capacité de conversion d'adresse de réseau et de port (NAPT) pour mappage entre une unique adresse IP mondiale à l'interface PS WAN et une ou plusieurs adresses IP privées dans le réseau local;
- offrir une capacité de conversion d'adresse de réseau (NAT) pour mappage bi-univoque entre adresses IP mondiales à l'interface PS WAN et adresses IP privées dans le réseau local;
- maintenir dans le réseau local le trafic entre dispositifs IP de réseau local et ne pas permettre qu'il traverse le réseau régional.

8.3.2 Directives de conception du système de portail CAP

Les directives de conception du système énumérées dans le Tableau 8-1 ont guidé la spécification de la fonctionnalité de portail d'adressage par câble IPCable2Home.

Tableau 8-1/J.192 – Directives de conception du système de portail CAP

Numéro	Directives
CAP 1	Les mécanismes d'adressage seront commandés par l'opérateur et lui offriront la connaissance et l'accessibilité des dispositifs IPCable2Home.
CAP 2	L'adressage ne fera rien qui puisse compromettre les architectures actuelles d'acheminement dans le réseau câblé (par exemple le routage fondé sur l'origine, la commutation MPLS).
CAP 3	Les mécanismes de gestion de trafic isoleront le réseau câblé du trafic produit par des communications résidentielles entre homologues.
CAP 4	Les adresses IP seront conservées si possible (aussi bien les adresses acheminables mondialement que les adresses de gestion privée du réseau câblé).
CAP 5	{texte informatif: le portail CAP permettra à des dispositifs UPnP de réseau local de configurer des mappages de conversion d'adresse de couche Réseau, mais dans la mesure où cela NE crée PAS de conflit avec les politiques de l'opérateur.}

8.3.3 Description du système de portail CAP

La fonctionnalité de conversion d'adresse et de traitement de paquet est fournie par l'entité fonctionnelle appelée *portail d'adressage IPCable2Home* (CAP), qui englobe les éléments suivants de conversion d'adresse et de réexpédition de paquet:

- conversion d'adresse IPCable2Home (CAT);
- fonction de transfert IPCable2Home;
- commutation de réexpédition sélective en amont (USFS).

Comme représenté dans la Figure 8-1, la fonction de conversion CAT offre un mécanisme permettant d'interconnecter le secteur d'adresses du réseau WAN-Data et le secteur d'adresses du réseau LAN-Trans (par conversion d'adresse), alors que la fonction de transfert offre un mécanisme permettant d'interconnecter le secteur d'adresses du réseau WAN-Data et le secteur d'adresses du réseau LAN-Pass (par dérivation). La fonction de conversion CAT est conforme à la conversion d'adresse réseau (NAT) traditionnelle [RFC 3022] section 2. Comme avec la conversion NAT

traditionnelle, il y a deux variantes de conversion CAT, dites *acheminement transparent de conversion d'adresse de réseau IPCable2Home* (C-NAT) et *acheminement transparent de conversion d'adresse réseau et de port IPCable2Home* (C-NAPT). L'acheminement transparent C-NAT est la version conforme à l'environnement IPCable2Home de la conversion NAT de base [RFC 3022] section 2.1 et l'acheminement transparent C-NAPT est la version conforme à l'environnement IPCable2Home de la conversion NAPT [RFC 3022] section 2.2.

Selon [RFC 3022], l'acheminement transparent C-NAT est "une méthode de mappage des adresses IP d'un groupe à un autre, transparente aux utilisateurs finals", et l'acheminement transparent C-NAPT "est une méthode par laquelle de nombreuses adresses de réseau et leurs ports TCP/UDP (protocole de commande de transmission/protocole de datagramme d'utilisateur) sont converties en une seule adresse de couche Réseau avec ses ports TCP/UDP". Egalement, selon [RFC 3022], l'objet de la fonctionnalité C-NAT et C-NAPT est de "fournir un mécanisme de connexion d'un secteur d'adresses privées à un secteur externe ayant des adresses mondiales enregistrées de façon unique".

La fonction de transfert IPCable2Home est un processus de routage spécifié par le modèle IPCable2Home qui interconnecte le secteur d'adresses du réseau WAN-Data et le secteur d'adresses du réseau LAN-Pass sans conversion d'adresse.

La commutation de réexpédition sélective en amont (USFS, *upstream selective forwarding switch*) définit au sein du portail CAP une fonction permettant de confiner le trafic domestique à l'intérieur du réseau domestique, même quand les dispositifs d'utilisateur qui produisent ce trafic résident dans des sous-réseaux logiques IP différents. Plus précisément, cette fonction réexpédie directement à sa destination le trafic qui provient d'une adresse IP située dans un des secteurs d'adresses de réseau local et qui est destiné à des secteurs d'adresses IP de réseau local. Cette fonctionnalité de réexpédition directe empêche le trafic de traverser le réseau en hybride HFC et interconnecte les secteurs d'adresses LAN-Trans et LAN-Pass.

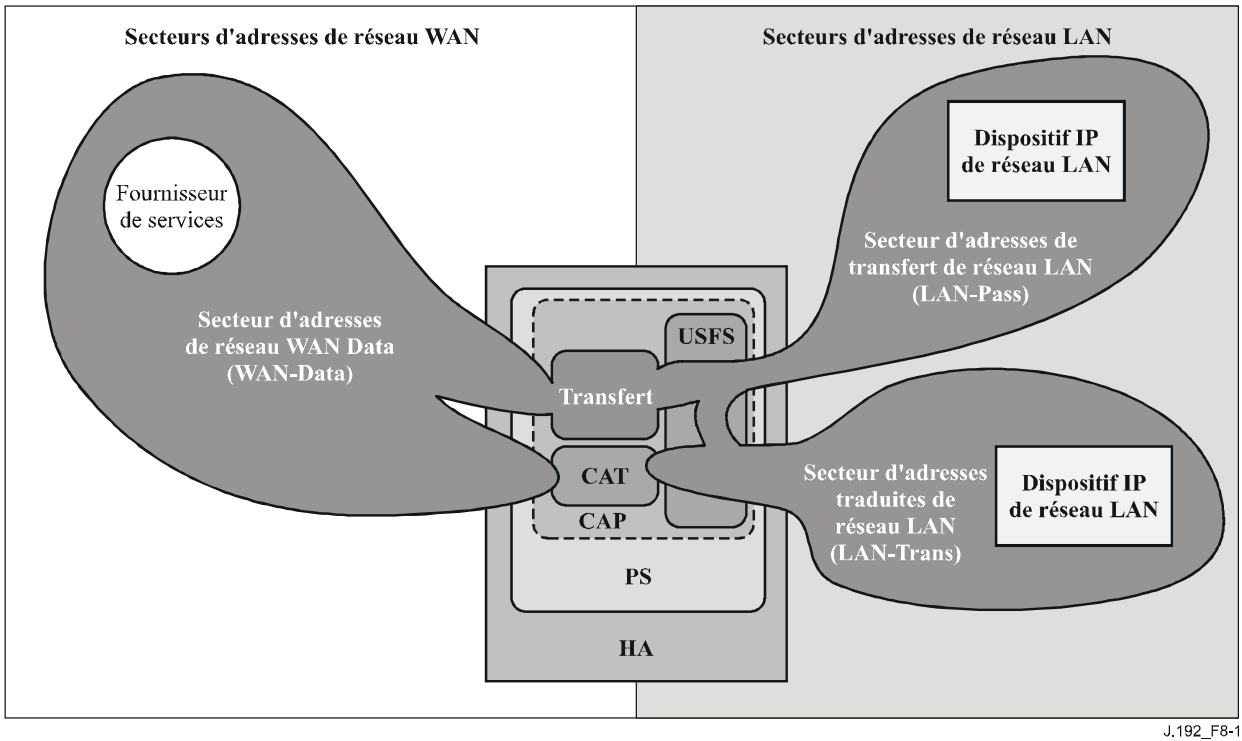


Figure 8-1/J.192 – Fonctions du portail d'adressage IPCable2Home (CAP)

Dans l'ensemble de la présente Recommandation, les termes *association d'adresse, non-association d'adresse, conversion d'adresse et session* sont utilisés selon les définitions du document [RFC 2663]. En outre, IPCable2Home définit le terme *mappage* comme étant les informations nécessaires afin d'exécuter l'acheminement transparent C-NAT/C-NAPT.

En particulier, un mappage C-NAT est défini comme un nuplet de la forme (adresse IP de réseau WAN-Data, adresse IP de réseau LAN-Trans) fournissant un mappage bi-univoque entre adresses de réseau WAN-Data et adresses de réseau LAN-Trans. De même, un mappage C-NAPT est défini comme un nuplet de la forme (adresse IP de réseau WAN-Data et port TCP/UDP, adresse IP de réseau LAN-Trans et port TCP/UDP) fournissant un mappage multivoque entre une adresse WAN-Data et de multiples adresses de réseau LAN-Trans. Pour le trafic en protocole ICMP (comme un sondage par écho), un identificateur ICMP est utilisé à la place du numéro de port TCP/UDP.

Le trafic de réseau local à réseau régional est défini comme étant formé de paquets issus de dispositifs IP de réseau local et destinés à des dispositifs situés du côté PS WAN. Le trafic de réseau régional à réseau local est défini comme étant formé de paquets issus de serveurs WAN destinés à des dispositifs IP de réseau local. Le trafic de réseau local à réseau local est défini comme étant formé de paquets issus de dispositifs IP de réseau local et destinés à des dispositifs IP de réseau local situés dans le même sous-réseau ou dans un sous-réseau différent.

8.3.3.1 Modes de traitement des paquets

L'élément de services de portail est configurable au moyen de l'objet cabhCapPrimaryMode de base MIB, de façon à fonctionner dans un des trois modes primaires de traitement de paquet lors du traitement du trafic de réseau local à réseau régional et du trafic de réseau régional à réseau local: le mode de transfert, le mode d'acheminement transparent C-NAT et le mode d'acheminement transparent C-NAPT. De plus, les modes primaires C-NAT ou C-NAPT peuvent également fonctionner dans un mode mixte, qui est décrit ci-dessous.

En mode de transfert, le portail CAP agit comme un pont transparent [ISO/CEI 10038], ponts entre le secteur WAN-Data et le secteur LAN-Pass. En mode de transfert, les décisions de réexpédition sont prises principalement dans la couche 2 de l'OSI (couche Liaison de données). Dans ce mode, le portail CAP n'exécute aucune fonction d'acheminement transparent C-NAT ou C-NAPT. Le trafic de routage PS pour dispositifs IP du secteur LAN-Pass est tenu de transmettre toutes les trames de la couche 2 de l'OSI qu'un câblo-modem conforme à DOCSIS est tenu de transmettre, y compris les trames du protocole SNAP [ISO/CEI 8802-2] et celles de la version 2.0 du protocole Ethernet du groupe DIX (DEC-Intel-Xerox).

Le portail CAP prend en charge la réexpédition dans la couche 3 de l'OSI (couche Réseau) à la fois dans le mode d'acheminement transparent C-NAT et dans le mode d'acheminement transparent C-NAPT, décrits ci-dessous.

En mode C-NAT, l'élément de services de portail (client CDC) acquiert une ou plusieurs adresses IP servant au trafic WAN-Data pendant le processus d'amorçage du dispositif PS. Après acquisition, ces adresses IP sont utilisées par le protocole DHCP comme portion d'adresses IP de réseau WAN-Data des nuplets de mappage C-NAT dynamiquement créés. Ces adresses IP de réseau régional constituent une réserve d'adresses disponible pour les mappages C-NAT dynamiquement créés. Si une adresse IP disponible existe dans la réserve d'adresses IP de réseau WAN-Data, le portail CAP crée un mappage dynamique C-NAT quand il détecte pour la première fois du trafic IP de réseau local à réseau régional qui ne possède pas de mappage existant. Si aucune adresse IP disponible n'existe dans la réserve d'adresses IP du réseau WAN-Data, le mappage dynamique C-NAT ne peut pas être créé et ce trafic est abandonné puis un événement est produit (voir l'Annexe B).

La portion d'adresses IP de réseau LAN-Trans des nuplets de mappage C-NAT dynamiquement créés est fournie par la réserve d'adresses IP définie par le câblo-opérateur dans la base MIB du portail CDP du réseau IPCable2Home. Le portail CAP introduit le nuplet de l'unique adresse IP de

réseau WAN-Data et une unique adresse IP de réseau LAN-Trans dans la table de mappage du portail CAP, de même que d'autres paramètres y compris les numéros des ports aux réseaux WAN et LAN, la méthode de mappage et le protocole de transport servant au mappage. Le numéro de port ne sera pas converti par le portail CAP pour les mappages C-NAT: les numéros des ports d'origine et de destination contenus dans l'en-tête UDP ou TCP seront conservés sans changement. Quand le dispositif PS doit fonctionner en mode primaire de traitement de paquet par conversion NAT (objet cabhCapPrimaryMode à la valeur = nat(2)), le portail CAP doit introduire la valeur 0 dans les entrées de la table de mappage du portail CAP concernant les numéros de port aux réseaux WAN et LAN. Le portail CAP doit également introduire la valeur 0 dans les entrées relatives aux numéros de port aux réseaux WAN et LAN de la table de mappage du portail CAP, pour les entrées préconfigurées de réexpédition par port statique de la table de mappage du portail CAP, quand le dispositif PS doit fonctionner en mode primaire de traitement de paquet par conversion NAPT (objet cabhCapPrimaryMode à la valeur = napt(1)). Dans le cas d'une entrée de réexpédition par port statique préconfigurée dans la table de mappage du portail CAP pour un dispositif PS fonctionnant en mode primaire de traitement de paquet par conversion NAPT, l'entrée correspondant au numéro de port de valeur 0 aura deux fonctions:

1) indiquer au portail CAP que les numéros de port ne doivent pas être convertis, c'est-à-dire que les ports sont "remplacés par une structure générique";

2) indiquer à tout lecteur de la table de mappage du portail CAP que ce mappage de port statique est effectivement un mappage C-NAT, ce qui permet d'établir une distinction entre entrées de réexpédition par port statique (mappages C-NAT avec numéro de port 0) et mappages C-NAPT (avec numéro de port différent de zéro).

Voir le paragraphe 8.3.3.2, "Structures génériques de réexpédition par port statique", pour de plus amples informations sur l'opération de réexpédition par port statique du portail CAP.

Les mappages dynamiques de conversion C-NAT pour le trafic en protocole UDP sont détruits quand une temporisation de période d'inactivité, objet cabhCapUdpTimeWait, arrive à expiration. Les mappages dynamiques de conversion C-NAT pour le trafic en protocole TCP sont détruits quand une temporisation de période d'inactivité, objet cabhCapTcpTimeWait, arrive à expiration ou qu'une session en protocole TCP se termine. Les mappages dynamiques de conversion C-NAT pour le trafic en protocole ICMP sont détruits quand une temporisation de période d'inactivité, objet cabhCapIcmpTimeWait, arrive à expiration. En outre, les mappages statiques C-NAT peuvent être créés ou détruits quand le système NMS écrit ou supprime des entrées de l'objet cabhCapMappingTable de base MIB.

En mode de conversion C-NAPT (mode par défaut fixées à l'usine pour le système) l'élément de services de portail (client CDC) acquiert une seule adresse IP, servant au trafic WAN-Data. Après acquisition par protocole DHCP, cette adresse IP est utilisée par le protocole DHCP comme portion d'adresse IP de réseau WAN-Data de nuplets de mappage C-NAPT créés dynamiquement. Si l'adresse IP de réseau WAN-Data a été acquise, des mappages dynamiques de conversion C-NAPT sont créés quand le portail CAP détecte pour la première fois du trafic IP de réseau local à réseau régional qui ne possède pas de mappage existant. Si l'adresse IP de réseau WAN-Data n'a pas été acquise (c'est-à-dire ne possède pas de location DHCP active), le mappage dynamique C-NAPT ne peut pas être créé, ce trafic est abandonné et un événement normalisé est produit (voir l'Annexe B).

Les mappages dynamiques de conversion C-NAPT pour le trafic en protocole UDP sont détruits quand une temporisation de période d'inactivité, objet cabhCapUdpTimeWait, arrive à expiration. Des mappages dynamiques de conversion C-NAPT pour le trafic en protocole TCP sont détruits quand une temporisation de période d'inactivité, objet cabhCapTcpTimeWait, arrive à expiration ou qu'une session en protocole TCP se termine. Les mappages dynamiques de conversion C-NAPT pour le trafic en protocole ICMP sont détruits quand une temporisation de période d'inactivité, objet cabhCapIcmpTimeWait, arrive à expiration. En outre, des mappages statiques de conversion

C-NAPT peuvent être créés ou détruits quand le système NMS écrit ou supprime des entrées de l'objet cabhCapMappingTable de base MIB.

La Figure 8-2 montre un processus typique de mappage dynamique C-NAPT avec un paquet TCP. Dans cet exemple, le dispositif PS est configuré de façon à fonctionner en mode NAPT et a déjà obtenu une adresse IP de réseau régional et le dispositif IP de réseau local a déjà obtenu une adresse IP dans le secteur LAN-Trans.

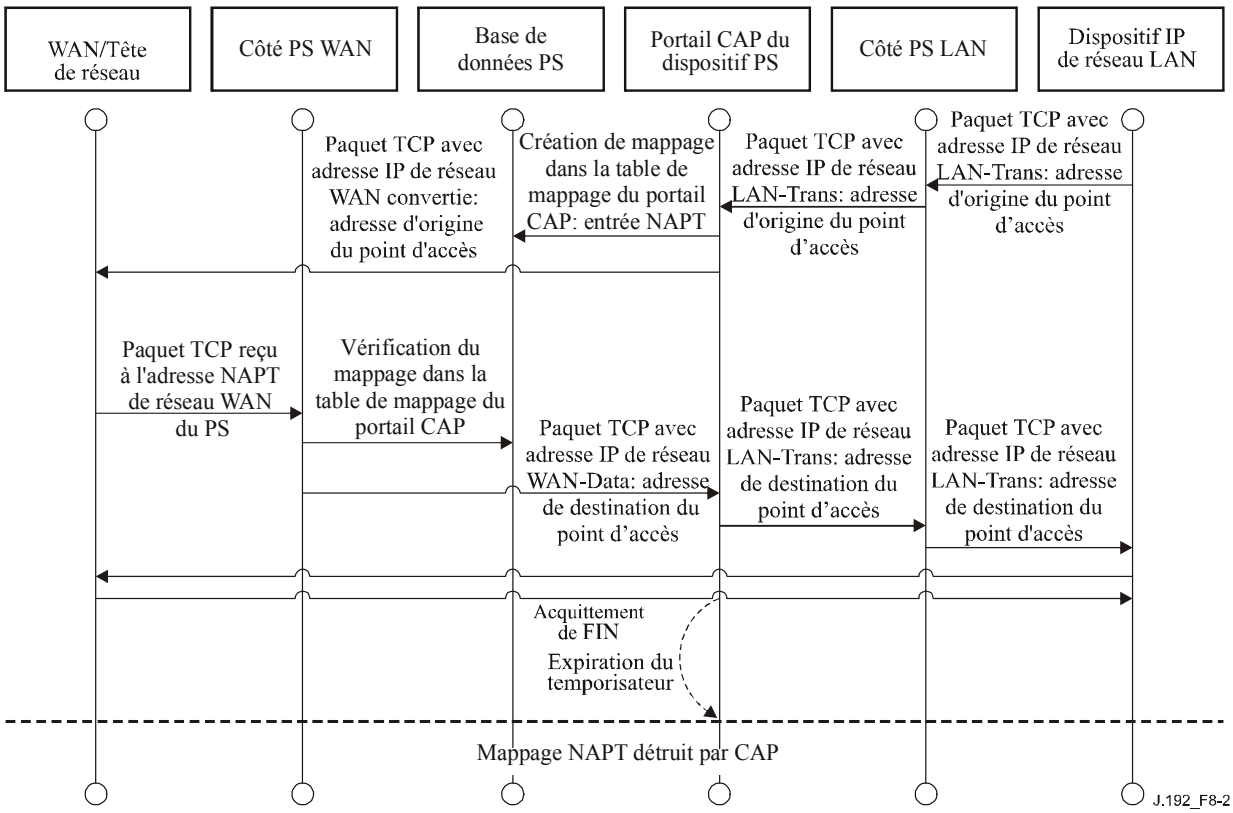


Figure 8-2/J.192 – Configuration des services de portail (table de mappage CAP-NAPT) – Diagramme séquentiel

Il est également possible que le dispositif PS fonctionne en mode mixte de routage/acheminement. Dans ce cas, le système NMS règle le mode primaire à l'acheminement transparent C-NAT ou C-NAPT et le système NMS écrit dans la table de transfert (objet cabhCapPassthroughTable), une ou plusieurs adresses MAC appartenant à des dispositifs IP de réseau local dont le trafic doit être dérivé. Dans ce mode mixte, le dispositif PS examine les adresses MAC des trames reçues afin de déterminer s'il faut dériver en transparence la trame ou appliquer d'éventuelles fonctions d'acheminement transparent C-NAT ou C-NAPT dans la couche IP. Dans le cas du trafic de réseau local à réseau régional, le dispositif PS examine l'adresse de commande MAC d'origine et, si cette adresse de commande MAC existe dans l'objet cabhCapPassthroughTable, la trame est dérivée en transparence vers l'interface avec le réseau WAN-Data. Dans le cas du trafic de réseau régional à réseau local, le dispositif PS examine l'adresse de destination MAC et, si cette adresse de commande MAC existe dans l'objet cabhCapPassthroughTable, la trame est dérivée en transparence vers l'interface appropriée avec un réseau local. Si l'adresse de couche MAC n'existe pas dans l'objet cabhCapPassthroughTable, le paquet est traité par les fonctions de couches supérieures, y compris la fonction d'acheminement transparent C-NAT/C-NAPT.

On suppose que, quand le dispositif PS est en mode d'acheminement (C-NAT/C-NAPT), il va traiter le trafic diffusé conformément aux documents [RFC 919], [RFC 922], [RFC 1812] et

[RFC 2644]. L'on part également du principe que, quand le dispositif PS est en mode de transfert, le trafic diffusé sera dérivé vers toutes les interfaces.

Quand le dispositif PS est en mode mixte de routage/acheminement et reçoit le trafic diffusé qui provient d'un dispositif figurant dans la table de transfert, ce dispositif PS est censé dériver le trafic diffusé vers toutes les interfaces. Quand le dispositif PS est en mode mixte de routage/acheminement et reçoit le trafic diffusé par une interface quelconque avec un réseau régional, le dispositif PS est censé dériver le trafic diffusé vers toutes les interfaces avec un réseau local.

Il y a lieu de remarquer que la fonctionnalité de commutation USFS (voir § 8.3.3.4) est appliquée dans chacun des trois modes primaires de traitement de paquet sans que l'utilisation du mode mixte entre en considération. Les décisions de réexpédition par commutation USFS auront priorité sur les autres décisions de réexpédition qui pourraient éventuellement réexpédier du trafic du réseau local vers le réseau régional.

8.3.3.2 Fonctionnalité de zone DM2 au portail CAP (réexpédition par port statique avec structures génériques de port)

Quand le dispositif PS est préconfiguré de façon à fonctionner en mode primaire de traitement de paquet C-NAPT et qu'un mappage de conversion C-NAPT est statiquement créé avec les deux numéros de port (WAN et LAN) réglés à zéro (c'est-à-dire lorsque une entrée de zone DMZ a été créée), alors le portail CAP doit traiter le trafic entrant de manière particulière. Le portail CAP va réexpédier tout le trafic de réseau régional à réseau local, non associé à une session de conversion C-NAPT existante ou à un mappage statique de conversion C-NAPT existante, à l'adresse IP de réseau local (adresse IP de zone DMZ) spécifiée dans ce type spécial de mappage de conversion C-NAPT existante, à l'adresse IP de réseau local (adresse IP de zone DMZ) spécifiée dans ce type spécial de mappage de conversion C-NAPT (en entrée de zone DMZ).

Le portail CAP va traiter les paquets comme suit:

1) vérifier tous les paquets entrants de réseau régional à réseau local afin de savoir s'ils sont associés à une session existante, spécifiée par un mappage dynamique de conversion C-NAPT. Si tel est le cas, alors le paquet est converti comme spécifié et réexpédié;
2) sinon, le portail CAP vérifie s'il y a un mappage statique de conversion C-NAPT associé au paquet. Si tel est le cas, alors le paquet est converti comme spécifié et réexpédié;
3) sinon, le portail CAP vérifie s'il y a un mappage statique de conversion C-NAPT pour cette adresse IP de réseau régional avec le numéro de port réglé à 0. Si tel est le cas, alors le portail CAP convertit l'adresse IP en l'adresse IP de réseau local spécifiée dans ce mappage statique spécial de conversion C-NAPT. Noter que la fonction C-NAPT ne convertit pas le port dans ce cas. Après la conversion d'adresse, le paquet est réexpédié.

NOTE – Si aucune des conditions ci-dessus n'est vérifiée, alors le paquet est abandonné.

Quand une entrée de zone DMZ est créée dans le portail CAP pour une adresse IP de réseau local qui est dynamiquement assignée par le dispositif PS (serveur CDS), ce dispositif PS est tenu de créer une réservation de location pour cette adresse IP. Cela garantit que l'adresse IP du dispositif de réseau local qui est réglée pour la fonctionnalité de zone déclassifiée ne change pas lors d'un renouvellement de location. Le dispositif PS peut rechercher l'adresse IP de zone DMZ dans les objets de table cabhCdpLanAddrTable. Si une entrée correspondante existe dans cette table avec la valeur de l'objet cabhCdpLanAddrMethod égale à soit dynamicActive(4) ou dynamicInactive(3), alors le dispositif PS est tenu de remplacer cette entrée de rangée par une autre qui représente une réservation de location d'adresse IP, c'est-à-dire par une entrée où la valeur de l'objet cabhCdpLanAddrMethod est égale à psReservationActive(6) ou à psReservationInactive(5), selon le cas. S'il n'y a pas d'entrée correspondant à l'adresse IP de zone DMZ dans la table d'objets cabhCdpLanAddrTable, alors le dispositif PS n'est pas tenu de créer une réservation de location

d'adresse IP pour cette adresse IP. Dans ce cas, il est possible que l'adresse IP de zone DMZ soit statiquement assignée au dispositif IP de réseau local.

Quand une entrée de zone DMZ est supprimée de la table d'objets cabhCapMappageTable pour une adresse IP de réseau local (serveur local de zone déclassifiée), le dispositif PS est tenu de supprimer la réservation de location d'adresse IP correspondante qu'il avait créée au niveau interne (identifiée par la valeur cabhCdpLanAddrMethod=psReservationActive(6)) dans la table cabhCdpLanAddrTable, et cela aussi longtemps que la table docsDevFilterIpTable ou cabhSec2FwLocalFilterIpTable ne possède pas une entrée correspondante de règle de filtrage de pare-feu qui l'exige. (Voir § 11.6.4.3.3, Ensemble de règles fixées par défaut à l'usine).

8.3.3.3 Prise en charge d'un réseau privé virtuel (VPN, *virtual private network*) dans le portail CAP

Le dispositif PS est tenu de mettre en œuvre une fonction de *Transfert de réseau VPN* qui permet aux clients du protocole IPSec [RFC 2401] situés dans un réseau privé virtuel d'échanger des clés au moyen du protocole d'échange de clés IP [RFC 2409]. Un seul client VPN domestique est pris en charge à la fois et ce client est censé répondre aux conditions suivantes:

- le dispositif IP de réseau local est dans le secteur LAN-Trans, c'est-à-dire qu'il a une adresse IP de réseau LAN-Trans;
- le dispositif IP de réseau local fait appel à IPSec en tant que protocole de réseau VPN;
- le dispositif IP de réseau local fait appel à l'échange de clés IP (IKE) afin d'échanger dynamiquement les clés de chiffrement avec le serveur de réseau VPN.

La présente Recommandation ne limite pas le nombre de clients de réseau privé virtuel dans le secteur LAN-Pass (c'est-à-dire le nombre de dispositifs IP de réseau local dont l'adresse de commande MAC est dans la table de transfert du dispositif PS) qui peuvent simultanément accéder à des serveurs VPN extérieurs à la résidence.

Pour que le client VPN puisse fonctionner correctement, un fichier de politique de pare-feu doit être actif dans le dispositif PS en ouvrant les ports appropriés au trafic entrant (de réseau régional à réseau local), plus précisément le port 500, pour le trafic d'échange IKE.

Quand des clés sont dynamiquement échangées au moyen du protocole IKE [RFC 2406] avant l'ouverture d'une session IPSec, le portail CAP va convertir les adresses réseau comme d'habitude et va, de plus, associer le port 500 comme port entrant pour l'adresse IP privée (de secteur LAN-Trans) du dispositif qui a établi la connexion VPN. Cela garantira que les messages IKE entrants seront correctement réexpédiés au client VPN. Les sessions IPSec sont définies dans le portail CAP par le port servant au trafic entrant et sortant, par le port servant à échanger des clés, par l'adresse du serveur VPN et par l'adresse du client VPN.

Même si le pare-feu a ouvert le port 500, le trafic entrant au port 500 ne sera réexpédié par le portail CAP qu'après le lancement d'une session IPSec par un client situé dans le secteur d'adresses du réseau LAN-Trans.

Si un deuxième client VPN domestique essaye de lancer une session IPSec avec un serveur VPN différent, le portail CAP va transférer les ports utilisés par l'adresse IP de réseau WAN-Data pour le trafic et l'échange de clés et les convertir en ports normalisés à l'adresse IP du client VPN situé dans le secteur LAN-Trans. Des clients supplémentaires de réseau privé virtuel peuvent être pris en charge également. Cependant, le portail CAP ne prend pas en charge plus d'un seul client VPN domestique se connectant au même serveur VPN.

Le protocole IPSec a trois modes qui peuvent être utilisés pour des VPN. Le dispositif PS est tenu de prendre en charge le mode de mise en tunnel de la charge utile de sécurité par encapsulage [RFC 2406]. Les prises en charge du mode de transport de la charge utile de sécurité par encapsulage [RFC 2406] et du mode d'en-tête d'authentification IP [RFC 2402] ne sont pas requises.

8.3.3.4 Commutation de réexpédition sélective en amont: aperçu général

Dans certains cas, un dispositif IP de réseau local situé dans le secteur d'adresses du réseau LAN-Pass va résider dans un sous-réseau logique IP différent de celui d'autres dispositifs IP de réseau local connectés au même élément de services de portail. Il est important d'empêcher le trafic entre ces dispositifs IP de réseau local de traverser le réseau en hybride HFC. Le blocage de ce trafic HFC indésirable est la fonction qui est offerte par la commutation de réexpédition sélective en amont (USFS).

Plus précisément, la commutation USFS achemine directement à sa destination le trafic qui provient du réseau domestique et qui lui est destiné. Le trafic provenant de dispositifs IP de réseau local dont l'adresse IP de destination est hors du secteur d'adresses du réseau local est transmise sans changement à la fonctionnalité de routage/acheminement du portail CAP.

La fonctionnalité de commutation USFS fait usage de la table de conversion d'adresses IP (comme définie dans le document [RFC 2011]) dans l'élément de services de portail. Cette table, objet [RFC 2011] ipNetToMediaTable, contient une liste d'adresses MAC, leurs adresses IP correspondantes et les numéros d'indice d'interface PS des interfaces physiques auxquelles ces adresses sont associées. La commutation USFS va se référer à cette table afin de prendre des décisions sur la façon de diriger le flux du trafic de réseau local à réseau régional. Afin de remplir la table ipNetToMediaTable, le dispositif PS apprend les adresses IP et MAC ainsi que leurs associations. Pour chaque interface physique associée, le dispositif PS apprend toutes les adresses IP de réseau LAN-Trans et LAN-Pass avec leurs liaisons MAC associées. Cet apprentissage peut intervenir par diverses méthodes. Les méthodes d'apprentissage d'adresses IP/MAC propres au vendeur peuvent être les suivantes: espionnage du portail ARP, surveillance du trafic et consultation des entrées du portail CDP. Les entrées sont purgées de la table ipNetToMediaTable après l'expiration d'une temporisation raisonnable de période d'inactivité.

La fonction de commutation USFS inspecte tout le trafic IP reçu par les interfaces PS LAN. Si l'adresse IP de destination se trouve (via la table ipNetToMediaTable) résider dans une interface PS LAN, l'adresse de destination dans la couche Liaison de données de la trame originale est modifiée de façon à passer de l'adresse de la passerelle par défaut à celle du dispositif IP de réseau local de destination et le trafic est – par la fonctionnalité de réexpédition et accès au support de la qualité de service (QFM) (voir § 10.2, "Architecture de qualité de service") contenue dans le dispositif PS – réexpédié vers l'interface PS LAN appropriée, selon la priorité des paquets. Si une correspondance avec l'adresse IP de destination n'est pas trouvée dans la table ipNetToMediaTable, le paquet est transmis, dans sa forme originale, à la fonction d'acheminement transparent C-NAT/C NAPT ou à la fonction de transfert en dérivation (selon le mode de traitement de paquet activé).

8.3.3.5 Liste de contrôle d'accès par commande MAC

Afin de contribuer à réduire ou à éliminer les probabilités de vol de service ou d'un autre accès non autorisé aux ressources du réseau local d'abonné, le modèle IPCable2Home prend en charge une liste de contrôle d'accès. Il s'agit d'une liste d'adresses matérielles visant les dispositifs IP de réseau local pour lesquels le dispositif PS va réexpédier du trafic. Cette liste est implémentée comme une table de base MIB (cabhPsDevAccessControlTable) qui se compose d'une énumération d'adresses physiques. La commande administrative de la table de contrôle d'accès est assurée par un objet scalaire de base MIB: cabhPsDevAccessControlEnable. Le contrôle d'accès est activé par un type d'interface, qui lui-même est activé pour le contrôle d'accès par positionnement du bit correspondant de l'objet cabhPsDevAccessControlEnable. Quand le bit correspondant à un type d'interface est positionné (1), le dispositif PS réexpédie le trafic à destination ou en provenance de tout dispositif IP de réseau local au moyen du type d'interface dont l'adresse physique ou matérielle fait partie de la table de contrôle d'accès, mais ne réexpédie pas le trafic au moyen de ce type d'interface à destination ou en provenance d'un dispositif IP de réseau local dont l'adresse physique ne fait pas partie de la table de contrôle d'accès. Quand le bit correspondant à un type d'interface n'est pas

positionné, le dispositif PS n'utilise pas la table de contrôle d'accès lorsqu'il détermine s'il y a lieu de réexpédier le trafic à destination ou en provenance des dispositifs au moyen de ce type d'interface. Voir la description de la table de contrôle d'accès dans la référence [§ E.4].

8.3.3.6 Multidiffusion

Le portail CAP prend en charge le trafic multidiffusé de réseau régional à réseau local par dérivation transparente en aval des paquets de messagerie IGMP [RFC 2236] et des paquets IP multidiffusés en aval. En outre, lorsqu'il est en mode d'acheminement transparent C-NAT/C-NAPT, le portail CAP effectue la conversion d'adresse dans les messages IGMP amont issus des dispositifs IP de réseau local résidant dans le domaine du réseau LAN-Trans. Le portail CAP réexpédie le trafic IGMP provenant du réseau régional vers le réseau local afin de permettre aux notifications d'atteindre les dispositifs IP de réseau local. Un dispositif IP de réseau local déterminera à quelle multidiffusion il souhaite se joindre et va envoyer un message multidiffusé "d'entrée en participation". La source multidiffusée sera alors capable de communiquer des données au dispositif IP de réseau local. Quand le service de multidiffusion n'est plus désiré, le dispositif IP de réseau local peut soit ignorer ce service (dont le flux arrivera en fin de temporisation) ou envoyer un message IGMP de "sortie de participation" à la chaîne afin de libérer le flux de trafic. La Figure 8-3 offre un exemple détaillé des processus IGMP et multidiffusés passant à travers un dispositif PS.

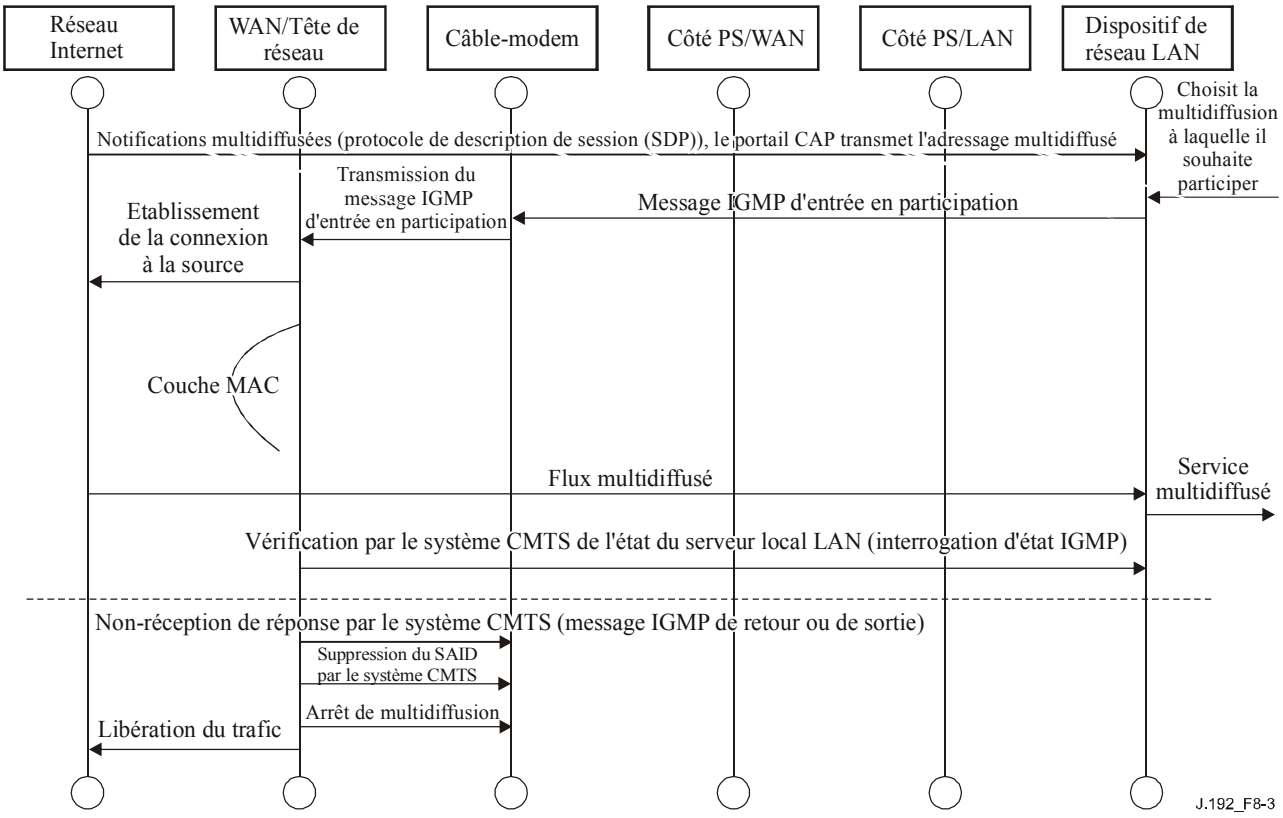


Figure 8-3/J.192 – Séquence de multidiffusion par protocole IGMP

{texte informatif:

8.3.3.7 Configuration de conversion C-NAPT utilisant le service UPnP de connexion IP par réseau régional

Le dispositif PS implémente le service UPnP de connexion IP par réseau régional (UWIC) afin de permettre à des applications de réseau local conformes au modèle UPnP de configurer des mappages de port au portail CAP.

Le dispositif PS déclare le service UPnP de connexion IP par réseau régional (UWIC) dans la description UPnP de dispositif de passerelle Internet (IGD). Le dispositif PS n'annonce le service de connexion IP par réseau régional que quand il fonctionne en mode de conversion NAPT.

8.3.3.7.1 Relation entre variables de connexion IP par réseau régional et objets de table cabhCapMappingTable

Le dispositif PS énumère tous les mappages de conversion d'adresse de couche Réseau dans la table cabhCapMappingTable. Il s'agit des mappages créés par gestion au moyen du protocole SNMP, par le dispositif PS dynamiquement et par des dispositifs de réseau local au moyen du modèle UPnP. Plusieurs objets contenus dans la table cabhCapMappingTable ont une variable de mise en correspondance qui est définie dans la spécification du service UPnP de dispositif de passerelle Internet (UIGD). Les relations entre les objets de table cabhCapMappingTable et les variables du service de connexion IP par réseau régional sont représentées dans le Tableau 8-2.

Tableau 8-2/J.192 – Relation entre objets cabhCapMappingTable et variables du service de connexion IP par réseau régional

cabhCapMappingTable	WANIPConnection
cabhCapMappingWanAddr	ExternalIpAddress
cabhCapMappingWanPort	ExternalPort
cabhCapMappingLanAddr	InternalClient
cabhCapMappingLanPort	InternalPort
cabhCapMappingProtocol	PortMappingProtocol
cabhCapMappingCreateTime	N/A
cabhCapMappingLastUpdate	N/A
cabhCapMappingDuration	PortMappingLeaseDuration
cabhCapMappingRowDescription	PortMappingDescription
cabhCapMappingNumPorts	N/A
cabhCapMappingMethod	N/A
cabhCapMappingRemoteHost	RemoteHost
CabhCapMappingEnable	PortMappingEnabled
(N/A non disponible)	

Le paragraphe suivant décrit la façon dont le dispositif PS utilise ces variables et objets dans le contexte des actions du service de connexion IP par réseau régional.

8.3.3.7.2 Analyse des actions

Le dispositif PS n'active le service de connexion IP par réseau régional que quand il fonctionne en mode de conversion NAPT. Dans tous les autres modes (c'est-à-dire le mode de conversion NAT, le mode de transfert ou le mode désactivé) le dispositif PS désactive le service de connexion IP par réseau régional.

Le dispositif PS implémente les actions suivantes du service de connexion IP par réseau régional afin de permettre aux dispositifs UPnP de créer, de modifier, de supprimer et de lire les mappages de port: GetNATRSIPStatus, AddPortMapping, DeletePortMapping, GetGenericPortMappingEntry, GetSpecificPortMappingEntry et GetExternalIpAddress.

Le dispositif PS implémente l'action GetNATRSIPStatus (conformément au service UWIC) afin de signaler – à un point de commande UPnP qui en présente la requête – si la conversion NAPT est activée ou non. La réponse du dispositif PS à cette action va dépendre de la question de savoir si le

dispositif présentant la requête est dans le domaine LAN-Trans ou LAN-Pass. Pour les dispositifs situés dans le domaine LAN-Trans, le dispositif PS va répondre que la conversion NAPT est activée et pour les dispositifs situés dans le domaine LAN-Pass va répondre que la conversion NAPT est désactivée.

Les points de commande UPnP peuvent créer de nouveaux mappages dans le dispositif PS en invoquant l'action AddPortMapping. Le dispositif PS montre les mappages créés au moyen de cette action dans la table cabhCapMappingTable avec une valeur de l'objet cabhCapMappingMethod égale à UPnP(3). Le dispositif PS crée un nouveau mappage quand les variables ExternalPort et PortMappingProtocol de l'action ne concordent pas avec un port et avec un protocole actuellement en usage, comme défini dans le modèle UPnP. Le dispositif PS crée également un nouveau mappage si les variables d'action concordent avec un port externe, avec un protocole de mappage de port et avec un client interne du mappage existant mais ne concordent pas avec le serveur local de l'autre extrémité, indiqué par ce mappage.

Les points de commande peuvent modifier les mappages de conversion NAPT dans le dispositif PS au moyen de l'action AddPortMapping. Comme défini dans le modèle UPnP, l'action spécifie un mappage déjà existant quand les variables RemoteHost, ExternalPort, PortMappingProtocol et InternalClient concordent avec le mappage. Le dispositif PS n'autorise les points de commande à modifier que les mappages créés au moyen du modèle UPnP. Le dispositif PS n'autorise pas les points de commande à modifier les mappages qui ont été créés dans le dispositif PS au moyen du protocole SNMP. Le dispositif PS, dès réception d'une action AddPortMapping qui concorde avec une entrée courante qui a été créée au moyen du protocole SNMP, ne modifiera pas cette entrée mais renverra un message "OK" en réponse à l'action.

Les points de commande peuvent invoquer l'action DeletePortMapping afin d'éliminer un mappage dans le dispositif PS. Quand cette action est exécutée, le dispositif PS supprime un mappage si celui-ci a été créé au moyen du modèle UPnP. Sinon le dispositif PS ne supprime pas le mappage et renvoie une erreur.

Quand un point de commande invoque l'action GetGenericPortMappingEntry, le dispositif PS renvoie les mappages qu'il a créés dynamiquement et ceux qui ont été créés dans le dispositif PS au moyen du protocole SNMP ou UPnP. Plus spécifiquement, le dispositif PS renverra tous les mappages dont l'objet cabhCapMappingProtocol a la valeur UDP(3) ou TCP(4) dans la table cabhCapMappingTable. Pour les mappages que le dispositif PS a créés dynamiquement ou qui ont été créés dans le dispositif PS au moyen du protocole SNMP, le dispositif PS renvoie pour la variable RemoteHost une chaîne vide et pour la variable PortMappingEnabled une valeur 1 (True).

Dès réception d'une action GetSpecificPortMappingEntry, le dispositif PS vérifie les entrées de la table cabhCapMappingTable et renvoie l'entrée qui, le cas échéant, concorde avec les paramètres d'entrée des actions RemoteHost, ExternalPort et PortMappingProtocol.

En réponse à une action GetExternalIPAddress, le dispositif PS renvoie l'adresse IP actuelle du réseau WAN-Data.

}

8.3.3.8 Exemples de traitement de paquet IPCable2Home

Le présent paragraphe offre quelques informations sur les processus impliqués dans le traitement de paquet. La Figure 8-4 montre un exemple d'étapes possibles de traitement de paquet pour le trafic unidiffusé de réseau local à réseau régional et la Figure 8-5 montre un exemple d'étapes possibles de traitement de paquet pour le trafic unidiffusé de réseau régional à réseau local.

NOTE – Ces exemples ne sont qu'informatifs et n'impliquent aucune obligation quant à leur implémentation.

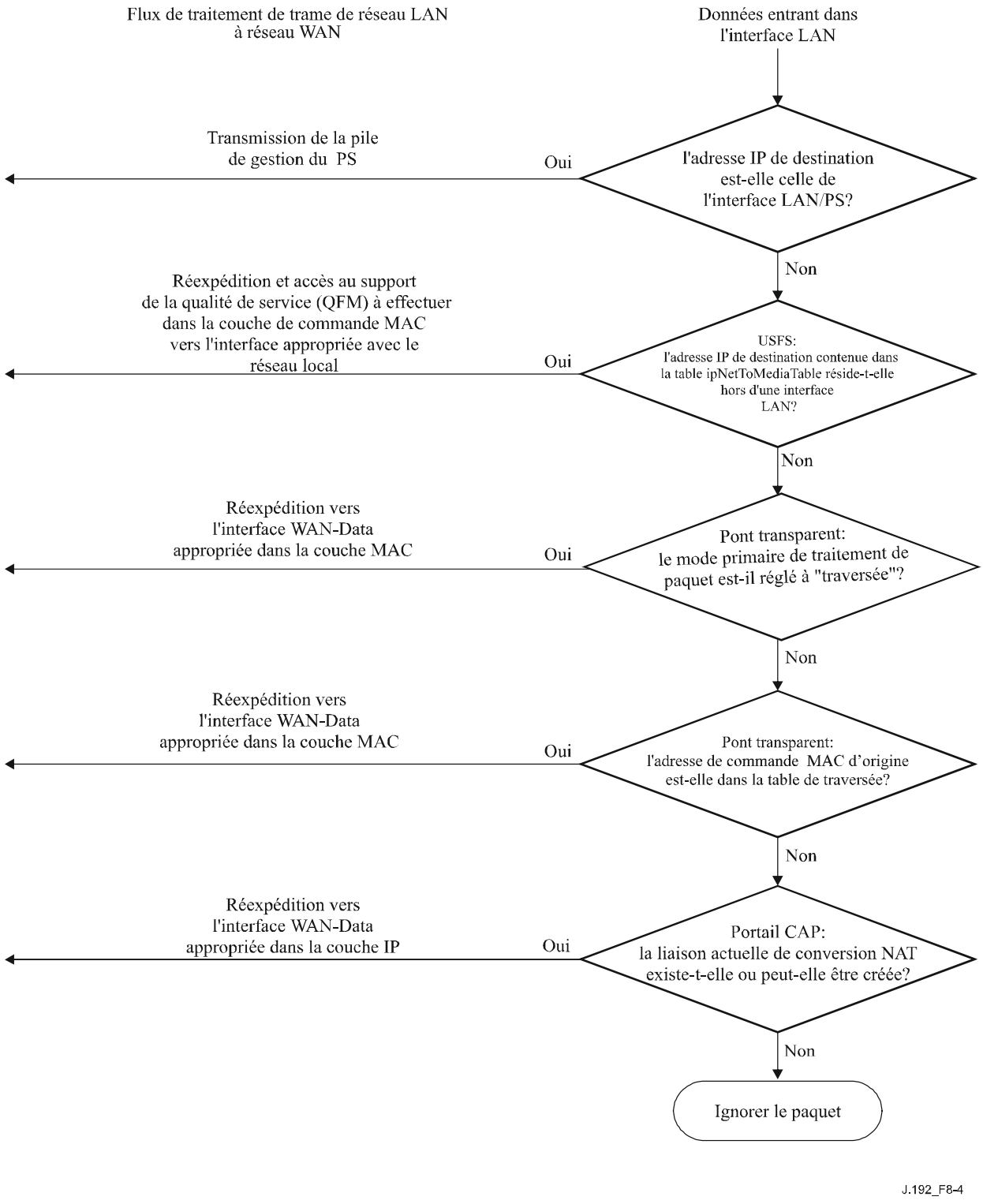


Figure 8-4/J.192 – Exemple de traitement de paquet de réseau local à réseau régional

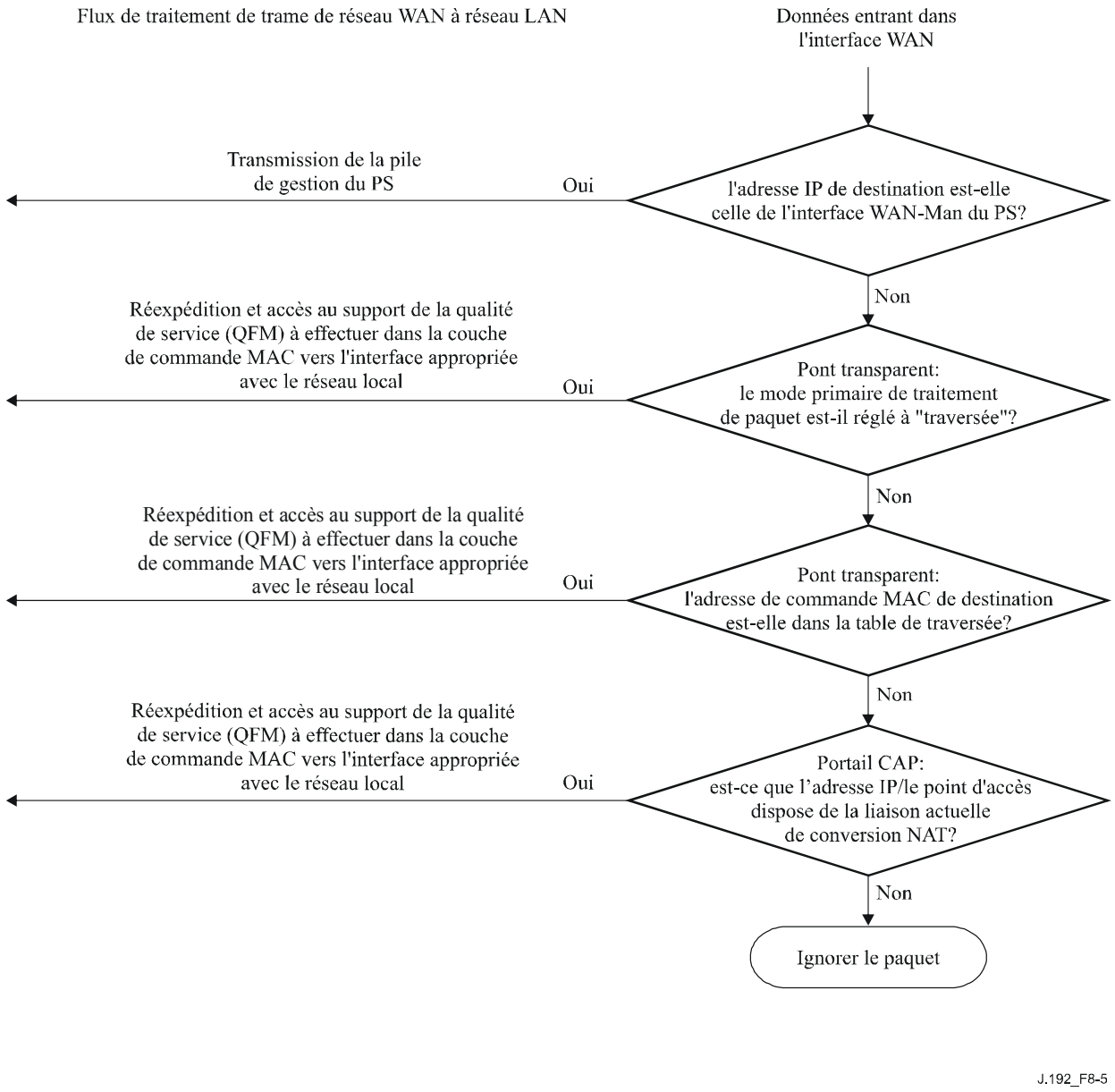


Figure 8-5/J.192 – Exemple de traitement de paquet de réseau régional à réseau local

8.3.4 Exigences relatives au portail CAP

8.3.4.1 Exigences générales

Toutes les interfaces IP logiques avec l'élément de services de portail DOIVENT être conformes aux documents [RFC 1122] et [RFC 1123], sections 3 et 4, afin d'activer les communications normalisées avec les serveurs locaux Internet.

Le dispositif PS DOIT prendre en charge le trafic multidiffusé de réseau régional à réseau local par dérivation transparente des paquets IP de messagerie IGMP de réseau régional à réseau local et des paquets IP de multidiffusion de réseau régional à réseau local comme défini dans [RFC 2236].

Si le mode primaire de traitement de paquet, objet cabhCapPrimaryMode, est réglé à "transfert", toute la messagerie IGMP de réseau local à réseau régional DOIT être dérivée en transparence.

Si le mode primaire de traitement de paquet, objet cabhCapPrimaryMode, est réglé à C-NAPT, l'adresse IP d'origine, pour tous les messages IGMP de réseau local à réseau régional provenant de dispositifs IP de réseau local résidant dans le domaine du réseau LAN-Trans, DOIT être convertie

en l'adresse IP de réseau WAN-Data utilisée pour les mappages C-NAPT puis être réexpédiée vers le réseau régional.

Si le mode primaire de traitement de paquet, objet cabhCapPrimaryMode, est réglé à C-NAT, l'adresse IP d'origine – pour tous les messages IGMP de réseau local à réseau régional provenant de dispositifs IP de réseau local résidant dans le domaine du réseau LAN-Trans et ayant une adresse IP faisant partie d'un mappage C-NAT existant – DOIT être convertie en l'adresse IP de réseau WAN-Data utilisée pour les mappages C-NAT puis être réexpédiée vers le réseau régional.

8.3.4.2 Exigences relatives au traitement des paquets

Le dispositif PS DOIT prendre en charge le mode de transfert, le mode d'acheminement transparent C-NAT et le mode d'acheminement transparent C-NAPT. Le dispositif PS DOIT prendre en charge la sélection de ce mode primaire de traitement de paquet par l'objet cabhCapPrimaryMode de base MIB.

Si le mode primaire de traitement de paquet, objet cabhCapPrimaryMode, est réglé à C-NAT, le dispositif PS DOIT s'assurer qu'il existe une adresse IP disponible fournie par la tête de réseau dans la réserve d'adresses IP de réseau WAN-Data (avec une location DHCP en cours) avant d'essayer d'utiliser cette adresse IP en tant que partie d'un mappage C-NAT. Si le portail CAP n'est pas en mesure de créer un mappage C-NAT du fait de la réduction de la réserve d'adresses IP de réseau WAN-Data, ce portail DOIT produire un événement normalisé (comme défini dans l'Annexe B).

Pour chaque mappage dynamique C-NAT qu'il crée, le dispositif PS DOIT régler à 0 les numéros de port aux réseaux WAN et LAN (objets cabhCapMappingWanPort et cabhCapMappingLanPort, respectivement) de la table de mappage du portail CAP.

Si le câblo-opérateur crée ou modifie une rangée dans la table de mappage du portail CAP, c'est-à-dire si une rangée est créée par la méthode de mappage statique (objet cabhCapMappingMethod à la valeur = static(1)) et si les objets de numéro de port de la rangée (objets cabhCapMappingLanPort et cabhCapMappingWanPort) ne sont pas spécifiés, le dispositif PS DOIT introduire zéro pour les objets cabhCapMappingLanPort et cabhCapMappingWanPort dans cette rangée.

Le dispositif PS NE DOIT PAS convertir le numéro de port d'un paquet dont l'adresse IP figure dans la table de mappage du portail CAP avec un numéro de port égal à zéro.

Si le mode primaire de traitement de paquet, cabhCapPrimaryMode, est réglé à C-NAPT, le dispositif PS DOIT s'assurer qu'il existe une adresse IP de réseau régional en cours (avec une location DHCP en cours venant de la préconfiguration par la tête de réseau) avant d'essayer d'utiliser cette adresse IP en tant que partie d'un mappage C-NAPT. Si le portail CAP n'est pas en mesure de créer un mappage C-NAPT du fait qu'il ne possède pas d'adresse IP de réseau régional en cours ou du fait qu'il manque des numéros de port, ce portail DOIT produire un événement normalisé (comme défini dans l'Annexe B).

Le trafic unidiffusé de réseau local à réseau local NE DOIT jamais être acheminé ou dérivé à la sortie d'une interface avec un réseau régional.

Quand la location DHCP d'une adresse IP de réseau WAN-Data – faisant partie d'un mappage de conversion C-NAT ou C-NAPT – arrive à expiration, tous les mappages associés à cette adresse IP DOIVENT être supprimés de l'objet cabhCapMappingTable.

8.3.4.3 Exigences relatives au mode de transfert

Quand le mode primaire de traitement de paquet du portail CAP, cabhCapPrimaryMode, est réglé à "transfert", le dispositif PS DOIT jouer le rôle d'un pont transparent, comme défini dans la norme [ISO/CEI 10038] Contrôle d'accès au support (MAC) – Ponts entre le secteur WAN-Data et le secteur LAN-Pass et NE DOIT PAS exécuter de fonctions d'acheminement transparent C-NAT ou C-NAPT. Un dispositif PS agissant comme un pont transparent pour les dispositifs du secteur

LAN-Pass (cabhCapPrimaryMode = transfert(3) ou cabhCapPrimaryMode = napt(1) avec des entrées dans la table cabhCapPassthroughTable) DOIT assurer le routage transparent de tous les types de trame que les spécifications DOCSIS obligent un câblo-modem à transmettre. Même quand le mode primaire de traitement de paquet est réglé à "transfert", le traitement par la fonction USFS DOIT avoir priorité sur les décisions de routage de réseau local à réseau régional .

8.3.4.4 Exigences relatives à l'acheminement transparent C-NAT et C-NAPT

Quand le mode primaire de traitement de paquet (objet cabhCapPrimaryMode) est réglé à "C-NAT", le dispositif PS DOIT prendre en charge les processus de conversion d'adresse C-NAT conformément aux exigences de base concernant la conversion C-NAT, définies dans le document [RFC 3022].

Quand le mode primaire de traitement de paquet (objet cabhCapPrimaryMode) est réglé à "C-NAPT", le dispositif PS DOIT prendre en charge les processus de conversion d'adresse C-NAPT conformément aux exigences de base concernant la conversion C-NAPT, définies dans le document [RFC 3022].

Sans tenir compte du mode primaire de traitement de paquet, le dispositif PS DOIT prendre en charge la création et la suppression des mappages statiques de conversion C-NAT et C-NAPT, en permettant au système NMS de lire, de créer et de supprimer (par le portail CMP) les entrées de mappage statique de portail CAP (objet cabhCapMappingTable).

Les mappages statiques de conversion C-NAT et C-NAPT créés par le système NMS DOIVENT persister au-delà des réamorçages du dispositif PS.

Le dispositif PS DOIT prendre en charge la création de mappages dynamiques de conversion C-NAT et C-NAPT, lancée par trafic en protocole TCP, UDP ou ICMP de réseau local à réseau régional. Le dispositif PS DOIT permettre au système NMS de lire (par le portail CMP) les entrées de mappage dynamique par portail CAP (objet cabhCapMappingTable).

Le dispositif PS DOIT prendre en charge la suppression de mappages dynamiques de conversion C-NAT et C-NAPT si un mappage donné est associé à une session en protocole TCP et que cette session TCP se termine ou que la temporisation de la période d'inactivité TCP, cabhCapTcpTimeWait, arrive à expiration pour ce mappage.

Le dispositif PS DOIT prendre en charge la suppression de mappages dynamiques de conversion C-NAT et C-NAPT si un mappage donné est associé à une session UDP et que la temporisation de la période d'inactivité UDP, cabhCapUdpTimeWait, arrive à expiration pour ce mappage.

Le dispositif PS DOIT prendre en charge la suppression de mappages dynamiques de conversion C-NAT et C-NAPT si un mappage donné est associé à une session ICMP et que la temporisation de la période d'inactivité ICMP, cabhCapIcmpTimeWait, arrive à expiration pour ce mappage.

Les mappages dynamiques de conversion C-NAT et C-NAPT NE DOIVENT PAS persister au-delà des réamorçages.

Une correspondance (ou "mappage") est créée dans la table de mappage du portail CAP (cabhCapMappingTable) entre d'une part l'adresse IP privée d'un dispositif IP de réseau local du secteur LAN-Trans et un numéro de port (paire privée: cabhCapMappingLanAddr et cabhCapMappingLanPort) et d'autre part une adresse IP publique et un numéro de port (paire publique: cabhCapMappingWanAddr et cabhCapMappingWanPort), correspondant à une session établie par le dispositif IP de réseau local. La combinaison paire privée – paire publique est désignée par le terme d'association de conversion ou de mappage. L'association de conversion est représentée comme une entrée dans la table de mappage du portail CAP. Elle est créée automatiquement par le dispositif PS quand le dispositif IP de réseau local du secteur LAN-Trans envoie du trafic destiné à un dispositif du réseau régional en faisant jouer au dispositif PS le rôle de passerelle par défaut du dispositif IP de réseau local. Cette association est créée automatiquement

par le dispositif PS dans les conditions de prise en charge définies au § 8.3.3.7 {texte informatif: service UPnP de connexion IP par réseau régional (UWIC)}, ou par configuration directe de la table de mappage du portail CAP au moyen d'un fichier de configuration PS ou au moyen de messages de requête de mise à jour SET du protocole SNMP. Les mappages d'adresse IP de conversion C-NAT ou C-NAPT (paires publiques et privées et associations de conversion) DOIVENT être cohérents et ne pas changer dans un dispositif IP de réseau local une fois qu'ils ont été créés et avant qu'ils soient détruits.

Chaque paire privée d'une entrée dans la table de mappage du portail CAP DOIT avoir la même paire publique correspondante chaque fois qu'elle apparaît dans la table de mappage du portail CAP, quelle que soit la valeur d'adresse IP du serveur local à l'autre extrémité (cabhCapMappingRemoteHostAddr) pour cette entrée. C'est-à-dire qu'une paire privée est tenue de toujours être associée à la même paire publique. Cette restriction interdit l'implémentation d'une conversion NAT symétrique comme décrit dans [RFC 3489].

Si un mappage existe dans la table de mappage du portail CAP pour un dispositif IP de réseau local dans le secteur LAN-Trans avec une valeur particulière d'adresse cabhCapMappingRemoteHostAddr, et si du trafic arrive à l'interface du dispositif PS avec le réseau local en provenance de ce même dispositif IP de réseau local avec la même adresse IP d'origine et le même numéro de port d'origine mais à destination d'une autre adresse IP de serveur local à l'autre extrémité, alors ce dispositif PS DOIT créer une nouvelle entrée dans la table de mappage du portail CAP avec la même paire privée (cabhCapMappingLanAddr et cabhCapMappingLanPort) et la même paire publique (cabhCapMappingWanAddr et cabhCapMappingWanPort), ainsi qu'avec une entrée cabhCapMappingRemoteHostAddr ayant la valeur de la nouvelle adresse IP de destination. C'est-à-dire que, pour la même paire privée, le dispositif PS est tenu d'utiliser la même paire publique pour l'association. Le dispositif PS est donc tenu de créer une nouvelle entrée unique dans la table de mappage du portail CAP avec une valeur différente d'adresse IP de serveur local à l'autre extrémité, mais avec la même association de conversion privée-publique qu'à l'entrée précédente. Le résultat pourrait être que l'association privée-publique (paire privée et paire publique dans une entrée de la table de mappage du portail CAP) apparaisse de multiples fois dans la table de mappage du portail CAP, mais avec une valeur différente d'adresse IP de serveur local à l'autre extrémité pour chaque entrée.

8.3.4.5 Exigences relatives à la prise en charge d'un réseau privé virtuel

Quand le portail CAP doit fonctionner en mode primaire de traitement de paquet pour conversion C-NAT ou C-NAPT (ce qui est indiqué par la valeur de l'objet cabhCapPrimaryMode), le dispositif PS DOIT reconnaître les sessions IPSec lancées par des clients de réseau privé virtuel dans le secteur LAN-Trans, créer les mappages appropriés dans la table de mappage du portail CAP et appliquer le port 500 au trafic entrant (de réseau régional à réseau local) vers l'adresse IP de réseau LAN-Trans associée au dispositif IP de réseau local qui a lancé la session.

Quand le portail CAP doit fonctionner en mode primaire de traitement de paquet pour conversion C-NAT ou C-NAPT (ce qui est indiqué par la valeur de l'objet cabhCapPrimaryMode) et qu'il reconnaît une session IPSec tandis qu'une autre a déjà été mappée dans la table de mappage du portail CAP vers un autre serveur VPN, le dispositif PS peut créer des mappages pour la nouvelle session, p. ex. par transfert de port.

Si le trafic entrant au port 500 est reçu par le portail CAP et qu'il n'y ait aucune session VPN active en protocole IPSec, alors les paquets reçus par le port 500 DOIVENT être rejetés.

Le dispositif PS DOIT prendre en charge les sessions IPSec au moyen du mode de mise en tunnel de la charge utile de sécurité par encapsulage [RFC 2406].

8.3.4.6 Exigences relatives à la fonctionnalité de zone DMZ au portail CAP

Quand le mode primaire de traitement de paquet (objet cabhCapPrimaryMode) est réglé à "C-NAPT" et qu'il y a une liaison statique de conversion C-NAPT avec le numéro de port du réseau régional et du réseau local réglé à 0 (c'est-à-dire lorsqu'une entrée de zone DMZ a été créée dans le portail CAP), alors le dispositif PS DOIT convertir les adresses IP spécifiées dans le mappage (entrée DMZ) pour les paquets qui ne sont pas associés à un mappage dynamique ou statique de conversion C-NAPT existante.

Quand une entrée de zone DMZ est créée dans la table de mappage du portail CAP pour une adresse IP de réseau local qui est dynamiquement assignée par le dispositif PS (serveur CDS), le dispositif PS DOIT créer une réservation de location pour cette adresse IP. Le dispositif PS DOIT déterminer si l'adresse IP de zone DMZ est dynamiquement assignée par le serveur CDS, p. ex. en le recherchant dans la table d'objets cabhCdpLanAddrTable. Si une entrée correspondante existe dans cette table avec la valeur de l'objet cabhCdpLanAddrMethod égale à dynamicActive(4) ou à dynamicInactive(3), alors le dispositif PS DOIT remplacer cette entrée par une autre qui représente une réservation de location pour cette adresse IP dans la table, c'est-à-dire par une entrée dont la valeur cabhCdpLanAddrMethod est réglée soit à psReservationActive(6) ou à psReservationInactive(5), selon le cas. S'il n'y a pas d'entrée dans la table de mappage du portail CAP correspondant à l'adresse IP de zone DMZ figurant dans la table d'objets cabhCdpLanAddrTable, alors le dispositif PS NE DOIT PAS créer de réservation de location pour cette adresse IP.

Quand une entrée de zone DMZ est supprimée de la table cabhCapMappingTable pour une adresse IP de réseau local (serveur local de zone déclassifiée), le dispositif PS DOIT supprimer la réservation de location d'adresse IP correspondante qu'il avait créée au niveau interne (identifiée par cabhCdpLanAddrMethod=psReservationActive(6)) dans la table cabhCdpLanAddrTable aussi longtemps que la table docsDevFilterIpTable ou cabhSec2FwLocalFilterIpTable ne possède pas d'entrée correspondante contenant une règle de filtrage de pare-feu qui l'exige.

8.3.4.7 Exigences relatives au mode mixte de routage/acheminement

Le dispositif PS DOIT prendre en charge le mode mixte de routage/acheminement comme décrit dans le § 8.3, dans lequel le mode primaire de traitement de paquet par le portail CAP, objet cabhCapPrimaryMode, est réglé à l'acheminement transparent C-NAT ou C-NAPT et dans lequel le portail CAP va également dériver en transparence du trafic pour des adresses MAC particulières. Si le mode primaire de traitement de paquet par le portail CAP, objet cabhCapPrimaryMode, est réglé à l'acheminement transparent C-NAT ou C-NAPT et si le système NMS a écrit dans l'objet cabhCapPassthroughTable une adresse MAC appartenant à un dispositif IP de réseau local, le dispositif PS DOIT dériver en transparence le trafic de réseau local à réseau régional issu de cette adresse de commande MAC, ainsi que le trafic de réseau régional à réseau local destiné à cette adresse MAC.

En mode mixte de routage/acheminement, comme décrit dans le § 8.3, la fonction de commutation USFS DOIT être appliquée à tout le trafic reçu d'un réseau local.

8.3.4.8 Exigences relatives à la commutation USFS

La fonctionnalité de commutation de réexpédition sélective en amont (USFS) DOIT être appliquée au traitement des paquets sans tenir compte du mode de traitement des paquets du portail CAP (transfert, C-NAT, C-NAPT, ou mode mixte de routage/acheminement).

La fonction de commutation USFS DOIT inspecter tout le trafic IP provenant des interfaces PS LAN, afin de déterminer si l'adresse IP de destination d'un paquet est celle d'un dispositif résidant dans une interface PS/LAN. Si l'adresse IP de destination contenue dans un paquet inspecté par la commutation USFS est celle d'un dispositif IP de réseau local résidant hors d'une interface PS LAN, la fonction de commutation USFS DOIT remplacer l'adresse de destination de couche

MAC, dans l'en-tête de couche 2 du paquet, par l'adresse de couche MAC de ce dispositif IP de réseau local de destination et réexpédier la trame vers l'entité de réexpédition/accès au support de la qualité de service (QFM) (voir § 10.3.1) située dans le dispositif PS, en vue de sa réexpédition à la sortie de l'interface physique appropriée avec un réseau local, selon la priorité des paquets.

La fonction de commutation USFS NE DOIT PAS réexpédier de paquets destinés à un dispositif IP de réseau local, à la sortie d'une quelconque interface avec un réseau régional.

{texte informatif:

8.3.4.9 Exigences relatives à la configuration de conversion C-NAPT utilisant le service UPnP de connexion IP par réseau régional

Le dispositif PS DOIT implémenter le service de connexion IP par réseau régional d'un dispositif de passerelle Internet comme défini dans le document relatif à la connexion UWIC (UPnP WAN IP Connection).

Le dispositif PS ne DOIT autoriser le service de connexion IP par réseau régional que quand il fonctionne en mode de conversion NAPT (cabhCapPrimaryMode = napt(1)) et que quand cabhCapUpnpPortForwardingEnable = true(1). Le dispositif PS NE DOIT PAS autoriser le service de connexion IP par réseau régional quand il fonctionne en mode de conversion NAT, en mode de transfert, ou en mode désactivé, ni quand cabhCapUpnpPortForwardingEnable = false(2). Chaque fois que le service de connexion IP par réseau régional est désactivé, le dispositif PS DOIT éliminer tous les mappages créés au moyen de ce service.

Quand le dispositif PS est configuré en mode de conversion NAPT, il DOIT prendre en charge les actions suivantes de connexion IP par réseau régional (UWIC) afin de permettre aux dispositifs UPnP de créer, de modifier, de supprimer et de lire les mappages de port: GetNATRSIPStatus, AddPortMapping, DeletePortMapping, GetGenericPortMappingEntry, GetSpecificPortMappingEntry et GetExternalIPAddress.

Si le dispositif PS est configuré en mode de conversion NAPT et reçoit une demande GetNATRSIPStatus issue d'un dispositif situé dans le domaine LAN-Trans, il DOIT répondre que la conversion NAT est activée. Si le dispositif PS est configuré en mode de conversion NAPT et reçoit une demande GetNATRSIPStatus issue d'un dispositif situé dans le domaine LAN-Pass, il DOIT répondre que la conversion NAT est désactivée.

Le dispositif PS DOIT énumérer les mappages créés au moyen de l'action AddPortMapping dans la table d'objets cabhCapMappingTable avec une valeur de méthode cabhCapMappingMethod égale à UPnP(3). Le dispositif PS DOIT créer un nouveau mappage quand les variables ExternalPort et PortMappingProtocol de l'action AddPortMapping ne concordent ni avec un port ni avec un protocole actuellement en usage dans un autre mappage. Le dispositif PS DOIT créer un nouveau mappage si les variables d'action concordent avec un port externe, un protocole de mappage de port et un client interne d'un mappage existant, mais ne concordent pas avec le serveur distant qui est indiqué par ce mappage.

Le dispositif PS DOIT permettre aux points de commande de modifier, au moyen de l'action AddPortMapping (UWIC), les mappages qui ont une valeur de méthode cabhCapMappingMethod égale à UPnP(3). Le dispositif PS est censé comprendre que l'action AddPortMapping se rapporte à un mappage déjà existant quand les variables d'action RemoteHost, ExternalPort, PortMappingProtocol et InternalClient concordent avec ce mappage. Le dispositif PS NE DOIT PAS modifier les mappages avec une méthode cabhCapMappingMethod de valeur static(1) en réponse à l'action AddPortMapping. Si l'action AddPortMapping spécifie un mappage existant avec une méthode cabhCapMappingMethod de valeur static(1), le dispositif PS DOIT toutefois renvoyer un message "OK" en réponse à cette action.

Quand l'action DeletePortMapping est invoquée, le dispositif PS DOIT supprimer un mappage qui concorde avec la demande si ce mappage possède une méthode cabhCapMappingMethod de valeur

UPnP(3). Si le mappage à supprimer possède une méthode cabhCapMappingMethod de valeur static(1) ou dynamic(2), le dispositif PS DOIT ignorer l'action DeletePortMapping et renvoyer le code d'erreur UPnP 501 (action échouée).

Quand un point de commande invoque l'action GetGenericPortMappingEntry, le dispositif PS DOIT renvoyer tous les mappages contenus dans la table d'objets cabhCapMappingTable avec un protocole cabhCapMappingProtocol de valeur UDP(3) ou TCP(4).

Dès réception d'une action GetSpecificPortMappingEntry, le dispositif PS DOIT vérifier les entrées de la table cabhCapMappingTable et renvoyer l'entrée, le cas échéant, qui concorde avec les paramètres d'entrée des actions RemoteHost, ExternalPort et PortMappingProtocol.

En réponse à une action GetExternalIPAddress, le dispositif PS DOIT renvoyer l'adresse IP actuelle du réseau WAN-Data.

}

9 Résolution du nom

9.1 Introduction/Aperçu général

9.1.1 Objectifs

Les objectifs de résolution du nom sont les suivants:

- offrir, aux clients du service DNS situés dans des dispositifs IP de réseau local, le service de nom de domaine (DNS, *domain name service*) à partir d'un serveur situé dans le dispositif PS, même pendant les coupures de connexion du câble;
- permettre aux abonnés de désigner des dispositifs locaux au moyen de noms de dispositif ayant une signification intuitive plutôt que par adresse IP;
- fournir, par interrogations récurrentes à des serveurs DNS (distants), des réponses aux clients DNS de réseau local lors d'interrogations portant sur la résolution de noms non locaux de serveurs locaux;
- offrir une récupération aisée du service DNS lors d'un rétablissement de connexité du câble après une coupure.

9.1.2 Hypothèses

Les hypothèses de fonctionnement des services de nommage sont les suivantes:

- le serveur DNS situé dans l'élément de services de portail est le seul serveur DNS qui fait foi pour les dispositifs IP de réseau local situés le secteur LAN-Trans;
- l'élément de services de portail ne fournira pas le service DNS aux dispositifs IP de réseau local situés dans le secteur LAN-Pass;
- si l'élément de services de portail utilise de multiples adresses de réseau WAN-Data, les informations de serveur DNS du réseau régional obtenues pendant le plus récent processus d'acquisition d'adresse de réseau WAN-Data (DHCP) seront utilisées.

9.2 Architecture

9.2.1 Directives de conception du système

Voir le Tableau 9-1.

Tableau 9-1/J.192 – Résolution du nom: directives de conception du système

Référence	Directives
Résolution de nom 1	Offrir le service de nom de domaine à partir d'un serveur situé dans le dispositif PS aux clients du service DNS situés dans des dispositifs IP de réseau local, pour résolution du nom de dispositifs IP de réseau local (indépendamment de l'état de la connexion du réseau régional).
Résolution de nom 2	Offrir des réponses DNS, par interrogations récurrentes commençant par un serveur DNS du réseau câblé, à des clients DNS situés dans des dispositifs IP de réseau local, pour la résolution de noms non locaux de serveurs locaux.

9.2.2 Description du système

Le présent paragraphe offre un aperçu général des services IPCable2Home de résolution de nom dans l'élément de services de portail.

9.2.2.1 Aperçu général fonctionnel de la résolution de nom

Le portail de nommage IPCable2Home (CNP) est un service fonctionnant dans le dispositif PS qui offre un simple serveur DNS aux dispositifs IP de réseau local situés dans le secteur d'adresses du réseau LAN-Trans. Cependant, la fonctionnalité de portail CNP pour le secteur d'adresses de réseau LAN-Trans est contournée si la table d'objets de base MIB cabhCdpServeurDnsAdresse est réglée à une valeur autre que cabhCdpServerRouter. Le portail CNP n'est pas utilisé par les dispositifs IP de réseau local situés dans le secteur d'adresses du réseau LAN-Pass, parce que ceux-ci seront directement desservis par des serveurs DNS extérieurs à la résidence.

En principe, les dispositifs IP de réseau local situés dans le secteur LAN-Trans sont configurés par le portail CDP de façon à utiliser le portail CNP comme leur serveur distant de noms de domaine. Le service de portail CNP dans le secteur LAN-Trans ne dépend pas de l'état de la connexion du réseau régional. Le portail CNP effectue les tâches suivantes:

- résolution des noms de serveur pour les dispositifs IP de réseau local, en retournant leurs adresses IP correspondantes;
- envoi de réponses DNS, par interrogations récurrentes commençant par un serveur DNS situé dans le réseau câblé, aux interrogations qui ne peuvent pas être résolues par les informations locales du dispositif PS. Cette action ne se produit que lorsque des informations de serveur DNS de réseau régional sont disponibles dans le dispositif PS. Sinon, le portail CNP renvoie une erreur indiquant que le nom ne peut pas être résolu.

Faire du portail CNP le serveur DNS primaire dans le réseau local évite d'avoir à reconfigurer les dispositifs IP de réseau local lors d'un changement d'état de la connexion du réseau régional. Cela permet également de modifier l'attribution de serveur DNS extérieur sans reconfiguration du dispositif IP de réseau local.

9.2.2.2 Fonctionnement de la résolution de nom

Lorsqu'elle est interrogée afin de résoudre un nom de serveur, la fonction de portail CNP du dispositif PS effectue le processus d'exploration qui est représenté dans la Figure 9-1. Le portail CNP répond aux interrogations initiales du service DNS normalisé [RFC 1035], dirigées vers l'objet cabhCdpServerDnsAddress, pour toutes les explorations de nom. Il appartient au portail CNP d'envoyer des interrogations récurrentes à des serveurs DNS externes – en commençant par la première entrée de l'objet cabhCdpWanDnsServerIp dans la table cabhCdpWanDnsServerTable du portail CDP – lors d'interrogations par un dispositif IP de réseau local. Il lui appartient également de répondre à ce dispositif IP de réseau local par un message de réponse ou d'erreur.

Le portail CNP repose sur la table cabhCdpLanAddrTable du portail CDP afin d'apprendre les noms de serveur associés aux adresses IP actuelles des dispositifs IP de réseau local actifs. Aussi

longtemps qu'un dispositif IP de réseau local conserve une location DHCP active avec le portail CDP et qu'il a offert un nom de serveur au portail CDP (au titre du processus d'acquisition de son adresse IP), son nom peut être résolu par le portail CNP. Si le nom de serveur dont la résolution est demandée ne peut pas être trouvé dans l'objet cabhCdpLanAddrTable, le portail CNP adresse des interrogations récurrentes à des serveurs DNS externes (dont le premier est appris par le client CDC par des options du protocole DHCP).

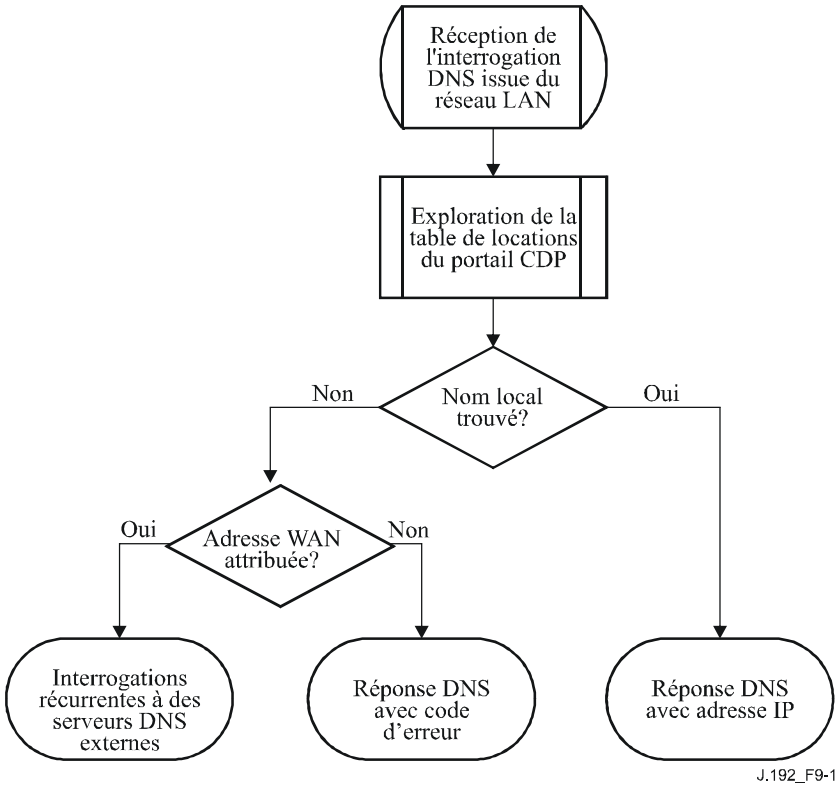


Figure 9-1/J.192 – Traitement de paquet au portail CNP

Une interrogation DNS normale spécifie un nom de domaine cible (QNAME), un type d'interrogation (QTYPE) et une classe d'interrogation (QCLASS). Elle demande des enregistrements de ressources qui correspondent. Le portail CNP répondra aux interrogations de serveur DNS par les champs QCLASS = IN et QTYPE = A, NS, SOA ou PTR comme défini dans le document [RFC 1035]. La prise en charge des transferts de zone et de service DNS par protocole TCP n'est pas requise.

Etant donné que le portail CNP est un serveur DNS qui fait foi à l'intérieur du secteur LAN-Trans, ce portail fournira sur demande les enregistrements de début d'autorisation (SOA, *start of authority*) et de serveur distant de noms autorisé (NS). Un exemple des champs d'enregistrement de début SOA (voir section 3.3.13 de [RFC 1035]) est reproduit ci-dessous:

Tableau 9-2/J.192 – Champs d'enregistrement SOA

Champ RDATA [RFC 1035]	Objet de base MIB de portail CDP IPCable2Home
MNAME	cabhCdpServerDomainName
RNAME	Non spécifié
SERIAL	Non spécifié
REFRESH	Non spécifié
RETRY	Non spécifié
EXPIRE	Non spécifié
MINIMUM	Non spécifié

Le champ MNAME est le nom de domaine du secteur d'adresses du réseau LAN-trans. Le portail CNP fait appel à la valeur mémorisée dans l'objet cabhCdpServerDomainName en tant que nom de domaine du secteur d'adresses LAN-trans.

Le champ RNAME est la boîte à lettres de la personne chargée du domaine. Si le dispositif PS conserve une adresse de courrier électronique pour un administrateur, ces informations pourront être spécifiées dans ce champ.

Le champ SERIAL est un nombre non signé de 32 bits, servant à identifier la version des informations de zone. Mais, dans la mesure où la présente Recommandation ne spécifie pas de transferts de zone, la valeur de ce champ n'est pas spécifiée.

9.3 Exigences relatives à la résolution du nom

Le portail CNP DOIT être conforme au format de message DNS normalisé et prendre en charge les interrogations DNS normalisées, comme décrit dans les documents [RFC 1034] et [RFC 1035].

Le portail CNP est un serveur sans états qui DOIT être capable de recevoir des interrogations et d'envoyer des réponses dans des paquets UDP [RFC 768].

Le portail CNP DOIT prendre en charge le mode récurrent, comme défini dans le document [RFC 1034].

Le portail CNP répond aux interrogations de nom en commençant par les informations locales contenues dans le dispositif PS et ses messages de réponse DOIVENT contenir une réponse ou une erreur.

Le portail CNP NE DOIT répondre qu'aux interrogations DNS qui sont envoyées à l'adresse IP représentée par la valeur de l'objet de base MIB cabhCdpServerRouter (c'est-à-dire l'adresse IP du côté réseau local du dispositif PS).

Le portail CNP NE DOIT PAS répondre aux interrogations DNS envoyées aux adresses IP des interfaces PS WAN-Man et PS WAN-Data.

Dès réception d'une interrogation initiale de résolution de nom de serveur à partir d'un dispositif IP de réseau local, le portail CNP DOIT accéder à la table cabhCdpLanAddrTable du portail CDP afin de rechercher les noms de serveur associés à des adresses IP louées à des dispositifs IP de réseau local.

Sans tenir compte de l'existence d'éventuelles entrées cabhCdpWanDnsServerIp dans la table cabhCdpWanDnsServerTable de base MIB du portail CDP, si le nom de serveur peut être résolu par le portail CNP à partir de données locales, le portail CNP DOIT répondre à l'interrogation de résolution de nom de serveur par l'adresse IP du dispositif IP de réseau local nommé.

Si le nom de serveur recherché ne peut pas être résolu par le portail CNP à partir de données locales et que la table cabhCdpWanDnsServerTable du portail CDP soit remplie avec au moins une seule

entrée cabhCdpWanDnsServerIp, la fonction de portail CNP du dispositif PS DOIT essayer de résoudre l'interrogation relative au nom de serveur au moyen d'interrogations récurrentes auprès de serveurs DNS externes, en commençant par des interrogations adressées au serveur DNS représenté par la première entrée de l'objet cabhCdpWanDnsServerIp dans la table cabhCdpWanDnsServerTable. Dans cette interrogation, le portail CNP DOIT utiliser l'adresse IP du réseau WAN-Data comme adresse IP d'origine pour le message d'interrogation DNS. Il est présumé que l'opérateur aura fourni une adresse IP publique comme adresse IP de réseau WAN-Data au portail CNP. Si tel n'est pas le cas, alors l'opérateur assurera le routage entre une adresse IP privée de réseau WAN-Data et le serveur DNS exploité par l'opérateur en tête de réseau.

Si le nom de serveur ne peut pas être résolu par le portail CNP à partir de données locales et qu'aucune entrée cabhCdpWanDnsServerIp n'existe dans l'objet cabhCdpWanDnsServerTable, la fonction de portail CNP du dispositif PS DOIT répondre à l'interrogation relative à la résolution du nom de serveur avec la valeur d'erreur appropriée, spécifiée par [RFC 1035].

Le portail CNP DOIT répondre aux interrogations DNS de type QCLASS = IN et des types QTYPE = A, NS, SOA ou PTR. SRV [RFC 2782] et ENUM [RFC 3761].

Les réponses du portail CNP aux interrogations DNS DOIVENT être conforme à la section 3.3 de [RFC 1035], avec le bit de réponse d'autorisation réglé à '1' dans la section d'en-tête (voir section 4.1.1 de [RFC 1035]).

Etant donné que le portail CNP est un serveur DNS qui fait foi à l'intérieur du secteur LAN-Trans, ce portail DOIT fournir sur demande les enregistrements de début d'autorisation (SOA) et de serveur distant de noms autorisé (NS). Les champs d'enregistrement SOA (voir section 3.3.13 de [RFC 1035]) DOIVENT contenir une entrée dans le champ MNAME qui soit égale à la valeur de l'objet de base MIB cabhCdpServerDomainName du portail CDP.

Si l'objet cabhCdpServerDomainName n'est pas réglé, le portail CNP DOIT continuer à offrir le service d'arbitrage de serveur DNS aux dispositifs IP de réseau local.

9.3.1 Enregistrement des types ENUM, NAPTR et SRV dans un serveur DNS

9.3.1.1 Interrogations et réponses de type ENUM au portail CNP [RFC 3761]

Le présent paragraphe décrit le comportement du portail CNP quand il reçoit des interrogations de serveur DNS de type ENUM en provenance de clients d'équipement CPE de réseau local.

Le portail CNP DOIT être en mesure d'accepter les interrogations de type ENUM issues des équipements CPE du réseau local et de les propager vers l'opérateur MSO au moyen de l'adresse cabhCdpWanDnsServerIp, quand cette base MIB est alimentée et que le serveur DNS de l'opérateur MSO est atteignable.

Le portail CNP DOIT essayer d'interroger le serveur DNS de l'opérateur MSO représenté dans la base cabhCdpWanDnsServerIp, afin de lui demander des enregistrements de conversion NAPT correspondant à l'interrogation DNS de type ENUM effectuée par l'équipement CPE de réseau local, comme spécifié dans [RFC 3761].

Si le portail CNP obtient des enregistrements de conversion NAPT pour l'interrogation de type ENUM, le portail CNP DOIT réexpédier ces enregistrements en transparence vers les clients d'équipement CPE de réseau local.

Le portail CNP n'est pas tenu d'implémenter le système de découverte par délégation dynamique (DDDS, *dynamic delegation discovery system*), comme spécifié dans les documents RFC 3401 à 3404. Il est suffisant que le portail CNP soit en mesure de propager les interrogations de serveur DNS de type ENUM vers les serveurs DNS d'opérateur MSO représentés dans la base cabhCdpWanDnsServerIp. Il est présumé que si un opérateur doit fournir à ses abonnés CableHome des services qui nécessitent la résolution d'interrogations de serveur DNS de type ENUM, alors cet

opérateur va offrir la capacité de résolution de ces interrogations ou aux serveurs DNS représentés dans la table d'objets de base MIB cabhCdpWanDnsServerIp.

9.3.1.2 Interrogations et réponses de type SRV au portail CNP [RFC 2782]

Le présent paragraphe décrit le comportement du portail CNP quand il reçoit des interrogations de serveur DNS de type SRV, en provenance de clients d'équipement CPE de réseau local.

Le portail CNP DOIT être en mesure d'accepter les interrogations de type SRV en provenance des équipements CPE du réseau local et de les propager vers l'opérateur au moyen de l'adresse cabhCdpWanDnsServerIp, quand cette base MIB est alimentée et que le serveur DNS de l'opérateur est atteignable.

Le portail CNP DOIT essayer d'interroger le serveur DNS de l'opérateur représenté dans la base cabhCdpWanDnsServerIp en demandant des enregistrements de type SRV correspondant à l'interrogation DNS de l'équipement CPE de réseau local, comme spécifié dans [RFC 3761].

Si le portail CNP obtient des enregistrements de type SRV en réponse à son interrogation, ce portail CNP DOIT réexpédier ces enregistrements, en transparence, vers les clients d'équipement CPE de réseau local.

Il est suffisant que le portail CNP soit en mesure de propager les interrogations de serveur DNS de type SRV vers les serveurs DNS d'opérateur représentés dans la base cabhCdpWanDnsServerIp. Il est également noté que si un opérateur MSO doit fournir à ses abonnés CableHome des services qui nécessitent la résolution d'interrogations de serveur DNS de type SRV, alors cet opérateur doit offrir la capacité de résolution de ces interrogations ou aux serveurs DNS représentés dans la table d'objets MIB cabhCdpWanDnsServerIp.

10 Qualité de service

10.1 Introduction

Le présent paragraphe décrit l'environnement IPCable2Home afin de permettre, aux applications de réseau domestique qui fonctionnent sur la base des dispositifs connectés au réseau domestique, d'utiliser des éléments de qualité de service (QS) pris en charge par le protocole du réseau local. Cet environnement offre un mécanisme de gestion qui donne priorité aux flux de données assurant un trafic d'applications en temps réel, comme la voix par Internet, la diffusion audiovisuelle et les jeux vidéo, en rendant prioritaires certains accès au support et en établissant des files d'attente. La qualité de service IPCable2Home est complémentaire des mécanismes de qualité de service IPCablecom et J.112, qui permettent la gestion du trafic de qualité de service sur le réseau en hybride HFC. {texte informatif: le modèe IPCable2Home utilise la messagerie de qualité de service UPnPTM (*universal plug and play, dispositifs prêts à l'emploi*) à l'interface (ou aux interfaces) avec le réseau local.}

La présente Recommandation définit les exigences de qualité de service d'élément et de sous-élément PS qui sont nécessaires afin de permettre aux applications d'établir différents niveaux de QS dans le réseau domestique et de permettre aux opérateurs et aux utilisateurs de communiquer le traitement de priorité souhaité aux applications activées par le câblo-opérateur dans le réseau domestique {texte informatif: ainsi qu'aux applications activées par le modèle UPnP}.

10.1.1 Objectifs

Les objectifs de la qualité de service IPCable2Home sont les suivants:

{texte informatif:

- permettre aux applications de réseau domestique d'établir une transmission de données priorisée entre serveurs locaux UPnP ainsi qu'entre ces derniers et la passerelle résidentielle au moyen d'une messagerie conforme au modèle UPnP;
- permettre aux applications de réseau domestique d'établir des priorités dans les sessions de transmission de données entre serveurs locaux ainsi qu'entre ces derniers et la passerelle résidentielle IPCable2Home, au moyen d'une messagerie conforme au modèle UPnP.

}

10.1.2 Hypothèses

Les hypothèses ci-après ont été faites pour la qualité de service IPCable2Home:

{texte informatif:

- les applications qui bénéficient de la qualité de service pourront être lancées soit dans des dispositifs de serveur local IPCable2Home ou dans des dispositifs conformes à la qualité de service UPnP;
- les applications de serveur local IPCable2Home pourront comprendre des services IPCablecom.

{texte informatif:

NOTE – Tout dispositif de serveur de réseau local susceptible de recevoir des messages QS pour des services d'opérateur devra être conforme à la spécification UPnP QoS 1.0 et le système d'exploitation ainsi que la pile du réseau de ce dispositif devront posséder des capacités de QS appropriées.}

10.2 Architecture de qualité de service

L'architecture de qualité de service IPCable2Home (CQoS) se compose d'éléments fonctionnels de passerelle résidentielle IPCable2Home (le dispositif PS et ses sous-éléments). Les développeurs de passerelle résidentielle IPCable2Home (p. ex. de matériels et de logiciels) implémenteront un ou plusieurs de ces éléments selon l'ensemble des caractéristiques recherchées de ces produits. Les éléments de base de la qualité CQoS sont présentés dans le § 10.2.3.

10.2.1 Directives de conception du système

Les directives de conception du système global de qualité de service IPCable2Home sont énumérées dans le Tableau 10-1 ci-dessous.

Tableau 10-1/J.192 – Qualité de service IPCable2Home: directives de conception du système

Numéro	Directives
QS 1	Accès au support de la QS: IPCable2Home définira une fonction de gestion dans la couche 3 qui commande l'accès de transmission au moyen de priorités d'accès à des supports partagés pour l'élément logique PS. Il offrira un accès prioritaire à divers dispositifs et applications situés dans le réseau domestique.
QS 2	Réexpédition de la QS: le dispositif PS prendra en charge un mécanisme de mise en file d'attente donnant la priorité aux paquets qui sont reçus de multiples interfaces (avec un réseau local ou régional) et qui doivent être retransmis/réexpédiés par des interfaces avec un réseau local.

Tableau 10-1/J.192 – Qualité de service IPCable2Home: directives de conception du système

Numéro	Directives
QS 3	{texte informatif: gestion de la politique de QS: le modèle IPCable2Home spécifiera un mécanisme de signalisation et de gestion pour la communication de politique de qualité de service entre le dispositif PS et les points BP recherchant la QS, ainsi qu'entre un dispositif PS et des dispositifs conformes à la QS UPnP, dans un réseau domestique. Ce mécanisme sera intégré et géré dans le dispositif PS.}
QS 4	Décrire les capacités appropriées à un dispositif PS afin de faciliter l'intégration dans les procédures multimédias IPCablecom en vue de réaliser ultérieurement une qualité de service de bout en bout.

{texte informatif:}

10.2.2 Relation avec la qualité de service UPnP

L'architecture CQoS utilise une messagerie conforme à la qualité de service UPnP entre les éléments à capacité de QS. Dans l'architecture UPnP, des messages de commande sont lancés à partir d'éléments de point de commande UPnP et reçoivent une réponse envoyée par des éléments de service UPnP. Ainsi, les éléments ou sous-éléments des entités du dispositif PS sont décrits en termes d'architecture de qualité de service d'un dispositif UPnP (UQA) composé d'un point de de commande de qualité de service UPnP et d'éléments de service de qualité de service UPnP.

L'architecture UPnP est également caractérisée par une structure répartie selon laquelle il peut y avoir de multiples instanciations d'un service particulier dans le réseau domestique, pouvant être utilisées de façon interchangeable. Alors que l'architecture CQS décrit certains services de QS UPnP qui sont contenus dans le dispositif PS, il peut y avoir d'autres dispositifs situés dans le réseau domestique qui implémentent également les mêmes services de QS UPnP. Quand des descriptions ou prescriptions de dispositif PS sont rédigées au moyen de la terminologie relative aux éléments de qualité de service UPnP, l'interaction peut intervenir avec des dispositifs autres que le dispositif PS. Par exemple, dans une description d'un point de commande interagissant avec un service de gestionnaire de QS, un point de commande peut entrer en interaction avec la fontionnalité de gestionnaire de QS d'un dispositif tiers au lieu d'interagir avec le service de gestionnaire de QS dans le dispositif PS.}

10.2.3 Qualité de service IPCable2Home: description du système

L'architecture de qualité CQoS se compose des entités suivantes:

- élément de services de portail (PS);
- sous-élément du portail de qualité de service IPCable2Home (CQP);
- {texte informatif: serveurs locaux UPnP avec capacités de QoS}.

L'équipement du réseau de transmission de données par câble (tête de réseau) gère les fonctions de qualité de service IPCable2Home.

10.2.3.1 Sous-élément de portail CQP

L'élément de services de portail comprend un sous-élément de portail de qualité de service IPCable2Home (CQP). Le portail CQP agit comme un portail de qualité CQoS pour les serveurs locaux UPnP à capacité de QS. Sa fonction primaire est d'offrir une qualité de service fondée sur des priorités aux dispositifs situés dans le réseau domestique. Il effectue la mise en file d'attente/réexpédition et l'accès au support sur la base de priorités pour le trafic provenant du dispositif PS ainsi que pour le trafic traversant le service de portail. Il est également chargé de la communication de politique de qualité de service {texte informatif: à un ou plusieurs gestionnaires

de qualité de service UPnP [UQM, UPnP QoS Manager] à l'intérieur de la résidence lorsqu'il fonctionne en tant qu'unique détenteur de la politique de qualité de service UPnP [UQPH, UPnP QoS Policy Holder].}

10.2.3.2 Fonctionnalité de qualité de service dans le portail CQP

Les sous-éléments de portail CQP se composent des fonctionnalités ci-après:

- **courtier de qualité de service IPCable2Home (CQB, IPCable2Home QoS Broker)**: cette fonctionnalité est chargée d'installer la qualité de service dans le réseau domestique ainsi que dans le réseau d'accès. Cette entité configure également la qualité de service dans le dispositif PS IPCable2Home. Le courtier CQB se compose des fonctionnalités suivantes:
  - **réexpédition et accès au support de la qualité de service (QFM)**: cette fonctionnalité spécifie la mise en file d'attente et la réexpédition de paquets en fonction de priorités ainsi que l'accès au support partagé en fonction de priorités dans le dispositif PS;
  - **interface avec le multimédia IPCable2Home-IPCablecom (CH-PCMM, *CableHome-PacketCable MultiMedia*)**: Il s'agit d'une interface permettant de demander la qualité de service du réseau d'accès conformément à l'architecture multimédia IPCablecom [Rec. UIT-T J.179], à partir des services de portail IPCable2Home. L'interface CH-PCMM peut également recevoir des requêtes visant à établir la qualité de service d'un réseau domestique à partir d'entités PCMM contenues dans le réseau régional. Lors d'une telle requête, l'entité de courtier de qualité de service CableHome (CQB) peut utiliser un point de commande de qualité de service CableHome afin de régler la qualité de service d'un réseau domestique. Les exigences spécifiques concernant cette interface feront l'objet d'un complément d'étude;
  - {texte informatif: **interface avec le service de dispositif de QS UPnP (QD, *UPnP QoS device*)**: le courtier CQB peut comprendre une interface avec le service de dispositif de QoS UPnP (UQD) aux fins suivantes:
    1) Au moyen de cette interface, le dispositif PS reçoit les requêtes de classificateur de trafic issues des entités du gestionnaire de qualité de service UPnP (UQM, *UPnP QoS Manager*) contenues dans le réseau local et place ces requêtes dans la base de données du dispositif PS. Ces classificateurs sont utilisés par la fonctionnalité de gestionnaire QFM pour la classification des paquets;
    2) Au moyen de cette interface de service, le dispositif PS peut déclencher une demande relative à la qualité de service du réseau d'accès pour les flux de trafic qui relient réseau d'accès et réseau domestique au moyen de l'interface CH-PCMM, qui reste à définir.}

{texte informatif:

- **serveur de politique de qualité de service (QPS, *QoS policy server*)**: cette fonctionnalité est chargée de conserver un répertoire de politique de qualité de service pour divers dispositifs et applications contenues dans le réseau domestique et également de communiquer cette politique de qualité de service sur demande d'une entité gestionnaire UQM dans le réseau local. Le serveur QPS utilise l'interface avec le service de détenteur de politique de QS UPnP (UQPH) afin de communiquer les politiques de QS dans le réseau local. Le serveur QPS possède une interface avec une base de données du côté réseau régional afin que les opérateurs puissent gérer et consulter les politiques de qualité de service;
- **service de gestionnaire de la qualité de service (QM)**: le portail CQP est tenu d'implémenter le service de gestionnaire de qualité de service UPnP (UQM). Cette exigence garantit qu'il y a au moins un service de gestionnaire de qualité de service UPnP pour que les points de commande UPnP puissent demander la qualité de service dans le réseau local domestique;

- **fonctionnalité de point de commande de qualité de service du dispositif PS (QCP, *QoS control point*)**: cette entité joue le rôle de point de commande pour différents services de QS UPnP dans le réseau local domestique. Elle est chargée de recueillir les annonces et événements de qualité de service UPnP ainsi que d'envoyer des ordres d'action selon les besoins pour divers services de QS UPnP contenus dans le réseau local.
  1) La logique de découverte de qualité de service de ce point de commande est chargée de collecter des informations associées à la QS, issues de divers services UPnP de QS dans le réseau local domestique et de les mémoriser dans la base de données du dispositif PS. Les câblo-opérateurs accèdent à ces informations de base de données PS dans le réseau régional au moyen de l'interface avec la base MIB du protocole SNMP;
  2) La logique de courtier de QS IPCable2Home de ce point de commande est chargée d'établir la qualité de service dans le réseau local domestique en utilisant la messagerie de qualité de service UPnP sous la direction du courtier de QS IPCable2Home. Cette logique est également chargée de demander la qualité de service du réseau d'accès au moyen de l'interface CH-PCMM.

}

{texte informatif:

10.2.3.3 Fonctionnalité de qualité de service dans les serveurs locaux UPnP

La fonctionnalité de qualité de service dans le serveur local UPnP se compose d'un ou de plusieurs des services suivants de qualité de service UPnP:

- service de gestionnaire de qualité de service UPnP (UQM);
- service de dispositif de qualité de service UPnP (UQD);
- service de gestionnaire de qualité de service UPnP (UQPH).

Le serveur local UPnP peut également implémenter un point de commande UPnP qui demande la qualité de service dans le réseau local domestique.

}

10.2.3.4 Classes de dispositifs physiques, éléments fonctionnels de qualité CQoS et interfaces de messagerie

Un exemple de la relation entre les dispositifs IPCable2Home et les éléments fonctionnels de qualité CQoS est présenté dans la Figure 10-1. La Figure 10-2 représente les interfaces de messagerie entre divers éléments fonctionnels de l'architecture CQoS et n'implique aucune implémentation spécifique. {texte informatif: les flèches en pointillés indiquent une éventuelle communication interne quand des entités de qualité de service UPnP interagissent dans le dispositif PS.}

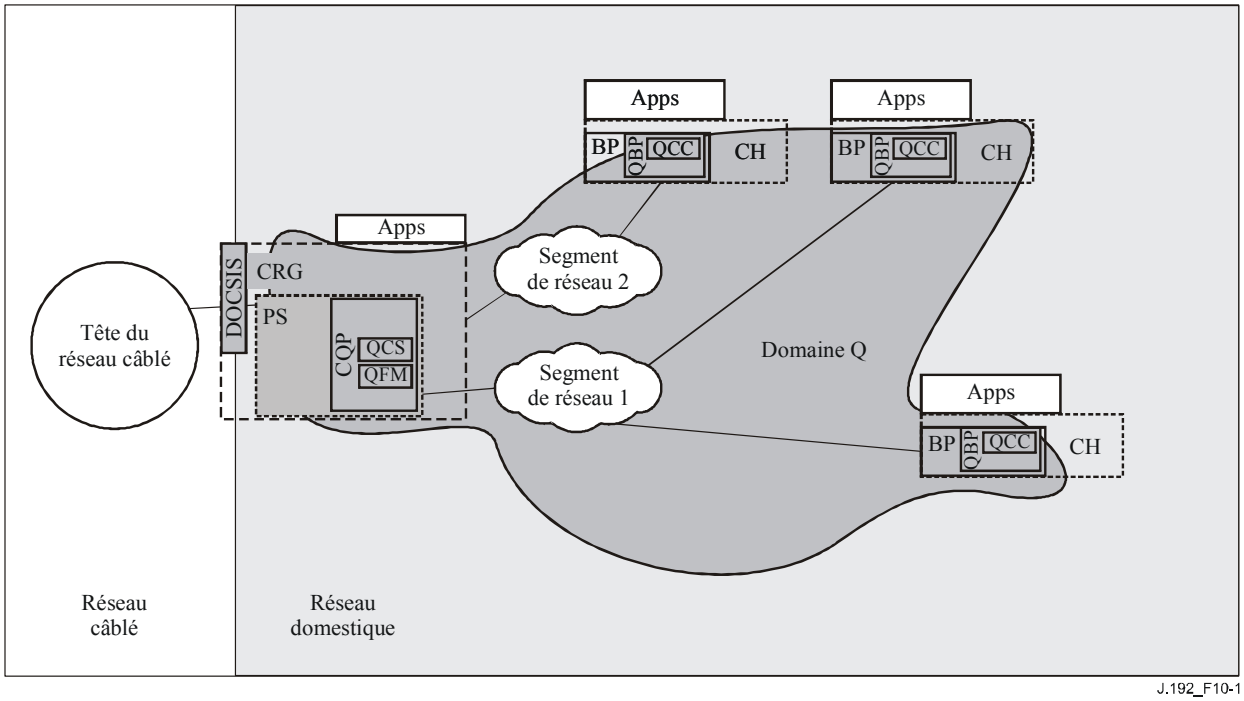


Figure 10-1/J.192 – Exemple d'éléments fonctionnels de qualité CQoS

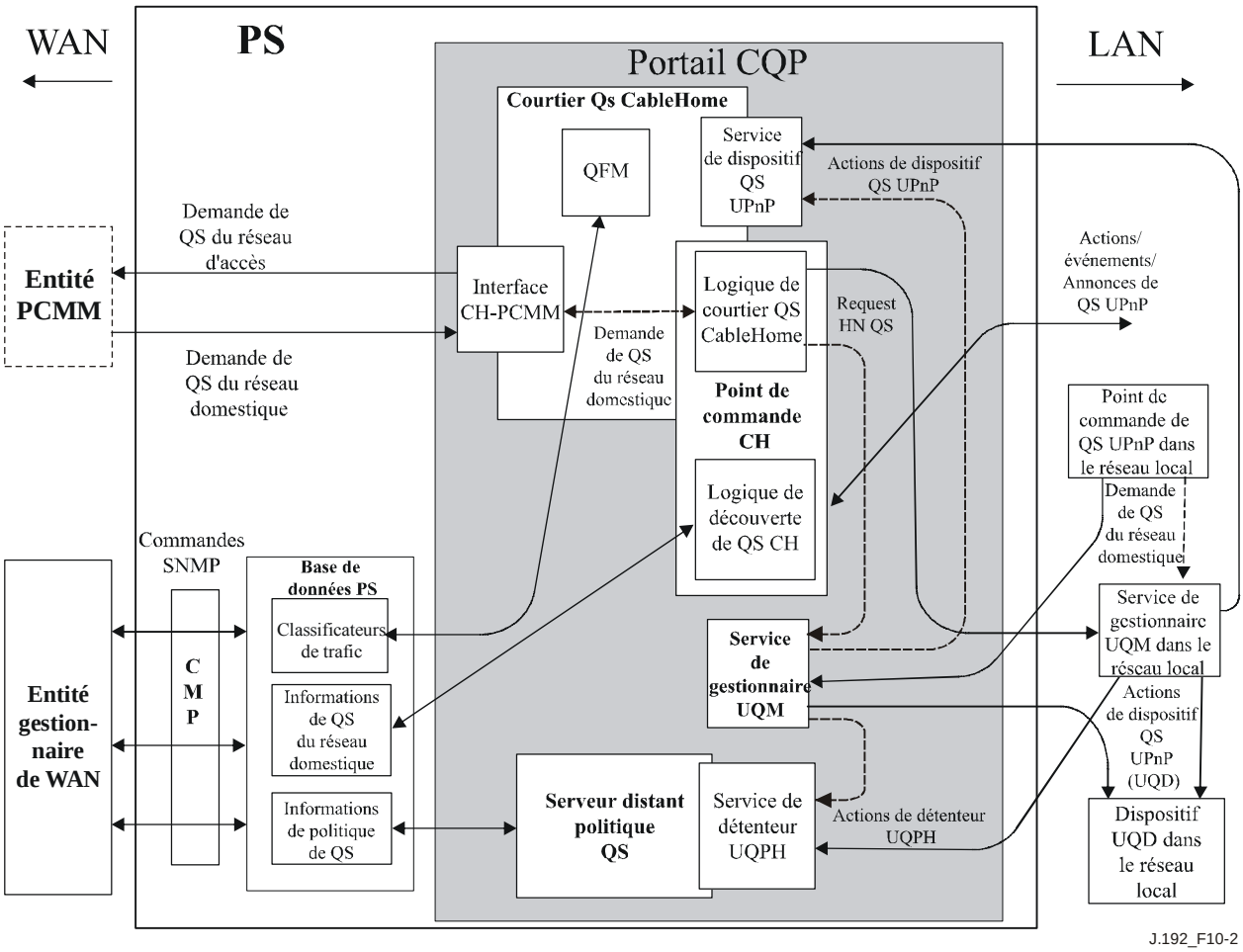


Figure 10-2/J.192 – Interfaces de messagerie dans l'architecture de qualité de service CableHome

10.2.3.5 Priorités IPCable2Home et leurs mappages

10.2.3.5.1 Priorités IPCable2Home

La présente Recommandation définit trois priorités de qualité de service différentes, qui sont les suivantes:

- {texte informatif:
  numéro d'importance du trafic UPnP};
- priorités IPCable2Home de mise en file d'attente;
- priorités IPCable2Home d'accès au support.

{texte informatif:

10.2.3.5.1.1 Numéro d'importance du trafic (TIN, *traffic importance number*) UPnP

Le numéro d'importance du trafic UPnP (TIN) n'est pas linéaire mais suit le même système de numérotation que les valeurs de priorité de paquet indiquées à l'Annexe G de l'ISO/CEI 10038. Ce système de numérotation est décrit dans le Tableau 10-2 ci-dessous. Les câblo-opérateurs assignent une valeur de numéro d'importance du trafic UPnP à un flux de trafic indiqué dans la table d'objets de politique de qualité de service (cabhQos2PolicyTable) (conformément au § E.7) qui est mémorisée dans la base de données du dispositif PS.

Tableau 10-2/J.192 – Système de numérotation pour le numéro d'importance du trafic UPnP

Numéro d'importance du trafic UPnP
7 (numéro le plus élevé)
6
5
4
3
0 (trafic au mieux /existant)
2
1 (numéro le moins élevé)

NOTE – Les valeurs 1 et 2 du numéro d'importance du trafic UPnP indiquent des valeurs de priorité inférieures à 0 (la valeur 0 est typiquement assignée au trafic existant au mieux).

}

10.2.3.5.1.2 Priorités IPCable2Home de mise en file d'attente

Dans le dispositif PS, des paquets peuvent arriver à partir de multiples interfaces et être destinés à une seule interface. Chaque interface est autorisée à implémenter une fonction de mise en file d'attente. Afin d'offrir une qualité de service priorisée pour le trafic domestique traversant le dispositif PS, la présente Recommandation spécifie une fonctionnalité de mise en file d'attente priorisée à chaque interface contenue dans le dispositif PS. A cette fin, une file d'attente individuelle dans une interface est désignée avec une certaine priorité de mise en file d'attente. Cette priorité est définie comme étant une priorité IPCable2Home de mise en file d'attente qui peut être identifiée pour chaque paquet à transmettre sur chaque interface avec le dispositif PS, de façon que ce paquet puisse être placé dans une file appropriée. Cette priorité de mise en file d'attente est déduite {texte informatif: du numéro d'importance du trafic UPnP qui est assigné à un flux de trafic au moyen du nombre de files d'attente prises en charge par une interface dans le dispositif PS. Ce mappage est effectué comme spécifié dans l'Annexe G de l'ISO/CEI 10038}.

10.2.3.6.1.3 Priorités IPCable2Home d'accès au support

La présente Recommandation définit un système d'accès priorisé de la qualité de service au support, dans lequel le trafic sur un support partagé peut être priorisé en fonction de la priorité attribuée aux paquets. Ainsi, une technique de partage de support peut assurer une qualité de service priorisée de façon qu'un paquet ayant une priorité plus élevée reçoive un accès préférentiel aux supports partagés, par rapport à un paquet ayant une priorité inférieure. Diverses techniques de supports partagés prennent en charge divers nombres de priorités d'accès au support (p. ex., le multimédia par réseau local sans fil (WMM, *Wi-Fi MultiMedia*) prend en charge quatre priorités d'accès au support). La technique de l'association HomePNA prend en charge huit priorités et la technique HomePlug prend en charge quatre priorités d'accès au support). {texte informatif: la priorité IPCable2Home d'accès au support d'un paquet est déduite de son numéro d'importance de trafic UPnP, fondé sur le nombre de priorités d'accès au support prises en charge par la technique de partage de support dans la couche 2 utilisée par l'interface. Ce mappage est exécuté comme spécifié dans l'Annexe G de l'ISO/CEI 15802-3.} Les valeurs des priorités IPCable2Home d'accès au support sont des niveaux logiques relatifs qui représentent un niveau de préférence qu'un paquet obtient pour l'accès au support.

10.3 Sous-élément logique de portail CQP de dispositif PS

Le portail CQP contient les fonctionnalités de courtier CQB, de gestionnaire QM, de point QCP et de serveur QPS comme représenté dans la Figure 10-1. La fonctionnalité de courtier CQB est décrite dans le § 10.3.1. La fonctionnalité de serveur QPS est décrite dans le § 10.3.2. La fonctionnalité de gestionnaire QM est décrite dans le § 10.3.3. La fonctionnalité de point QCP est décrite dans le § 10.3.4.

10.3.1 Courtier de qualité de service IPCable2Home (CQB)

Le courtier CQB se compose de la fonctionnalité de réexpédition et accès au support de la qualité de service (QFM) et, facultativement, d'une interface avec le service de dispositif de QS.

10.3.1.1 Réexpédition et accès au support de la qualité de service (QFM)

La fonctionnalité de réexpédition et accès au support de la qualité de service (QFM) dans le dispositif PS est chargée de la réexpédition et de l'accès au support priorisés pour les paquets traversant le dispositif PS vers le réseau local domestique. Le présent paragraphe offre une description de la fonctionnalité de réexpédition QFM dans le dispositif PS et spécifie les exigences PS associées.

10.3.1.1.1 Réexpédition et accès au support de la qualité de service: objectifs

Les objectifs de la fonctionnalité de réexpédition et accès au support de la qualité de service sont les suivants:

- ordonner les paquets arrivant de multiples interfaces avec le dispositif PS et les réexpédier vers une interface avec le réseau local de destination en fonction de leurs priorités et des capacités de mise en file d'attente dans les interfaces avec un réseau local;
- offrir un accès priorisé aux supports partagés pendant la transmission des paquets dans les interfaces avec un réseau local, en fonction de la priorité des paquets et des capacités d'accès priorisé au support des interfaces avec un réseau local.

10.3.1.1.2 Réexpédition et accès au support de la qualité de service: directives de conception

Voir le Tableau 10-3.

Tableau 10-3/J.192 – QFM: directives de conception du système

Numéro	Directives
QFM.1	La fonction QFM peut fonctionner sur les paquets à destination et en provenance des secteurs d'adresses LAN-Trans et LAN-Pass.
QFM.2	La fonction QFM peut déterminer la priorité des paquets au moyen des informations de classification des paquets disponibles dans la base de données du dispositif PS.
QFM.3	La fonction QFM peut ordonner les paquets entrants de façon qu'ils ressortent par les interfaces avec un réseau local conformément à leurs priorités.
QFM.4	La fonction QFM devrait être capable d'opérer avec différents nombres de files d'attente par interface.
QFM.5	{texte informatif: la fonction QFM applique le numéro d'importance du trafic UPnP du paquet sur la priorité de file d'attente IPCable2Home conformément au mappage défini.}
QFM.6	La fonction QFM peut offrir un accès priorisé aux supports partagés à chaque interface avec le réseau local, selon la priorité des paquets et selon les capacités d'accès priorisé au support des interfaces avec le réseau local.
QFM.7	{texte informatif: la fonction QFM applique le numéro d'importance du trafic UPnP du paquet sur la priorité IPCable2Home d'accès au support conformément au mappage défini.}
QFM.8	La fonction QFM devrait être en mesure de fonctionner avec des interfaces qui prennent en charge différents nombres de priorités d'accès au support.

10.3.1.1.3 Réexpédition et accès au support de la qualité de service: hypothèses de conception

- chaque interface PS LAN PEUT prendre en charge moins de huit files d'attente;
- le nombre maximal de files d'attente prises en charge par une interface PS LAN est de huit;
- chaque technique de mise en réseau à une interface PS LAN PEUT prendre en charge moins de huit priorités d'accès au support;
- le nombre maximal de priorités d'accès au support prises en charge par une technique de mise en réseau à une interface PS LAN est de huit.

10.3.1.1.4 Réexpédition et accès au support de la qualité de service: description du système

La fonction QFM offre au dispositif PS un mécanisme permettant d'ordonner et de transmettre des paquets du côté sortant d'une interface avec un réseau local, conformément aux priorités attribuées. C'est par l'attribution de priorités à des paquets et par l'action de la fonction QFM que les paquets traversant le dispositif PS vers le réseau local domestique reçoivent un accès priorisé aux supports partagés par le réseau local. La fonction QFM est chargée des trois opérations suivantes.

1) {texte informatif: processus de classification afin d'identifier le numéro d'importance du trafic (TIN) UPnP du paquet};
2) mise en file d'attente priorisée;
3) accès priorisé au support.

{texte informatif:

10.3.1.1.4.1 Classification du paquet afin d'identifier le numéro d'importance du trafic UPnP

Les paquets traversant le dispositif PS à destination d'une interface avec un réseau local peuvent être issus soit du réseau régional (trafic descendant de WAN à LAN) ou d'une autre interface avec le réseau local dans le dispositif PS (trafic résidentiel LAN-LAN). Pour le trafic résidentiel LAN-LAN, la fonction QFM peut facultativement exécuter la classification des paquets. Cependant,

pour le trafic descendant de WAN à LAN, la fonction QFM est tenue d'exécuter la classification des paquets afin de déterminer le numéro approprié d'importance de trafic UPnP (TIN) si le côté sortant de l'interface avec le réseau local prend en charge de multiples files d'attente ou de multiples priorités.

Afin d'exécuter la classification des paquets, le dispositif PS examine ces derniersafin de repérer leur numéro d'importance du trafic UPnP. Le dispositif PS examine l'adresse IP d'origine, le port d'origine, l'adresse IP de destination, le port de destination et le type de protocole du paquet. Puis il essaie de trouver une première concordance dans les tables de classificateurs mémorisées dans la base de données du dispositif PS qui est représentée par la base MIB cabhQos2TraficClassTable (voir l'Annexe A). Si le dispositif PS trouve une entrée concordante, alors il utilise la valeur représentée par la base cabhQos2TraficClassImpNumMIB pour cette entrée en tant que numéro d'importance du trafic UPnP pour ce paquet. Si aucune entrée concordante n'est trouvée, alors le dispositif PS utilise une valeur de 0 du numéro d'importance du trafic UPnP pour ce paquet. Le dispositif PS utilise cette valeur du numéro d'importance du trafic UPnP afin de déterminer la priorité de mise en file d'attente IPCable2Home ainsi que la priorité d'accès au support IPCable2Home de ce paquet.

10.3.1.1.4.2 Mise en file d'attente priorisée

Le nombre de files d'attente prises en charge par une interface avec le dispositif PS, à laquelle le paquet est destiné, peut être différent des huit niveaux du numéro d'importance du trafic UPnP. Le dispositif PS applique donc la valeur de numéro d'importance du trafic UPnP du paquet sur une valeur de priorité IPCable2Home de mise en file d'attente comme défini dans [802.1D] Annexe G. Puis le dispositif PS place le paquet dans une file d'attente appropriée de l'interface de destination qui correspond à cette valeur mappée de priorité de mise en file d'attente IPCable2Home.

Pour chaque interface sortante, la fonction QFM explore toutes les files d'attente de cette interface conformément à leur priorité afin d'extraire des paquets à transmettre sur les supports partagés. Chaque fois que la fonction QFM doit extraire un paquet à partir des files d'attente pour une interface particulière avec le dispositif PS, elle commence toujours son exploration par la file d'attente ayant la priorité la plus élevée. Si cette file n'a aucun paquet à envoyer, la fonction QFM explore la prochaine file d'attente ayant la priorité la plus élevée parmi les files d'attente restant dans la hiérarchie jusqu'à ce qu'elle trouve un paquet à envoyer dans une de ces files d'attente. Les paquets sont extraits de chaque file d'attente dans l'ordre de leur arrivée. Ainsi, le procédé de mise en file d'attente utilisé par la fonction QFM peut être décrit comme étant de type premier entré/premier sorti avec priorités et de type file d'attente prioritaire en premier.

10.3.1.1.4.3 Accès priorisé au support

Une fois que la fonction QFM a extrait un paquet de l'ensemble des files d'attente d'une interface, le paquet doit être transmis sur les supports partagés du réseau local avec une priorité appropriée. Donc, la fonction QFM applique la valeur de numéro d'importance du trafic UPnP du paquet à la valeur de priorité IPCable2Home d'accès au support comme défini dans [802.1D] Annexe G. Cette valeur détermine le niveau de préférence que le paquet devrait utiliser afin d'accéder aux supports partagés. Donc, les vendeurs ont besoin de garantir que les préférences d'accès relatif au support, requises par les valeurs de priorité IPCable2Home d'accès au support, sont conservées lors de la transmission des paquets sur les supports partagés du réseau local.

10.3.1.1.4.4 Prise en charge des applications IPCablecom

Etant donné que l'objectif de la qualité de service (QS) est de n'être fournie que dans le réseau domestique, la présente Recommandation ne prête pas une attention particulière à la qualité de service du réseau d'accès. Cependant, la présente Recommandation conserve la prise en charge des applications de mise en réseau domestique afin d'établir des sessions de transmission de données priorisées entre le système CMTS et le dispositif de passerelle résidentielle IPCable2Home, au

moyen de la messagerie conforme au modèle IPCablecom, comme spécifié par la Rec. UIT-T J.191. Les exigences nécessaires pour prendre en charge cette fonctionnalité dans le dispositif PS, telles qu'elles figurent dans la Rec. UIT-T J.191, sont donc incluses dans les spécifications de qualité de service.

Le dispositif PS joue le rôle de pont transparent et réexpédie la messagerie de qualité de service IPCablecom entre le système CMTS et les applications IPCablecom. Les données applicatives sont associées à un flux de service DOCSIS conformément à un classificateur qui est créé dans l'interface avec le câblo-modem, sur la base des informations incluses dans les messages IPCablecom (tels que le message PATH du protocole RSVP).

Etant donné que le dispositif PS est tenu de réexpédier la messagerie de qualité de service IPCablecom, il ne dépend pas du système NMS pour remplir cette fonction. Cette fonction de portail CQP reste donc la même pour les deux modes de préconfiguration: DHCP et SNMP (voir § 5.5).

La messagerie de qualité de service IPCable2Home sur l'hybride HFC ou dans le réseau d'accès est définie par les Recommandations UIT-T J.161 et J.163. En tant que telles les fonctions IPCable2Home de gestion de la politique de qualité de service et de contrôle d'admission concernant la qualité de service du réseau d'accès sont également définies par les Recommandations UIT-T J.161 et J.163.

10.3.1.1.5 Réexpédition et accès au support de la qualité de service: exigences

10.3.1.1.5.1 Classification de paquet: exigences

Le dispositif PS PEUT exécuter la classification des paquets pour trafic de réseau local à réseau local.

Pour le trafic de réseau régional à réseau régional, si une interface sortante avec le réseau local implémente de multiples files d'attente ou de multiples priorités, alors le dispositif PS DOIT exécuter la classification des paquets.

Afin d'exécuter la classification des paquets, le dispositif PS DOIT effectuer les actions suivantes:

1) le dispositif PS DOIT examiner les valeurs d'adresse IP d'origine, dadresse IP de destination, de port d'origine, de port de destination et de type de protocole du paquet et DOIT trouver une première entrée concordante (c'est-à-dire le numéro d'indice le moins élevé) dans la table de classificateurs du dispositif PS (cabhQos2TrafficClassTable) mémorisée dans la base de données du dispositif PS (voir l'Annexe);
2) {texte informatif: le dispositif PS DOIT utiliser la valeur de base MIB d'objets cabhQos2TrafficClassImpNum de l'entrée concordante comme numéro d'importance du trafic UPnP pour ce paquet;
3) si aucune entrée concordante n'est trouvée dans la table de classificateurs, alors le dispositif PS DOIT assigner au paquet le numéro 0 d'importance du trafic UPnP.

10.3.1.1.5.2 Mise en file d'attente priorisée: exigences

}

{texte informatif:

le dispositif PS DOIT mémoriser le nombre de files d'attente implémenté par chacune de ses interfaces dans la base de données PS, ce nombre pouvant être obtenu par une valeur d'objet cabhQos2PsIfAttribIfNumQueues de base MIB [voir § E.7].

Le dispositif PS DOIT mapper la valeur de numéro d'importance du trafic UPnP du paquet identifié pendant le processus de classification, à la valeur de priorité IPCable2Home de mise en file d'attente spécifiée dans [802.1D] Annexe G au moyen du nombre de files d'attente (objet

cabhQos2PsIfAttribIfNumQueues) (Annexe E.7) implémenté par une interface au travers de laquelle le paquet doit être transmis. Le dispositif PS DOIT mettre correctement en file d'attente le paquet à l'interface de destination conformément à cette valeur mappée de priorité IPCable2Home de mise en file d'attente.

Pour chaque interface avec un réseau local, le dispositif PS DOIT explorer diverses files d'attente à cette interface conformément à leur priorité afin d'extraire les paquets à transmettre sur les supports partagés. Chaque fois que le dispositif PS doit extraire un paquet des diverses files d'attente pour une interface particulière, il DOIT toujours commencer son exploration par la file d'attente ayant la priorité la plus élevée. Si cette file n'a aucun paquet à envoyer, le dispositif PS DOIT explorer la prochaine file d'attente ayant la priorité la plus élevée parmi les files d'attente restant dans la hiérarchie, jusqu'à ce qu'il trouve le prochain paquet disponible à envoyer avec la priorité la plus élevée. Le dispositif PS DOIT toujours extraire les paquets de chaque file d'attente dans l'ordre de leur arrivée.

10.3.1.1.5.3 Accès prioritaire au support: exigences

Le dispositif PS DOIT mémoriser le nombre de priorités initiales d'accès au support dans la couche 2, prises en charge par chacune de ses interfaces dans la base de données PS et accessibles par un objet de base MIB cabhQos2PsIfAttribIfNumPriorities (voir § E.7).

Après que le paquet a été extrait des files d'attente d'une interface particulière, le dispositif PS DOIT appliquer le numéro d'importance du trafic UPnP du paquet à la priorité IPCable2Home d'accès au support, comme défini dans [802.1D] Annexe G, au moyen du nombre de priorités d'accès au support prises en charge (objet cabhQos2PsIfAttribIfNumPriorities) par cette interface. Le dispositif PS DOIT transmettre le paquet par la technique de partage du support de telle sorte que son accès préférentiel relatif au support, comme requis par la valeur de priorité IPCable2Home d'accès au support, soit conservé.

}

10.3.1.1.5.4 Exigences relatives à la prise en charge des applications IPCablecom

Le dispositif PS DOIT jouer le rôle d'un pont transparent et réexpédier la messagerie de QS IPCablecom [Rec. UIT-T J.161], [Rec. UIT-T J.163] entre le système CMTS et les applications IPCablecom. Les données applicatives sont associées à un flux de service de câblo-modem conformément à un classificateur qui est créé dans l'interface avec le CM, fondée sur les informations incluses dans les messages IPCablecom (comme RSVP PATH).

Etant donné que l'exigence du dispositif PS concernant le modèle IPCable2Home est juste de réexpédier la messagerie de qualité de service IPCablecom, il n'y a aucune dépendance du système NMS afin d'assurer cette fonction. Donc, cette fonction de portail CQP reste la même pour les deux modes de préconfiguration: DHCP et SNMP (voir § 5.5).

{texte informatif:

10.3.1.2 Interface UPnP avec le service de dispositif de QS (QDS, *QoS Device Service*)

10.3.1.2.1 Interface UPnP avec le service de dispositif de QS: objectifs

- Offrir une interface avec un service de gestionnaire de qualité de service UPnP afin de régler la qualité de service d'un réseau domestique dans les interfaces avec un réseau local du dispositif PS CableHome.
- Offrir une interface avec un dispositif PS CableHome afin de détecter la nécessité d'une qualité de service du réseau d'accès pour une session qui relie réseau d'accès et réseau domestique.

10.3.1.2.2 Interface UPnP avec le service de dispositif de QS: directives de conception

Voir le Tableau 10-4

Tableau 10-4/J.192 – Service de dispositif de QS UPnP – Directives de conception

Numéro	Directives
QDS.1	Le service QDS fournit une interface avec une entité gestionnaire de la qualité de service UPnP afin de régler la qualité de service dans le dispositif PS CableHome.
QDS.2	Le service QDS installe les classificateurs de paquet dans le dispositif PS CableHome.
QFM.3	Le service QDS détecte la nécessité d'une négociation de la qualité de service du réseau d'accès pour une session.

10.3.1.2.3 Interface UPnP avec le service de dispositif de QS: hypothèses

Afin de régler la qualité de service, les points de commande contenus dans le réseau local domestique peuvent utiliser l'entité gestionnaire de la qualité de service dans le réseau local domestique (entité gestionnaire UQM), qui ne fait pas partie du dispositif PS CableHome.

10.3.1.2.4 Interface UPnP avec le service de dispositif de QS: description

Le dispositif PS CableHome peut facultativement mettre en œuvre une interface UPnP avec le service de dispositif de QS (UQD) contenu du côté réseau local. Si cette interface est implémentée, le service de dispositif de QS UPnP est réputé faire partie du dispositif radical des services de portail CableHome. Le service de dispositif de QS UPnP fournit une interface de façon que l'entité gestionnaire de la qualité de service UPnP contenue dans le réseau local puisse configurer le dispositif PS CableHome avec les réglages appropriés de qualité de service. Quand une entité gestionnaire de la qualité de service UPnP invoque l'action SetUpTrafficQoS du service QDS dans le dispositif PS CableHome, celui-ci installe les classificateurs de paquet au moyen des informations contenues dans le descripteur de trafic UPnP qui est transmis sous forme d'argument d'entrée de l'action. Ces classificateurs sont utilisés par le gestionnaire QFM en vue de la classification des paquets. Si une adresse IP d'origine ou de destination contenue dans le descripteur de trafic UPnP réside dans le réseau régional, alors le dispositif PS CableHome détecte que la qualité de service du réseau d'accès est également requise pour la session en cours.

10.3.1.2.5 Interface UPnP avec le service de dispositif de QS: exigences

Le dispositif PS PEUT implémenter le service de dispositif de QS UPnP (UQD).

Si le dispositif PS implémente le service de dispositif de QS UPnP, alors il est tenu d'adhérer aux exigences suivantes.

Le dispositif PS DOIT annoncer le service de dispositif de QS UPnP comme un service intégré de dispositif radical de services de portail CableHome.

Le dispositif PS DOIT être en mesure de traiter l'action GetQoSCapabilities du service de dispositif de QS UPnP. Dès réception de cette action, le dispositif PS NE DOIT renvoyer QUE les attributs de ses interfaces avec le côté réseau local qui sont représentés par la base MIB d'interfaces ifTable dans l'argument de sortie QoSDeviceCapabilities de l'action, comme spécifié dans le Tableau 10-5 ci-après.

Tableau 10-5/J.192 – Valeurs de base MIB ifTable et variable d'état QoSDeviceCapabilities UPnP

Valeurs de base MIB ifTable	Valeurs XML de la variable d'état QoSDeviceCapabilities UPnP
IfIndex	InterfaceId
IfPhysAddress	PhysAddress
IfType	IanaTechnologyType
IfSpeed	MaxPhyRate

Le dispositif PS DOIT être en mesure de traiter l'action GetQosState du service de dispositif de QS UPnP. Dès réception de cette action, le dispositif PS DOIT renvoyer tous les classificateurs de paquet représentés par la base MIB cabhQos2TrafficClassTable dans l'argument de sortie XML ListOfTrafficDescriptors et renvoyer le nombre total de classificateurs de paquet contenu dans l'argument de sortie NumberOfTrafficDescriptors. Le dispositif PS DOIT également renvoyer l'identificateur QoSStateId comme argument de sortie.

Le dispositif PS DOIT prendre en charge l'action SetUpTrafficQoS du service de dispositif de QS UPnP. Dès réception de cette action, le dispositif PS DOIT utiliser l'argument d'entrée SetupTrafficDescriptor afin d'établir un classificateur de paquets dans la base de données du dispositif PS qui est accessible via la base MIB cabhQos2TrafficClassTable de ce dispositif PS.

Le dispositif PS DOIT prendre en charge la réception de l'action ReleaseTrafficQos du service de dispositif de QS UPnP. Dès réception de cette action, le dispositif PS DOIT supprimer une entrée de classificateur de paquets mémorisée dans sa base de données identifiés par le ReleaseTraficHandle argument d'entrée de l'action.

}

{texte informatif:

10.3.2 Serveur distant de politique de qualité de service (QPS) du dispositif PS

Le serveur distant de politique de qualité de service (QPS) joue dans le dispositif PS le rôle de répertoire des politiques de qualité de service d'un réseau domestique qui ont été établies par un câblo-opérateur ainsi que par un utilisateur domestique. Le serveur QPS possède une interface en protocole SNMP avec le côté réseau régional permettant aux câblo-opérateurs de gérer les politiques de qualité de service. Du côté réseau local, le serveur QPS possède une interface avec le service de détenteur de politique de qualité de service UPnP (UQPH) afin de communiquer Les politiques de qualité de service à la demande d'une entité gestionnaire de la qualité de service UPnP. Le serveur QPS peut également avoir une interface non spécifiée avec le réseau local qui permet aux utilisateurs domestiques de gérer les politiques de qualité de service indépendamment. Le présent paragraphe fournit la description de la fonctionnalité de serveur QPS et des exigences associées pour le dispositif PS.

10.3.2.1 Serveur distant de politique de qualité de service: objectifs

- Etablir un ensemble de critères permettant aux applications et aux services de demander et d'utiliser des politiques de qualité de service pour le trafic dans le réseau domestique.
- Permettre la configuration de politique de qualité de service aussi bien par le câblo-opérateur que par l'utilisateur dans le dispositif PS IPCable2Home.
- Assurer un mécanisme permettant au réseau de transmission de données par câble de communiquer les politiques de qualité de service recherchées aux services de portail puis à des dispositifs de qualité de service UPnP conformes, par l'intermédiaire de toute entité gestionnaire de qualité de service à l'intérieur du réseau domestique.

10.3.2.2 Serveur distant de politique de qualité de service: directives de conception

Voir le Tableau 10-6.

Tableau 10-6/J.192 – Directives de conception du serveur QPS

Numéro	Directives
QPS.1	Le serveur QPS recevra des informations sur la politiques de qualité de service pour chaque application à partir du serveur distant de gestion de réseau (NMS) situé dans la tête de réseau, ainsi qu'à partir d'un utilisateur domestique du côté réseau local.
QPS.2	Les informations de politique de qualité de service fournies au serveur QPS pourront être mises à jour par la tête de réseau ainsi que par l'utilisateur domestique. Les informations mises à jour ne sont obtenues que lorsque l'entité gestionnaire de qualité de service en formule la requête.
QPS.3	Les informations de politique de qualité de service fournies au serveur QPS par la tête de réseau peuvent contenir des règles de politique qui ne peuvent pas être mises à jour par l'utilisateur domestique. Le serveur QPS utilisera la messagerie UPnP
QPS.4	Le serveur QPS utilisera une interface définie avec le contenu des messages (base MIB) afin de fournir des informations sur diverses applications de réseau local domestique au serveur distant de gestion de réseau (NMS) situé dans la tête de réseau.

10.3.2.3 Serveur distant de politique de qualité de service: hypothèses

Le modèle IPCable2Home utilise la messagerie UPnP afin d'échanger des informations de politique de qualité de service entre le dispositif PS et des entités de qualité de service conformes au modèle UPnP. Les serveurs locaux UPnP peuvent avoir défini plusieurs services ou applications.

10.3.2.4 Serveur distant de politique de qualité de service: description du système

Le serveur QPS conserve une base de données des politiques de qualité de service concernant le trafic dans le dispositif PS. Le serveur QPS peut recevoir des informations sur la règle politique de qualité de service à partir de la tête de réseau, par le téléchargement initial du fichier de configuration du dispositif PS ou par une interface avec une base MIB dans le portail CMP. Le serveur QPS peut également recevoir des informations sur la règle politique de qualité de service à partir de l'utilisateur domestique au moyen d'une interface avec le réseau local (comme un serveur distant de protocole HTTP) non spécifiée dans le modèle CableHome 1.1 mais qui doit aussi être représentée dans la base de données de politique de trafic du serveur QPS. Celui-ci communiquera les informations de politique à tout gestionnaire de qualité de service UPnP (UQM) qui en fera la demande en vue d'un accès prioritaire au support par des applications ou services du réseau local.

10.3.2.4.1 Echange d'informations du côté réseau régional

Du côté réseau régional, la tête de réseau du câblo-opérateur fournit au dispositif PS les politiques de qualité de service du trafic, au moyen d'un fichier de configuration ou d'une interface avec une base MIB de protocole SNMP. Le système NMS, en tête de réseau, peut lire et mettre à jour (ajouter/modifier/supprimer) ces politiques de qualité de service du trafic dans la base de données PS au moyen d'une interface avec une base MIB SNMP.

10.3.2.4.1.1 Informations de politique de qualité de service IPCable2Home allant du réseau régional au dispositif PS

La tête de réseau offre au dispositif PS une liste des politiques ordonnées de qualité de service du trafic qu'un câblo-opérateur souhaite voir utilisées par les applications et par les services. Ces informations sont fournies aux services de portail par un fichier de configuration au moment de l'initialisation du dispositif PS, ou au moyen de commandes SET du protocole SNMP à partir de la

tête de réseau. Le dispositif PS mémorise ces informations dans la base de données PS qui est accessible par la table de base MIB cabhQos2PolicyTable.

Le dispositif PS peut également recevoir des demandes issues du système NMS afin de mettre à jour (ajouter/modifier/supprimer) ces politiques de qualité de service du trafic pour les applications et services contenus dans sa table de politique, au moyen du protocole SNMP. En réponse à ces requêtes, le dispositif PS met à jour (ajouter/modifier/supprimer) les informations de politique contenues dans la base de données du dispositif PS à laquelle on peut accéder par l'intermédiaire de la base MIB cabhQos2PolicyTable au moyen de l'interface SNMP. Voir Figure 10.3.

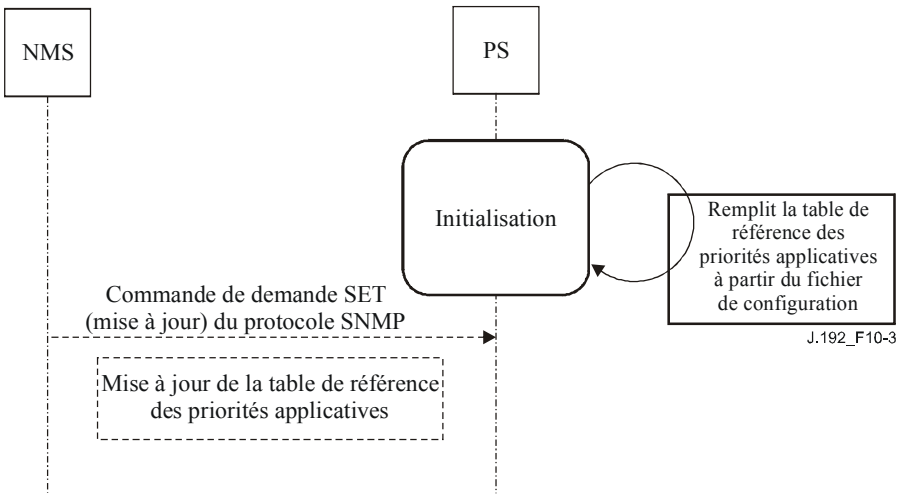


Figure 10-3/J.192 – Echange et traitement d'informations de réseau régional dans le dispositif PS

10.3.2.4.2 Interface avec le service de détenteur de politique de qualité de service (QPH) UPnP pour le réseau local

Du côté réseau local, le service de détenteur de politique de qualité de service UPnP s'interface directement avec tout gestionnaire de qualité de service UPnP pour l'extraction d'une politique de trafic conformément à un descripteur de trafic spécifique. En réponse à une demande du gestionnaire de qualité de service UPnP concernant une politique de trafic, le service de détenteur QPH renverra les valeurs de numéro d'importance du trafic, de numéro d'importance de l'utilisateur et de politique d'admission activée pour le descripteur de trafic correspondant. Si une concordance n'est pas trouvée, le serveur QPS renvoie 0 pour le numéro d'importance du trafic et 0 pour le numéro d'importance de l'utilisateur.

10.3.2.5 Exigences relatives au serveur distant de politique de qualité de service

10.3.2.5.1 Exigences relatives à l'échange d'informations du côté réseau régional

Le dispositif PS DOIT mémoriser une liste de politiques de trafic offerte par un câblo-opérateur, dans la base de données PS qui est accessible au moyen de l'interface avec la base MIB SNMP d'objets cabhQos2PolicyTable. Le dispositif PS DOIT prendre en charge la mise à jour (ajouter/modifier/supprimer) de cette table cabhQos2PolicyTable au moyen d'un fichier de configuration au moment de l'initialisation du dispositif PS, ou au moyen de commandes SET (mise à jour) du protocole SNMP à partir de la tête de réseau.

10.3.2.5.2 Exigences relatives au service UPnP de détenteur QPH

Le dispositif PS DOIT prendre en charge au moins (32) entrées de rangée de type 'operatorOnly' dans la table 'cabhQos2PolicyTable'.

Le dispositif PS DOIT prendre en charge au moins (32) entrées de rangée de type 'homeUser' dans la table 'cabhQos2PolicyTable'.

Le dispositif PS DOIT prendre en charge au moins (32) entrées de rangée de type 'operatorForHomeUser' dans la table 'cabhQos2PolicyTable'.

Le dispositif PS doit prendre en charge l'action 'GetTrafficPolicy' du service de détenteur de politique de qualité de service UPnP (UQPH).

En réponse à une action GetTrafficPolicy du service de détenteur QPH UPnP, le dispositif PS DOIT exécuter les fonctions ci-après.

1) Le dispositif PS DOIT trouver la première concordance avec une règle de politique de qualité de service dans la table 'cabhQos2PolicyTable'. Le dispositif PS DOIT traiter les règles en fonction de l'indice pointant dans la table SNMP et en fonction de la base MIB cabhQos2PolicyRuleOrder. C'est-à-dire que le dispositif PS DOIT traiter d'abord toutes les entrées de type 'operatorOnly' de la table d'objets cabhQos2PolicyTable, puis les entrées de type 'homeUser' et enfin les entrées de type 'operatorForHomeUser'. En outre, dans ces entrées individuelles de "propriétaire", le dispositif PS traite les entrées ayant la valeur numérique la moins élevée dans la base 'cabhQos2PolicyRuleOrder'.
2) Après que le dispositif PS a trouvé une première entrée concordante dans une rangée de la table cabhQos2PolicyTable, il DOIT renvoyer la valeur de la base MIB cabhQos2PolicyTraffImpNum (voir § E.7) comme argument de sortie "trafficImportanceNumber" de l'action GetTrafficPolicy.
3) Le dispositif PS DOIT également renvoyer la valeur de la base MIB cabhQos2PolicyAdmissionPolicyEnable comme argument de sortie "admissionPolicyEnable" de l'action GetTrafficPolicy.
4) Le dispositif PS DOIT également renvoyer la valeur de la base MIB cabhQos2PolicyUserImportanceNumber comme argument de sortie "userImportanceNumber" de l'action GetTrafficPolicy.
5) Si aucune entrée concordante n'est trouvée dans la table d'objets de politique, alors le dispositif PS DOIT renvoyer 0 pour les arguments de sortie "trafficImportanceNumber" et "userImportanceNumber". Dans ce cas, le dispositif PS DOIT renvoyer la valeur de la base MIB cabhQos2PolicyAdmissionPolicyEnable comme argument de sortie "admissionPolicyEnable" de l'action GetTrafficPolicy. En outre, le dispositif PS DOIT créer une entrée de règle de politique de type "UPnP" dans la table de base MIB cabhQos2PolicyTable avec un descripteur de trafic UPnP envoyé dans l'action GetTrafficPolicy. Le dispositif PS DOIT régler à 0 l'objet cabhQosPolicyTraffImpNum pour une telle entrée. L'utilisateur ou l'opérateur peut modifier de telles entrées, auquel cas le dispositif PS DOIT modifier l'entrée en la mettant respectivement à la valeur "homeUser" ou "operatorForHomeUser". Le dispositif PS NE DOIT PAS modifier les entrées de type "upnp" en "operatorOnly"}

{texte informatif:

10.3.3 Service de gestionnaire de qualité de service UPnP (QM)

10.3.3.1 Service de gestionnaire de qualité de service UPnP: objectifs

Garantir qu'il y a au moins un service de gestionnaire de qualité de service UPnP pour que des points de commande conformes au modèle UPnP puissent demander la qualité de service dans le réseau local domestique.

10.3.3.2 Service de gestionnaire de qualité de service UPnP: directives de conception

Le portail CQP implémente la fonctionnalité complète de gestionnaire de qualité de service UPnP selon le modèle UQM.

10.3.3.3 Service de gestionnaire de qualité de service UPnP: hypothèses

Il peut y avoir d'autres gestionnaires de qualité de service UPnP dans le réseau local domestique.

10.3.3.4 Service de gestionnaire de qualité de service UPnP: description du système

Le dispositif PS implémente le service de gestionnaire de qualité de service UPnP exactement comme défini dans le modèle UQM. Le service de gestionnaire de qualité de service UPnP dans le dispositif PS ne possède pas d'interface ou de contrôlabilité à partir du réseau régional car il est autonome.

10.3.3.5 Service de gestionnaire de qualité de service UPnP: exigences

Le dispositif PS DOIT implémenter la fonctionnalité complète de gestionnaire de qualité de service UPnP selon le modèle UQM.

Le dispositif PS DOIT annoncer le service de gestionnaire de la qualité de service comme partie du dispositif radical de services de portail CableHome.

Le dispositif PS DOIT prendre en charge l'action RequestTrafficQos du service de gestionnaire de qualité de service UPnP.

Quand un point de commande UPnP invoque l'action QM:RequestTrafficQos du dispositif PS, celui-ci DOIT exécuter ce qui suit:

1) conformément au modèle UQM, si le dispositif PS trouve de multiples instances du service de détenteur de politique de qualité de service UPnP, ce dispositif PS DOIT utiliser la table de politique par défaut du gestionnaire de qualité de service UPnP et DOIT renvoyer le numéro d'importance du trafic UPnP fondé sur cette table par défaut;
2) si le dispositif PS trouve seulement le service de détenteur de politique de qualité de service UPnP résident dans le dispositif PS, alors celui-ci DOIT utiliser les valeurs du numéro d'importance du trafic UPnP, du numéro d'importance de l'utilisateur et d'activation de politique d'admission qui sont extraites de la base MIB cabhQosPolicyTable lors de l'invocation de l'action QD:SetUpTrafficQoS sur diverses instances du service de dispositif de qualité de service UPnP contenues dans le réseau local;
3) si le service de détenteur de politique de qualité de service du dispositif PS est désactivé et si le dispositif PS trouve un seul détenteur de politique de qualité de service UPnP extérieur au dispositif PS, celui-ci DOIT appeler l'action QPH:GetTrafficPolicy pour ce service de détenteur de politique de qualité de service et DOIT utiliser les valeurs de numéro d'importance du trafic, de numéro d'importance de l'utilisateur et d'activation de politique d'admission qui sont renvoyées;
4) le dispositif PS PEUT appeler l'action QD:GetPathInformation sur les instances du service de dispositif de qualité de service (UQD) contenues dans le réseau local;
5) afin de distribuer le numéro d'importance du trafic UPnP, le dispositif PS DOIT appeler l'action QD:SetUpTrafficQoS sur l'instance du service de dispositif de qualité de service au point d'origine et PEUT appeler l'action QD:SetUpTrafficQoS sur d'autres instances du service de dispositif de qualité de service contenues dans le réseau local.

Le dispositif PS DOIT prendre en charge l'action UpdateTrafficQos du service de gestionnaire de qualité de service UPnP.

Quand un point de commande UPnP invoque l'action QM:UpdateTrafficQos du dispositif PS, celui-ci DOIT exécuter ce qui suit:

1) il DOIT d'abord invoquer l'action QD:ReleaseTrafficQos sur l'instance du service de dispositif de qualité de service au point d'origine et PEUT invoquer l'action QD:ReleaseTrafficQos sur d'autres instances du service de dispositif de qualité de service contenues dans le réseau local;

2) il DOIT ensuite invoquer l'action QD:SetUpTrafficQos sur l'instance du service de dispositif de qualité de service au point d'origine et PEUT invoquer l'action QD:SetUpTrafficQos sur des instances du service de dispositif de qualité de service se trouvant sur le trajet, avec le descripteur de trafic mis à jour et fourni par le point de commande dans l'action QM:UpdateTrafficQos.

Le dispositif PS DOIT prendre en charge l'action ReleaseTrafficQos du service de gestionnaire de qualité de service UPnP.

Quand un point de commande UPnP invoque l'action QM:ReleaseTrafficQos dans le dispositif PS, celui-ci DOIT invoquer l'action QD:ReleaseTrafficQos sur l'instance du service de dispositif de qualité de service au point d'origine et PEUT l'appeler sur d'autres instances du service de dispositif de qualité de service contenues dans le réseau local.

Le dispositif PS DOIT prendre en charge l'action BrowseAllTrafficDescriptors du service de gestionnaire de qualité de service UPnP.

Quand un point de commande UPnP invoque l'action QM:BrowseAllTrafficDescriptors dans le dispositif PS, celui-ci DOIT appeler l'action GetQosState sur toutes les instances connues du service de dispositif de qualité de service et renvoyer les informations au point de commande.

10.3.4 Fonctionnalité de qualité de service d'un point de commande (QCP) du dispositif PS

La fonctionnalité de qualité de service d'un point de commande du dispositif PS (point QCP) joue le rôle de point de commande pour toutes les instances du service UPnP de qualité de service dans le réseau domestique. Elle exécute les fonctions associées à un point de commande en termes de découverte, de description et de commande de dispositif et de service. Une autre fonction importante du point de commande de qualité de service du dispositif PS consiste à implémenter la logique permettant de régler la qualité de service du réseau d'accès en réponse à des requêtes de qualité de service d'un réseau domestique via la qualité de service UPnP; et permettant de régler la qualité de service d'un réseau domestique en réponse à des requêtes de qualité de service du réseau d'accès via l'interface CH-PCMM.

10.3.4.1 Fonctionnalité de qualité de service d'un point de commande du dispositif PS: objectifs

Autoriser les câblo-opérateurs à collecter des informations sur divers dispositifs et services UPnP à capacité de qualité de service dans le réseau local domestique.

Autoriser les dispositif PS CableHome à demander la qualité de service d'un réseau domestique en utilisant la messagerie de qualité de service UPnP.

10.3.4.2 Fonctionnalité de qualité de service d'un point de commande du dispositif PS: directives de conception du système

Voir le Tableau 10-7.

Tableau 10-7/J.192 – Fonctionnalité de qualité de service d'un point de commande du dispositif PS – Directives de conception du système

Numéro	Directives
QPSCP.1	Le point de commande du dispositif PS va implémenter la logique de commande compatible avec la qualité de service UPnP.
QPSCP.2	Le point de commande du dispositif PS peut implémenter la logique permettant de demander la qualité de service du réseau local (via la qualité de service UPnP) en réponse à des requêtes de qualité de service du réseau d'accès via l'interface PCMM.

10.3.4.3 Fonctionnalité de qualité de service d'un point de commande du dispositif PS: hypothèses

Le réseau local résidentiel se compose de dispositifs de serveur local UPnP qui implémentent une fonctionnalité de qualité de service compatible avec la qualité de service UPnP.

10.3.4.4 Fonctionnalité de qualité de service d'un point de commande du dispositif PS: description du système

La fonctionnalité de qualité de service d'un point de commande du dispositif PS se compose des éléments suivants:

- logique de découverte de qualité de service;
- logique de courtier de qualité de service CableHome.

10.3.4.4.1 Logique de découverte de qualité de service

La logique de découverte de qualité de service est chargée de découvrir et de décrire toutes les entités de qualité de service UPnP dans le réseau local domestique.

Le point de commande du dispositif PS joue le rôle de point de commande UPnP chargé de la découverte, de la description, de la commande, etc. conformément à l'architecture de dispositif UPnP 1.0 (UDA 1.0). La fonctionnalité de qualité de service du point de commande du dispositif PS est spécifiquement chargée d'exécuter les appels d'action de qualité de service UPnP à appliquer, selon les nécessités, aux instances du service UPnP de qualité de service dans le réseau domestique.

Le modèle CableHome définit la base MIB d'objets cabhPsDevUpnpCommandUpdate afin de demander au dispositif PS de mettre à jour sa table cabhPsDevUpnpInfoTable conformément aux contraintes spécifiées dans les bases cabhPsDevUpnpInfoIp et cabhPsDevUpnpCommand.

Si la base MIB cabhPsDevUpnpCommand est réglée à la valeur qoSDeviceCapabilities et si la base cabhPsDevUpnpCommandUpdate est réglée à la valeur "true", la fonctionnalité de qualité de service de point de commande du dispositif PS invoque l'action QD:GetQoSCapabilities sur l'adresse IP spécifiée dans cabhPsDevUpnpInfoIp. Le dispositif PS mémorise les informations relatives à la capacité du dispositif qui sont renvoyées par le dispositif de qualité de service situé dans la base de données du dispositif PS. Ces informations sont accessibles via la table d'objets de base MIB cabhPsDevUpnpInfoTable.

Si la base MIB cabhPsDevUpnpCommand est réglée à la valeur qoSDeviceState et si la base cabhPsDevUpnpCommandUpdate est réglée à la valeur "true", la fonctionnalité de qualité de service de point de commande du dispositif PS invoque l'action QD:GetQosState() sur l'adresse IP spécifiée dans la base cabhPsDevUpnpCommandIp. Le dispositif PS mémorise les informations relatives à la capacité du dispositif qui sont renvoyées par le dispositif de qualité de service situé dans la base de données du dispositif PS. Ces informations sont accessibles via la base MIB d'objets cabhPsDevUpnpInfoTable.

10.3.4.4.2 Logique de courtier de qualité de service CableHome

La logique de courtier de qualité de service CableHome du point de commande du dispositif PS est chargée de régler la qualité de service dans le réseau domestique en réponse à une demande de l'interface CH-PCMM.

Comme expliqué au § 10.2, Architecture de qualité de service, l'entité de courtier de qualité de service CableHome peut implémenter l'interface CH-PCMM du côté réseau régional afin de négocier la qualité de service du réseau d'accès pour le flux qui relie réseau domestique et réseau d'accès. Le dispositif PS peut recevoir une demande relative à la qualité de service d'un réseau domestique, issue de l'interface CH-PCMM. Le point de commande du dispositif PS est chargé de régler la qualité de service dans le réseau domestique en réponse à une telle requête issue de l'interface CH-PCMM. Il convient de noter que les exigences réelles, concernant l'interface CH-PCMM et le réglage de la qualité de service dans le réseau domestique en réponse à des requêtes issues de l'interface PCMM, seront définies dans les futures spécifications CableHome.

10.3.4.5 Fonctionnalité de qualité de service d'un point de commande du dispositif PS: exigences

1) Quand la base MIB cabhPsDevUpnpCommand [voir § E.4] est réglée à la valeur qoSDeviceCapabilities et quand la base cabhPsDevUpnpCommandUpdate [voir § E.4] est réglée à la valeur "true", le dispositif PS DOIT invoquer l'action QD:GetQoSCapabilities() sur l'adresse IP spécifiée dans la base cabhPsDevUpnpInfoIp [voir § E.4].
2) Le dispositif PS DOIT mémoriser les informations relatives à la capacité du dispositif qui ont été renvoyées par le dispositif de qualité de service en réponse à l'action QD:GetQoSCapabilities() dans la base de données du dispositif PS, informations auxquelles l'on peut accéder au moyen de la base MIB cabhPsDevUpnpInfoTable [voir § E.4].
3) Quand la base MIB cabhPsUpnpCommand est réglée à la valeur qoSDeviceState et quand la base cabhPsDevUpnpCommandUpdate est réglée à la valeur "true", le dispositif PS DOIT invoquer l'action QD:GetQosState() sur l'adresse IP spécifiée dans la base cabhPsDevUpnpInfoIp.

Le dispositif PS DOIT mémoriser les informations relatives à la capacité du dispositif qui ont été renvoyées par le service de dispositif de qualité de service en réponse à l'action QD:GetQosState() dans la base de données du dispositif PS, informations auxquelles l'on peut accéder au moyen de la base MIB cabhPsDevUpnpInfoTable.}

11 Sécurité

11.1 Introduction/Aperçu général

Le présent paragraphe définit les interfaces, les protocoles et les exigences fonctionnelles nécessaires pour sécuriser le dispositif PS et ses opérations.

Assurer la livraison de services IP multimédia fiables aux dispositifs clients dans un réseau domestique exige une passerelle résidentielle sécurisée de même que des mécanismes de sécurité afin de protéger ces services des accès, surveillances et interruptions illicites. L'objet de toute technique de sécurité est de protéger la valeur, y compris les services fondés sur un revenu. Des menaces contre un flux de revenu existent quand un utilisateur du réseau perçoit la valeur, dépense des efforts et de l'argent puis invente une technique afin d'échapper aux paiements nécessaires (voir l'Annexe C). Certains utilisateurs du réseau iront très loin afin de voler quand une valeur est perçue. L'ajout de techniques de sécurité afin de protéger la valeur a un coût associé; plus on dépense d'argent, plus grande est la sécurité (dont l'efficacité relève donc de l'économie de base).

L'architecture de sécurité est centrée sur la sécurisation du réseau local contre les attaques dans le réseau ainsi que sur la sécurisation des communications entre le dispositif PS et les serveurs de tête de réseau. La fonctionnalité PS peut fournir une fondation à d'autres applications et services offerts par le câblo-opérateur au réseau local domestique. La sécurité peut exister pour ces applications indépendamment de l'architecture de sécurité IPCable2Home. Le modèle IPCablecom spécifie des interfaces pour des applications multimédias et possède sa propre architecture de sécurité. Pour toutes références à la sécurité IPCablecom, voir [Rec. UIT-T J.170].

11.1.1 Objectifs

Les objectifs du modèle de sécurité sont les suivants:

- employer une technique de sécurité rentable afin de forcer tout utilisateur ayant l'intention de voler ou d'interrompre des services du réseau à dépenser une quantité déraisonnable d'argent ou de temps;
- sécuriser le réseau IPCable2Home servant à offrir des services de haute valeur par câble de façon qu'il soit au moins aussi sûr que les techniques CableModem et IPCablecom sur le réseau hybride fibre-coaxial (HFC, *hybrid fibre-coax*);
- si possible, aligner les mécanismes de sécurité avec les Recommandations relatives à la sécurité des modèles CableModem et IPCablecom;
- à partir du réseau local, l'architecture de sécurité vise à aider un opérateur, possédant une identité sécurisée, à rendre difficile l'obtention, par un abonné moyen, d'un accès non autorisé au réseau en hybride HFC et aux services par câble.

11.1.2 Hypothèses

Les hypothèses relatives à l'environnement de sécurité sont les suivantes:

- le dispositif PS intégré est censé contenir un câblo-modem J.112 ou J.122;
- le réseau domestique comprend moins de sécurité pour les services de faible valeur;
- des configurations administratives ne sont pas spécifiées et le modèle IPCable2Home implique des configurations minimales par le câblo-opérateur de façon à fonctionner dans les modes spécifiés.

11.2 Architecture de sécurité

L'architecture de sécurité est fondée sur l'architecture de référence définie au § 5. Cette architecture définit un élément de services de portail (PS, *portal service*) qui comprend des fonctions de gestion, de préconfiguration, de sécurité et de qualité de service.

L'architecture comprend également l'ensemble suivant d'éléments de tête de réseau: système de terminaison de câblo-modem (CMTS, *cable modem termination system*), serveur de protocole de configuration dynamique du serveur local (DHCP, *dynamic host configuration protocol*) [RFC 2131], système de gestion de réseau, serveur de protocole trivial de transfert de fichiers (TFTP) dans le réseau câblé, client TFTP dans le dispositif PS, serveur de protocole de transfert d'hypertextes (HTTP) dans le réseau câblé, client http dans le dispositif PS, serveur distant de sécurité de la couche Transport (TLS) [RFC 2246] dans le réseau câblé, client TLS dans le dispositif PS et un serveur de centre de distribution de clés (KDC, *key distribution centre*) dans le réseau câblé.

L'architecture de sécurité se concentre sur la sécurisation du réseau local contre des attaques dans le réseau, ainsi que sur la sécurisation des communications entre le dispositif PS et les serveurs de tête de réseau.

11.2.1 Directives de conception du système

Les exigences relatives à la conception de la sécurité sont énumérées dans le Tableau 11-1 ci-dessous. Cette liste offre des indications sur la mise au point de l'architecture de sécurité.

Tableau 11-1/J.192 – Sécurité: directives de conception du système

Référence	Directives de conception du système de sécurité
SEC1	Ce niveau comprend les capacités nécessaires afin de communiquer les justificatifs d'authentification des éléments.
SEC2	Des justificatifs d'authentification pour le dispositif PS et pour les serveurs administratifs critiques seront fournis. Ces justificatifs définiront un usage spécifique et garantiront une source de confiance.
SEC3	Les messages de gestion de réseau entre la tête du réseau câblé et le dispositif PS peuvent être authentifiés et (facultativement) chiffrés afin de protéger contre une surveillance et une prise de contrôle illicites.
SEC4	Le pare-feu acceptera les fichiers de configuration dans un langage et un format normalisés. (Note).
SEC5	Le câblo-opérateur possédera la capacité de gérer à distance les produits conformes de pare-feu par fichier de configuration ou par commandes SNMP
SEC6	Le pare-feu comportera un ensemble par défaut de règles pour un ensemble minimal prévu de fonctionnalités.
SEC7	Ce niveau offrira la prise en charge nécessaire du modèle IPCablecom par l'intermédiaire du pare-feu.
SEC8	Un ensemble minimal d'exigences sera imposé aux capacités de filtrage par pare-feu concernant les paquets, les ports, les adresses IP et l'heure locale.
SEC9	Une interface détaillée avec la journalisation des événements de pare-feu permettra au câblo-opérateur de surveiller et de réexaminer l'activité de pare-feu comme configuré.
SEC10	Le pare-feu prendra en charge les applications d'usage courant dans des scénarios spécifiques.
SEC11	Le pare-feu protégera les réseaux locaux et régionaux des attaques courantes dans le réseau.
SEC12	La gestion des événements et les ensembles de règles pour le pare-feu seront définis en détail par la base MIB de sécurité.
SEC13	Le câblo-opérateur possédera la capacité de télécharger en sécurité les images logicielles vers l'élément de services de portail.
SEC14	Le câblo-opérateur possédera la capacité d'authentifier et (facultativement) de chiffrer le transport des fichiers de configuration pour le dispositif PS ou le dispositif de pare-feu.
NOTE – Les exigences relatives au fichier de configuration du pare-feu sont définies dans le § 7.4, "Fonction de services de portail – Configuration globale des services de portail (BPSC)".	

Le présent paragraphe limite le domaine d'application de l'architecture de sécurité spécifiée de façon à répondre à ces exigences primaires de sécurité du système. Cependant, il est admis que, dans certains cas, une sécurité supplémentaire est recherchée et peut être ajoutée par le câblo-opérateur selon les besoins. Les préoccupations de câblo-opérateurs ou de constructeurs individuels peuvent se traduire par des protections de sécurité accrues. La présente Recommandation ne restreint pas l'utilisation de protections supplémentaires, aussi longtemps qu'elles n'entrent pas en conflit avec l'intention et les directives de la présente Recommandation.

11.2.2 Description du système

L'architecture de sécurité comprend les éléments de sécurité ci-après:

- domaine de sécurité;
- fonction de services de portail (PS);
- fonction de portail de sécurité par câble (CSP);
- pare-feu (FW);
- centre de distribution de clés (KDC);
- serveur HTTPS avec sécurité TLS.

L'architecture définit l'élément de services de portail dans la passerelle résidentielle. La sécurité n'existe que dans un petit nombre des interfaces spécifiées, comme les directives de conception du système l'exigent. La Figure 11-1 décrit la relation entre les divers éléments qui contiennent des fonctions de sécurité.

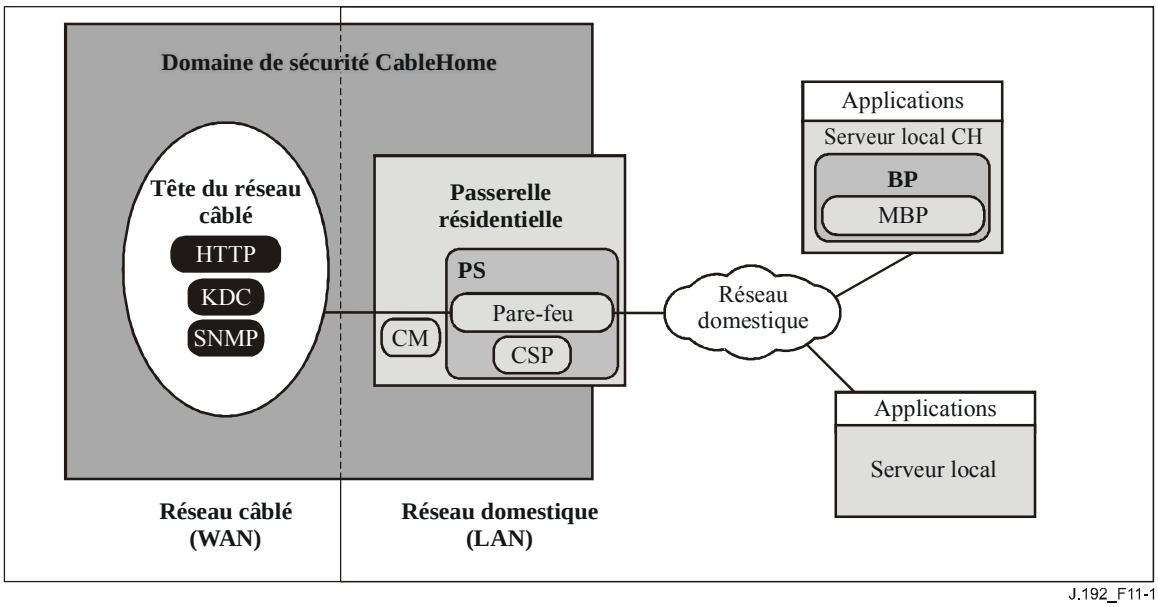


Figure 11-1/J.192 – Eléments de sécurité IPCable2Home

11.2.2.1 Domaine de sécurité

Le domaine de sécurité est défini dans la Figure 11-1 et correspond à l'élément de services de portail situé dans la passerelle résidentielle et aux serveurs de tête de réseau illustrés, avec la sécurité spécifiée. Le domaine de sécurité définit la frontière de la sphère d'influence directe dans laquelle la fonctionnalité de sécurité est étendue à la passerelle résidentielle à partir de la tête du réseau câblé. L'élément de services de portail est entièrement dans le domaine de sécurité, à l'exception de la fonctionnalité de commutation USFS du côté réseau local. Le portail CSP et le pare-feu agissent en tant qu'éléments frontaliers entre le domaine sécurisé et le domaine non sécurisé.

11.2.2.2 Sous-éléments de sécurité associés au dispositif PS

Le dispositif PS comprend les éléments de sécurité ci-après:

- portail de sécurité par câble (CSP);
- pare-feu (FW).

Le portail CSP agit comme un portail de sécurité pour d'autres éléments de services de portail comme la négociation des clés SNMPv3 par codage Diffie-Helman ou Kerberos, comme requis. Le

portail CSP garantit qu'il existe une sécurité pour le protocole SNMPv3 entre le système NMS et le dispositif PS, quand il est activé par le câblo-opérateur. Le portail CSP offre la capacité de valider et de vérifier les certificats numériques aux fins de l'authentification et du chiffrement. Le portail CSP ouvre, gère et ferme une session de sécurité TLS afin de sécuriser le téléchargement du fichier de configuration du dispositif PS et du fichier de configuration du pare-feu, si l'instruction lui en est donnée par le câblo-opérateur pendant l'échange de messages DHCP.

La fonctionnalité de pare-feu du dispositif PS offre une protection à l'utilisateur, ainsi qu'au réseau en hybride HFC, à l'égard du trafic indésirable provenant des secteurs d'adresses WAN, LAN ou PS. De tels trafics peuvent inclure des attaques délibérées contre le réseau domestique, ainsi qu'une limitation du trafic pour des applications de commande parentale. Les exigences de sécurité comprennent des règles spécifiques pour la gestion à distance par le câblo-opérateur.

11.2.2.3 Serveur de centre de distribution de clés (KDC)

Le serveur de centre de distribution de clés (KDC) est requis si le câblo-opérateur déploie le modèle IPCable2Home en mode de préconfiguration SNMP. Si un serveur de centre KDC est disponible dans la tête de réseau, il servira à offrir des services d'authentification mutuelle et de distribution de clés au moyen du protocole Kerberos. S'il est disponible, le centre KDC communiquera avec la fonction de portail CSP afin d'établir ces services.

11.3 Infrastructure d'authentification de dispositif PS

Le présent paragraphe décrit l'authentification du dispositif PS et sa communication avec le centre KDC et avec le serveur HTTPS.

11.3.1 Infrastructure d'authentification de dispositif PS: objectifs

Il est important d'établir l'identité sécurisée de l'élément de services de portail afin d'atteindre les objectifs suivants:

- réduire la possibilité de clonage du dispositif et du logiciel, ainsi que le vol de service. Les passerelles sont dans un environnement réparti où le consommateur a un accès physique domestique à la passerelle. Le fait de fournir une identité sécurisée diminue le risque d'effraction avec le dispositif matériel de passerelle;
- établir la source de confiance. L'infrastructure PKI offre une source de confiance établie qui est enracinée dans la base du constructeur.

11.3.2 Infrastructure d'authentification: directives de conception du système

Voir le Tableau 11-2.

Tableau 11-2/J.192 – Infrastructure d'authentification: directives de conception du système

Référence	Directives
SEC1	Ce niveau comprend les capacités nécessaires afin de communiquer les justificatifs d'authentification pour les éléments IPCable2Home.
SEC2	Les justificatifs d'authentification pour l'équipement CPE et pour les serveurs administratifs critiques seront fournis. Ces justificatifs définiront un usage spécifique et garantiront une source de confiance.

11.3.3 Infrastructure d'authentification: description du système

Aux fins de la sécurité, il est important de savoir avec qui l'on est en communication avant d'échanger des informations significatives. L'authentification offre une identité sécurisée. Il y a trois parties dans l'authentification: le justificatif d'identité, la vérification de la validité du justificatif

d'identité et les moyens communs de communiquer en sécurité les informations d'identité. On spécifie un justificatif d'identification normalisé par l'industrie, constitué par les certificats X.509, en conjonction avec le document [RFC 3280] pour l'utilisation des certificats et Kerberos. Ce justificatif est un protocole de communication courant pour l'authentification mutuelle. Les certificats X.509 sont échangés entre l'élément de services de portail et le centre KDC pendant l'échange PKINIT du protocole Kerberos, lequel est enveloppé dans les messages de demande REQUEST AS et de réponse REPLY AS. Le certificat d'élément de services de portail fournit l'identité de l'élément de services de portail associé en liant cryptographiquement à un certificat de clé publique l'adresse de commande MAC de l'interface entre l'élément PS et le réseau WAN-Man. Chaque côté valide les informations contenues dans le certificat et vérifie la chaîne des certificats en remontant jusqu'à la racine de chaque chaîne. Une fois que la confiance a été établie, les informations relatives aux clés SNMPv3 sont envoyées du centre KDC à l'élément de services de portail. Ce paragraphe relatif à l'authentification décrit l'utilisation du protocole Kerberos et des certificats X.509.

11.3.4 Infrastructure d'authentification: exigences

11.3.4.1 Elément d'authentification par protocole Kerberos

L'authentification est spécifiée quand un centre KDC qui prend en charge IPCable2Home est disponible dans la tête de réseau. Si un centre KDC est disponible, il est recommandé que le câblo-opérateur préconfigure l'élément de services de portail en mode de préconfiguration SNMP (comme décrit dans le § 5.5) afin de tirer parti du protocole d'authentification mutuelle spécifié en se servant du protocole Kerberos, au moyen de l'extension PKINIT. Kerberos offre un protocole permettant de sécuriser l'authentification mutuelle afin d'offrir des matériaux de verrouillage par clés et de n'établir des communications qu'entre les parties authentifiées dans le réseau IPCable2Home. Etant donné que ce modèle d'authentification a déjà été spécifié par un autre projet de l'UIT, c'est-à-dire IPCablecom, le modèle IPCable2Home se réfère au modèle IPCablecom en tant que de besoin.

Divers objets de la base MIB Kerberos sont requis par le modèle IPCablecom. Certains objets de base MIB du modèle IPCablecom, permettant de couvrir la fonctionnalité Kerberos requise par IPCable2Home, ont été définis dans la base MIB de sécurité et sont décrits dans les paragraphes relatifs aux objets de base MIB du présent paragraphe.

La communication entre le centre KDC et le dispositif PS est lancée par le dispositif PS immédiatement après que les options DHCP ont été traitées pendant la préconfiguration, si les options DHCP exigent que le dispositif PS lance une communication vers le centre KDC. Les options DHCP spécifiées dans le § 7.3.3.2.4 exigent la sous-option 10 de l'option 122, qui contient la valeur d'adresse IP du centre KDC à inclure avec les autres options DHCP, et qui DOIT être utilisée par le dispositif PS afin d'établir une communication entre le dispositif PS et le centre KDC. Bien que le modèle IPCablecom exige un nom résolu par service DNS en tant que partie des options DHCP, le service DNS n'est pas requis pour IPCable2Home et l'adresse IP du centre KDC sera donc requise pour que le dispositif PS soit capable de trouver le centre KDC approprié.

11.3.4.1.1 Kerberos/PKINIT

Quand l'élément de services de portail est préconfiguré en mode SNMP, on spécifie l'utilisation du protocole Kerberos avec l'extension de clé publique par authentification PKINIT afin d'authentifier des éléments IPCable2Home et de prendre en charge les exigences relatives à la gestion des clés. Les éléments IPCable2Home (clients) s'authentifient eux-mêmes auprès du centre KDC par le protocole d'authentification PKINIT. Une fois authentifiés auprès du centre KDC, les clients recevront un ticket Kerberos afin de s'authentifier eux-mêmes auprès d'un serveur particulier.

En mode de préconfiguration SNMP, l'élément de services de portail, le système NMS (c'est-à-dire le gestionnaire SNMP) et le centre KDC DOIVENT suivre la spécification relative à

Kerberos/PKINIT, comme défini dans les § 6.4 et 6.5 de la Rec. UIT-T J.170, sauf indication contraire dans la présente Recommandation. Le centre KDC du modèle IPCable2Home est équivalent ou identique au centre KDC d'opérateur MSO du modèle IPCablecom (qui spécifie l'utilisation de plusieurs centres KDC). La spécification IPCable2Home fait appel au terme de *systèmes de gestion de réseau* (NMS) afin d'offrir la fonctionnalité SNMP. Lorsqu'il est fait référence à la suite des spécifications IPCablecom, il est noté que le modèle IPCablecom fait appel au terme *serveur de préconfiguration* afin de désigner la fonctionnalité SNMP, laquelle doit généralement être compatible dans les deux spécifications. Cependant, celles-ci ne sont pas identiques lorsqu'on spécifie des informations propres au modèle IPCablecom et des informations propres au modèle IPCable2Home. L'élément de services de portail DOIT agir en tant que client auprès du centre KDC. Dans la spécification sur la sécurité IPCablecom, c'est l'adaptateur MTA qui est le client. On suppose que les réalisations IPCable2Home utiliseront, pour l'élément de services de portail, la fonctionnalité de client qui est spécifiée pour l'adaptateur MTA. L'élément de services de portail utilise le protocole Kerberos pour la gestion des clés SNMP, ainsi que pour les dispositif d'authentification. Les certificats utilisés dans le protocole PKINIT pour IPCable2Home sont spécifiés dans le paragraphe de la présente Recommandation qui concerne l'infrastructure de clé publique (PKI). Lorsque le modèle IPCablecom spécifie un certificat de dispositif adaptateur MTA, le modèle IPCable2Home offre un certificat pour l'élément de services de portail (certificat d'élément de services de portail) et les implémentations des éléments de services de portail DOIVENT inclure le certificat d'élément de services de portail.

Les paragraphes ci-après de [Rec. UIT-T J.170], concernant la fonctionnalité Kerberos, ne s'appliquent pas au modèle IPCable2Home:

- Paragraphe 6.4.2.1.3, Préauthentificateur pour la localisation du serveur de préconfiguration;
- Paragraphe 6.4.5, Conventions relatives aux emplacements et aux noms des serveurs Kerberos;
- Paragraphe 6.4.6, Noms des mandants d'adaptateur MTA;
- Paragraphe 6.4.7, Mappage d'adresse MAC d'adaptateur MTA sur un nom FQDN d'adaptateur MTA;
- Paragraphe 6.4.9, Suivi des versions des clés de service;
- Paragraphe 6.5.2.1, Messages de renouvellement de clé;
- Paragraphe 6.5.3, Protocole IPSec cerbérisé.

11.3.4.1.2 Variables d'authentification propres au modèle IPCable2Home

Le modèle IPCablecom inclut certains noms de variable dans l'architecture de réseau IPCablecom pour Kerberos. Afin que le modèle IPCable2Home puisse utiliser le modèle IPCablecom, les noms de variable suivants DOIVENT être changés:

- remplacer pktcKdcToMtaMaxClockSkew comme défini dans la spécification de sécurité IPCablecom, par KdcToClientMaxClockSkew;
- remplacer pktcSrvrToMtaMaxClockSkew comme défini dans la spécification de sécurité IPCablecom, par SrvrToClientMaxClockSkew;
- remplacer mtaprovsrvr comme défini dans la spécification sur la sécurité IPCablecom, par provsrvr.

Les implémentations Kerberos du modèle IPCable2Home DOIVENT ignorer la portion de champ contenant l'identificateur d'objet (OID), qui se lit clabProjIPCablecom (2) dans les données AppSpecificTypedData des messages KRB-ERROR.

11.3.4.1.3 Profil pour les conventions relatives aux emplacements et aux noms des serveurs Kerberos

Dans le secteur Kerberos, les noms PEUVENT utiliser la même syntaxe qu'un nom de domaine. Cependant, les secteurs Kerberos DOIVENT être écrits en lettres majuscules. Les détails du secteur Kerberos DOIVENT être suivis conformément à l'Annexe B/J.170.

Les conventions relatives aux centres KDC, énumérées dans le § 6.4.5.2/J.170, sont considérées comme informatives avec la réserve que le centre KDC va exécuter les fonctions nécessaires sur le plan administratif afin d'échanger les informations appropriées avec le système NMS (serveur de préconfiguration ou gestionnaire SNMP). L'élément de services de portail a fourni au centre KDC l'adresse IP du serveur de préconfiguration, dans le message de demande AS, en tant qu'informations nécessaires afin d'établir le contact approprié entre le centre KDC et le serveur de préconfiguration.

Le nom de mandant de l'élément de services de portail DOIT être de type NT-SRV-INST avec exactement deux composants, où le premier composant DOIT être la chaîne "PS" (non compris les guillemets) et où le deuxième composant DOIT être l'adresse MAC du réseau WAN-Man, soit:

PSElement/<WAN-Man-MAC>

où <WAN-Man-MAC> est l'adresse MAC de gestion de réseau régional de l'élément de services de portail. Le format du champ <WAN-Man-MAC> DOIT être "XX:XX:XX:XX:XX:XX" (non compris les guillemets), où X est un caractère hexadécimal de l'adresse MAC. Les caractères hexadécimaux a à f DOIVENT être en minuscules.

Un nom de mandant d'élément de système NMS DOIT être de type NT-SRV-HST avec exactement deux composants, où le premier DOIT être la chaîne "provsrvr" (non compris les guillemets) et où le deuxième DOIT être l'adresse d'entité SNMP du fournisseur de services:

provsrvr/<SNMP entity address>

où l'expression <Adresse de gestionnaire SNMP> DOIT être l'adresse IP du gestionnaire SNMP du fournisseur de services (sous-option 3 de l'option DHCP 122 d'un client CDC) en notation à points entre crochets (p. ex. [12.34.56.78]).

11.3.4.2 Infrastructure de clé publique (PKI)

On utilise des certificats de clé publique qui sont conformes à la Rec. UIT-T X.509 et au document [RFC 3280] du groupe IETF.

11.3.4.2.1 Exigences génériques relatives aux certificats

Le présent paragraphe décrit ce qui est couramment désigné par le terme de *structure générique*, car tous les certificats partagent ces exigences. Tous les certificats spécifiés dans le présent paragraphe DOIVENT inclure les informations suivantes:

- **version du certificat** – la version des certificats DOIT être [Rec. UIT-T X.509], v3, ce qui est noté comme v2 dans le certificat final. Tous les certificats DOIVENT être conformes au document [RFC 3280], sauf si la non-conformité avec le document RFC est explicitement déclarée dans le présent paragraphe. Une quelconque demande de non-conformité selon la présente Recommandation quant au contenu n'implique pas la non-conformité quant au format. Toute demande spécifique de non-conformité quant au format sera explicitement décrite;
- **type de clé publique** – les clés publiques à codage RSA sont utilisées dans toutes les hiérarchies de certificat décrites dans le § 11.3.4.2.2. L'identificateur d'objet subjectPublicKeyInfo.algorithm utilisé DOIT être 1.2.840.113549.1.1.1 (rsaEncryption). L'exposant public pour toutes les clés RSA DOIT être F_4 – 65537;

- **extensions** – les extensions (subjectKeyIdentifier, authorityKeyIdentifier, keyUsage et basicConstraints) DOIVENT suivre le document [RFC 3280]. Toutes les autres extensions de certificat, si incluses, DOIVENT être marquées comme étant non critiques. Les balises de codage sont [c:critique, n:non critiques; m:obligatoire, o:facultatif] et sont identifiées dans le tableau pour chaque certificat;
- **subjectKeyIdentifier** – l'extension subjectKeyIdentifier incluse dans tous les certificats comme requis par le document [RFC 3280] (p. ex. tous les certificats à l'exception des certificats de dispositif et d'auxiliaire) DOIT inclure la valeur KeyIdentifier composée du hachage SHA-1 sur 160 bits de la valeur de la chaîne binaire (BIT STRING) subjectPublicKey (excluant la balise, la longueur et le nombre de bits inutilisés du codage ASN.1) [voir RFC 3280]);
- **authorityKeyIdentifier** – l'extension authorityKeyIdentifier incluse dans tous les certificats comme requis par le document [RFC 3280] DOIT inclure l'identificateur subjectKeyIdentifier extrait du certificat de l'émetteur [RFC 3280]), à l'exception des certificats radicaux;
- **keyUsage** – l'extension keyUsage DOIT servir à tous les certificats d'autorité de certification (CA) et à tous les certificats de vérification de code (CVC). Pour les certificats d'autorité CA, l'extension keyUsage DOIT être marquée comme critique avec une valeur de keyCertSign et cRLSign. Pour les certificats CVC, l'extension keyUsage DOIT être marquée comme critique avec une valeur de digitalSignature et keyEncipherment. Les certificats d'entité terminale PEUVENT utiliser l'extension keyUsage comme indiqué dans le document [RFC 3280];
- **basicConstraints** – l'extension basicConstraints DOIT servir à tous les certificats CA et CVC et DOIT être marquée comme critique. Les valeurs propres à chaque certificat ayant l'extension basicConstraints DOIVENT être marquées comme spécifié dans les Tableaux 11-3 à 11-14 de description de certificat;
- **algorithme de signature** – le mécanisme de signature utilisé DOIT être SHA-1 [FIPS 186-2] avec codage RSA. L'identificateur OID spécifique est 1.2.840.113549.1.1.5;
- **subjectName et issuerName** – si une chaîne ne peut pas être codée comme une chaîne de type PrintableString, elle DOIT être codée comme une chaîne de type UTF8String (balise [UNIVERSAL 12]).

Lors du codage d'un nom X.500:

- chaque nom distinctif relatif (RDN) ne DOIT contenir qu'un seul élément de l'ensemble des attributs X.500;
- l'ordre des noms RDN dans un nom X.500 DOIT être celui dans lequel ils sont présentés dans la présente Recommandation;
- **serialNumber** – le numéro de série DOIT être un nombre entier, unique et positif, attribué par l'autorité CA à chaque certificat (c'est-à-dire que le nom de l'émetteur et le numéro de série désignent un unique certificat). Les autorités CA DOIVENT forcer le numéro de série à être un entier non négatif. Le constructeur NE DEVRAIT PAS imposer ou suggérer de relation entre le numéro de série du certificat et le numéro de série du modem auquel le certificat est envoyé.

  Compte tenu des exigences d'unicité ci-dessus, l'on peut prévoir que les numéros de série contiendront des entiers longs. Les utilisateurs des certificats DOIVENT être capables de manipuler des valeurs de numéro de série jusqu'à 20 octets. Les autorités CA conformes NE DOIVENT PAS utiliser de valeurs de numéro de série de longueur supérieure à 20 octets.

11.3.4.2.2 Hiérarchies des certificats

Trois hiérarchies distinctes de certificat sont utilisées:

1) la chaîne de constructeur sert à identifier les constructeurs autorisés;
2) la chaîne de vérification de code sert à identifier les images logicielles conformes;
3) la chaîne de fournisseur de services sert à identifier les dispositifs contenus dans le réseau du fournisseur de services pour l'authentification mutuelle avec les dispositifs de l'abonné.

Les hiérarchies de certificats décrites dans la présente Recommandation peuvent s'appliquer à tous les projets associés ayant besoin de certificats. Chaque projet peut adopter cette hiérarchie car il est possible de migrer vers une structure de certificat plus générique et partagée. Également, chaque projet peut apporter des ajustements spécifiques aux exigences le concernant. L'objectif est de créer une infrastructure PKI qui puisse être réutilisée pour chaque projet. Il peut y avoir des différences entre les certificats d'entité terminale requis pour chaque projet. Cependant, lorsque des certificats d'entité terminale se superposent, un même certificat d'entité terminale pourrait servir à plusieurs services dans l'infrastructure câblée. Par exemple, le modèle IPCablecom exige un centre KDC pour le fournisseur de services et le modèle IPCable2Home exige également un centre KDC pour le fournisseur de services. Si celui-ci fait fonctionner les deux architectures de réseau sur ses systèmes, il peut utiliser le même centre KDC et le même certificat de centre KDC pour les communications dans les deux systèmes, c'est-à-dire IPCablecom et IPCable2Home. Dans ce cas, le centre KDC du modèle IPCable2Home est équivalent au centre KDC de l'opérateur MSO du modèle IPCablecom (qui spécifie l'utilisation de plusieurs centres KDC).

Dans la Figure 11-2, le terme *autorité de certification* est abrégé en *autorité CA* et le terme *certificat de vérification de code* est abrégé en *certificat CVC.*

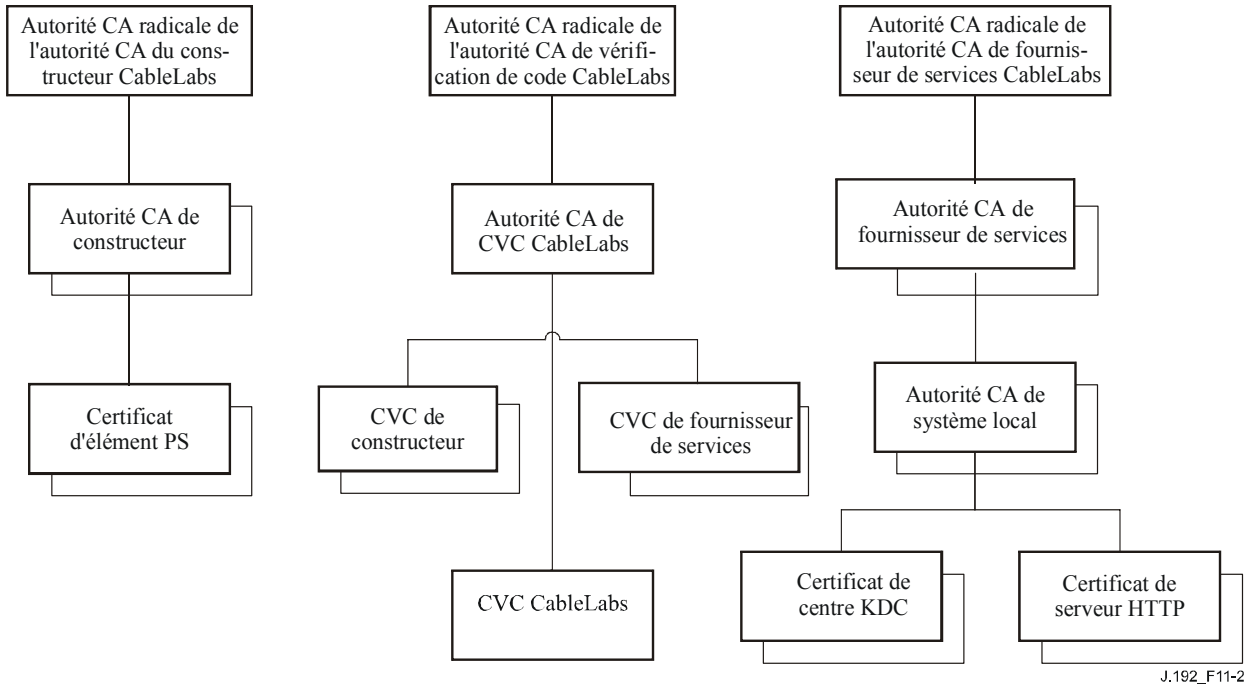


Figure 11-2/J.192 – Hiérarchie des certificats IPCable2Home

11.3.4.2.2.1 Hiérarchie des certificats de constructeur

La hiérarchie des certificats de constructeur, ou de chaîne de constructeurs, est enracinée dans une autorité radicale de constructeur qui sert à envoyer des certificats d'autorité de certification (CA) de constructeur pour un ensemble de constructeurs autorisés. Ceux-ci demandent des certificats individuels d'élément de services de portail à une autorité CA de premier niveau (comme une autorité CA de constructeur ou l'autorité CA du constructeur hébergé localement). Cette chaîne sert à l'authentification des dispositifs domestiques.

Les informations contenues dans les tableaux ci-après sont les valeurs spécifiques pour les champs requis conformément au document [RFC 3280]. Ces valeurs spécifiques de la hiérarchie des certificats de constructeur DOIVENT être suivies selon les Tableaux 11-3, 11-4, 11-5 et 11-6. Si un champ requis n'est pas précisément inscrit dans les tableaux, alors les directives du document [RFC 3280] DOIVENT être suivies. Les extensions génériques DOIVENT également être incluses comme spécifié dans le § 11.3.4.2 sur l'infrastructure PKI.

Certificat d'autorité CA radicale de constructeur

Le certificat d'autorité CA radicale de constructeur (voir le Tableau 11-3) DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat d'autorité CA radicale de constructeur, le certificat d'autorité CA de constructeur et le certificat d'élément de services de portail.

Tableau 11-3/J.192 – Certificat d'autorité CA radicale de constructeur

Forme du nom du titulaire	C=<country> O=<Company Name> CN=[Company Name] autorité radicale de constructeur
Usage prévu	Ce certificat sert à émettre des certificats d'autorité CA de constructeur.
Signé par	Autosigné
Période de validité	20 à 30 ans
Longueur du module	2048
Extensions	keyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true)

Certificat d'autorité CA de constructeur

Si un certificat d'autorité CA est envoyé à un constructeur et sert à émettre le certificat d'élément de services de portail, ce certificat DOIT être vérifié en tant que partie d'une chaîne de certificats contenant le certificat d'autorité CA radicale de constructeur, le certificat d'autorité CA de constructeur et le certificat d'élément de services de portail.

L'état/la région, la ville et l'usine du constructeur sont des attributs facultatifs. Un constructeur peut avoir plusieurs certificats d'autorité CA de constructeur. Si un constructeur utilise plusieurs certificats d'autorité CA de constructeur, l'élément de services de portail DOIT avoir accès au certificat approprié tel que vérifié par mise en correspondance du nom de l'émetteur contenu dans le certificat d'élément de services de portail avec le nom du titulaire contenu dans le certificat d'autorité CA de constructeur. L'identificateur authorityKeyIdentifier du certificat d'élément de services de portail DOIT être mis en correspondance avec l'identificateur subjectKeyIdentifier du certificat du constructeur comme décrit dans [RFC 3280].

Tableau 11-4/J.192 – Certificat d'autorité CA de constructeur

Forme du nom du titulaire	C=<country> O=<Company Name> [ST=<state/province>] [L=<city>] OU= <organization unit> [OU=<Manufacturer's Facility>] CN=<Company Name> Mfg CA
Usage prévu	Ce certificat est envoyé à chaque constructeur par une autorité de certification (CA) radicale de constructeur et peut être offert à chaque élément de services de portail, soit au moment de la construction, ou pendant une mise à jour de code de champ. Ce certificat figure comme un paramètre en lecture seule dans l'élément de services de portail. Ce certificat produit des certificats d'élément de services de portail. Ce certificat, de même que le certificat d'autorité CA radicale de constructeur et le certificat d'élément de services de portail, sert à authentifier l'identité de l'élément de services de portail. L'énumération facultative concernant l'usine du constructeur peut être le nom de l'usine et/ou son emplacement.
Signé par	L'autorité radicale de constructeur indiquée dans la hiérarchie
Période de validité	20 ans
Longueur du module	2048
Extensions	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=0)

Le nom de l'entreprise inséré dans le champ d'organisation (O) PEUT être différent du nom de l'entreprise inséré dans le champ de nom courant (CN, *common name*).

Certificat d'autorité CA de constructeur hébergé localement

Lorsque le certificat d'autorité CA de constructeur hébergé localement sert à émettre le certificat d'élément de services de portail, ce certificat DOIT être vérifié dans le cadre d'une chaîne de certificats contenant le certificat d'autorité CA radicale de constructeur, le certificat d'autorité CA de constructeur hébergé localement, et le certificat d'élément de services de portail.

L'état ou la région, la ville et l'usine du constructeur sont des attributs facultatifs. L'identificateur authorityKeyIdentifier du certificat d'élément de services de portail DOIT être en concordance avec l'identificateur subjectKeyIdentifier du certificat d'autorité CA comme décrit dans [RFC 3280].

Tableau 11-5/J.192 – Certificat d'autorité CA de constructeur hébergé localement

Forme du nom du titulaire	C=<country> O=<CompanyName> [ST=<state/province>] [L=<city>] OU=<CA Identifier>] CN=<CompanyName> Mfg CA
Usage prévu	Ce certificat est envoyé par l'autorité CA radicale de constructeur et peut être fourni à chaque élément de services de portail, soit au moment de la construction, ou pendant une mise à jour de code de champ. Ce certificat figure comme un paramètre en lecture seule dans l'élément de services de portail. Ce certificat produit des certificats d'élément de services de portail. Ce certificat, de même que le certificat d'autorité CA radicale de constructeur et le certificat d'élément de services de portail, sert à authentifier l'identité de l'élément de services de portail.
Signé par	Autorité radicale de constructeur
Période de validité	20 ans
Longueur du module	2048
Extensions	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=0)

Le nom de l'entreprise inséré dans le champ d'organisation (O) PEUT être différent du nom de l'entreprise inséré dans le champ de nom courant (CN, *common name*).

Certificat d'élément de services de portail

Le certificat d'élément de services de portail DOIT être vérifié en tant que partie d'une chaîne de certificats contenant le certificat d'autorité CA radicale de constructeur, le certificat d'autorité CA de constructeur ou le certificat d'autorité CA du constructeur hébergé localement et le certificat d'élément de services de portail.

L'état/la région, la ville, le nom du produit et l'usine du constructeur sont des attributs facultatifs.

L'adresse de commande MAC de l'interface entre l'élément PS et le réseau WAN-Man DOIT être exprimée comme six paires de chiffres hexadécimaux séparés par deux points, par exemple "00:60:21:A5:0A:23". Les caractères hexadécimaux alphabétiques (A à F) DOIVENT être exprimés en majuscules.

Un certificat d'élément de services de portail est installé en permanence, non renouvelable et non remplaçable. Donc, le certificat d'élément de services de portail a une période de validité supérieure à la durée de vie opérationnelle attendue du dispositif spécifique.

Tableau 11-6/J.192 – Certificat d'élément de services de portail

Forme du nom du titulaire	C=<country> O=<Company Name> [ST=<state/province>] [L=<city>] OU=<organization unit> [OU=<Product Name>] [OU=<Manufacturer's Facility>] CN=<WAN-Man MAC Address>
Usage prévu	Ce certificat est envoyé par l'autorité CA du constructeur et installé dans l'usine. Le serveur du système NMS ne peut pas mettre à jour ce certificat. Ce certificat figure comme un paramètre en lecture seule dans l'élément de services de portail. Ce certificat sert à authentifier l'identité de l'élément de services de portail.
Signé par	Autorité CA du constructeur
Période de validité	20 ans au moins
Longueur du module	1024, 1536, 2048
Extensions	keyUsage[c,m](digitalSignature, keyEncipherment), authorityKeyIdentifier [n,m]

11.3.4.2.2.2 Hiérarchie des certificats de vérification de code

La hiérarchie des certificats de vérification de code (CVC), ou chaîne de vérification de code, est enracinée dans une autorité CA radicale de vérification de code qui émet le certificat d'autorité CA de vérification de code. L'autorité CA de vérification de code sert à envoyer des certificats CVC à un ensemble de constructeurs et fournisseurs de services autorisés. L'autorité CA de vérification de code envoie également le certificat CVC. Cette chaîne sert plus précisément à authentifier les téléchargements de logiciel. L'infrastructure PKI du modèle IPCable2Home autorise des certificats CVC de constructeur, un certificat CVC et des certificats CVC de fournisseur de services.

L'entreprise CableLabs sera chargée d'enregistrer les noms des souscripteurs autorisés de certificat CVC. Il appartiendra à l'autorité CA de vérification de code chez CableLabs de garantir que le nom d'organisation de chaque souscripteur de certificat CVC est différent. Les directives suivantes DOIVENT être appliquées lors de l'attribution de noms d'organisation à des cosignataires de fichier de code:

- le nom d'organisation servant à s'identifier comme agent cosignataire de fichier de code dans un certificat CVC DOIT être assigné par CableLabs;
- le nom DOIT être une chaîne imprimable de huit chiffres hexadécimaux qui désigne de façon univoque un agent cosignataire de fichier de code de tous les autres agents;
- chaque chiffre hexadécimal dans le nom DOIT être choisi dans le jeu de caractères 0-9 (0x30-0x39) ou A-F (0x41-0x46);
- la chaîne composée de huit chiffres 0 n'est pas autorisée et NE DOIT PAS être utilisée dans un certificat CVC.

Les informations contenues dans les tableaux ci-après sont les valeurs spécifiques pour les champs requis conformément au document [RFC 3280]. Ces valeurs spécifiques pour la hiérarchie des certificats de vérification de code DOIVENT être suivies selon les Tableaux 11-7, 11-8, 11-9, 11-10 et 11-11 ci-dessous. Si un champ requis n'est pas plus précisément énuméré dans ces tableaux, les

directives figurant dans le document [RFC 3280] DOIVENT être suivies. Les extensions génériques DOIVENT également être incluses comme spécifié dans le § 11.3.4.2 concernant l'infrastructure PKI.

Certificat d'autorité CA radicale de vérification de code

Ce certificat DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat d'autorité CA radicale de vérification de code, l'autorité CA de vérification de code et les certificats de vérification de code.

Tableau 11-7/J.192 – Certificat d'autorité CA radicale de vérification de code

Forme du nom du titulaire	C=<country> O=<Company Name> CN= [Company Name] Autorité CA radicale de certificat CVC
Usage prévu	Ce certificat sert à signer les certificats d'autorité CA de vérification de code
Signé par	Autosigné
Période de validité	20 à 30 ans
Longueur du module	2048
Extensions	keyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true)

Certificat d'autorité CA de vérification de code

Le certificat d'autorité CA de vérification de code DOIT être vérifié en tant que partie d'une chaîne de certificats contenant le certificat d'autorité CA radicale de vérification de code, le certificat d'autorité CA de vérification de code et le certificat de vérification de code. Un dispositif PS autonome NE DOIT prendre en charge en charge qu'une seule autorité CA de vérification de code à la fois.

Tableau 11-8/J.192 – Certificat d'autorité CA de vérification de code

Forme du nom du titulaire	C=<country> O=<Company Name><Eight (8)> character hexadecimal value> CN= [Company Name] CVC CA
Usage prévu	Ce certificat est envoyé à l'autorité de certification par l'autorité CA radicale de vérification de code. Ce certificat produit des certificats de vérification de code.
Signé par	L'autorité CA radicale de vérification de code de la hiérarchie
Période de validité	20 ans
Longueur du module	2048
Extensions	keyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints [c,m](cA=true, pathLenConstraint=0)

Certificat de vérification de code de constructeur

Ce certificat DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat d'autorité CA radicale de vérification de code, le certificat d'autorité CA de vérification de code et les certificats de vérification de code.

Tableau 11-9/J.192 – Certificat de vérification de code de constructeur

Forme du nom du titulaire	C=<country> O=<Company Name> [ST=<state/province>] [L=<city>] CN=<Company Name> Mfg CVC
Usage prévu	L'autorité CA de vérification de code envoie ce certificat à chaque constructeur autorisé. Il sert à la politique établie par le câblo-opérateur pour le téléchargement sécurisé de logiciel. Le nom d'entreprise peut être différent dans les champs O et CN.
Signé par	L'autorité CA de vérification de code
Période de validité	jusqu'à 10 ans
Longueur du module	1024, 1536, 2048
Extensions	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m]

Certificat de vérification de code

Le certificat de vérification de code DOIT être vérifié en tant que partie d'une chaîne de certificats contenant le certificat d'autorité CA radicale de vérification de code, le certificat d'autorité CA de vérification de code et le certificat de vérification de code.

Tableau 11-10/J.192 – Certificat de vérification de code

Forme du nom du titulaire	C=<country> O=<Eight (8)> character hexadecimal value> CN=<Company Name>CVC
Usage prévu	L'autorité CA de vérification de code envoie ce certificat. Il sert à authentifier le code certifié. Il sert à la politique établie par le câblo-opérateur pour le téléchargement sécurisé de logiciel.
Signé par	L'autorité CA de vérification de code
Période de validité	jusqu'à 10 ans
Longueur du module	1024, 1536, 2048
Extensions	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m]

Certificat de vérification de code du fournisseur de services

Le certificat de vérification de code du fournisseur de services DOIT être vérifié en tant que partie d'une chaîne de certificats contenant le certificat d'autorité CA radicale de vérification de code, le certificat d'autorité CA de vérification de code et le certificat de vérification de code du fournisseur de services.

Tableau 11-11/J.192 – Certificat de vérification de code du fournisseur de services

Forme du nom du titulaire	C=<country> O=<Eight (8) character hexadecimal value> [ST=<state/province>] [L=<city>] CN=<Company Name> Certificat CVC du fournisseur de services
Usage prévu	L'autorité CA de vérification de code envoie ce certificat à chaque fournisseur de services autorisé. Il sert à la politique établie par le câblo-opérateur pour le téléchargement sécurisé de logiciel. Le nom d'entreprise peut être différent dans les champs O et CN.
Signé par	L'autorité CA de vérification de code
Période de validité	jusqu'à 10 ans
Longueur du module	1024, 1536, 2048
Extensions	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m]

11.3.4.2.2.3 Hiérarchie des certificats de fournisseur de services

La hiérarchie des certificats de fournisseur de services, ou chaîne de fournisseur de services, est enracinée dans une autorité CA radicale de fournisseur de services qui sert à envoyer des certificats à un ensemble de fournisseurs de services autorisés. L'autorité CA de fournisseur de services peut servir à envoyer des certificats facultatifs d'autorité CA de système local ou des certificats auxiliaires. Si l'autorité CA de fournisseur de services ne produit pas les certificats auxiliaires, c'est l'autorité CA du système local qui le fera. Les certificats auxiliaires sont les certificats d'entité terminale dans le réseau du câblo-opérateur.

Les informations contenues dans les tableaux ci-après sont les valeurs spécifiques pour les champs requis conformément au [RFC 3280]. Ces valeurs spécifiques pour la hiérarchie des certificats de fournisseur de services DOIVENT être suivies selon les Tableaux 11-12 à 11-16 ci-dessous. Si un champ requis n'est pas plus précisément énuméré dans les tableaux, les directives figurant dans [RFC 3280] DOIVENT être suivies. Les extensions génériques du modèle IPCable2Home DOIVENT également être incluses comme spécifié dans le § 11.3.4.2 concernant l'infrastructure PKI.

Certificat d'autorité CA radicale de fournisseur de services

Ce certificat DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat d'autorité CA radicale de fournisseur de services, le certificat d'autorité CA de fournisseur de services, le certificat facultatif d'autorité CA du système local et les certificats auxiliaires.

Tableau 11-12/J.192 – Certificat d'autorité CA radicale de fournisseur de services

Forme du nom du titulaire	C=<country> O=<Company Name> CN=<Company Name> Autorité CA radicale de fournisseur de services
Usage prévu	Ce certificat sert à envoyer les certificats d'autorité CA du fournisseur de services
Signé par	Autosigné
Période de validité	20 à 30 ans
Longueur du module	2048
Extensions	keyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true)

Certificat d'autorité CA de fournisseur de services

Le certificat d'autorité CA de fournisseur de services DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat d'autorité CA radicale de fournisseur de services, le certificat d'autorité CA de fournisseur de services, le certificat facultatif d'autorité CA du système local et les certificats auxiliaires.

Tableau 11-13/J.192 – Certificat d'autorité CA de fournisseur de services

Forme du nom du titulaire	C=<country> O=<Company Name> CN=<Company Name> Autorité CA de fournisseur de services
Usage prévu	L'autorité CA radicale de fournisseur de services envoie ce certificat à chaque fournisseur de services. Afin de faciliter la mise à jour de ce certificat, chaque élément de réseau est configuré avec l'attribut OrganizationName du nom SubjectName contenu dans le certificat d'autorité CA de fournisseur de services. C'est le seul attribut dans le certificat qui doit rester constant. Ce certificat figure comme un paramètre en lecture-écriture dans l'objet de base MIB qui identifie l'attribut OrganizationName pour le secteur Kerberos du modèle IPCable2Home. L'élément IPCable2Home n'accepte pas les certificats de fournisseur de services qui ne correspondent pas à cette valeur de l'attribut OrganizationName dans le champ SubjectName. Si la tête de réseau contient un centre KDC qui prend en charge IPCable2Home, alors l'élément de services de portail doit exécuter le premier échange PKINIT avec le centre KDC juste après un réamorçage, moment auquel ses tables de base MIB ne sont pas encore configurées. A ce moment, le client Kerberos dans le modèle IPCable2Home DOIT accepter tout attribut OrganizationalName du fournisseur de services, mais DOIT vérifier ultérieurement que la valeur ajoutée dans l'objet de base MIB pour ce secteur est celle qui est contenue dans la réponse PKINIT initiale. Cette autorité CA envoie de certificats d'autorité CA de système local ou des certificats auxiliaires.

Tableau 11-13/J.192 – Certificat d'autorité CA de fournisseur de services

Signé par	Autorité CA radicale de fournisseur de services
Période de validité	20 ans
Longueur du module	2048
Extensions	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=1)

Le nom de l'entreprise dans le champ d'organisation (O) peut être différent du nom de l'entreprise dans le champ de nom courant (CN).

Certificat d'autorité CA de système local

Ce certificat est facultatif pour le fournisseur de services. Si ce certificat existe, il DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat d'autorité CA radicale de fournisseur de services, le certificat d'autorité CA de fournisseur de services, le certificat facultatif d'autorité CA du système local et les certificats auxiliaires.

Tableau 11-14/J.192 – Certificat d'autorité CA de système local

Forme du nom du titulaire	C=<country> O=<Company Name> OU=<Local System Name> CN=<Company Name> Autorité CA de système local
Usage prévu	Ce certificat est facultatif et, s'il existe, est envoyé par l'autorité CA de fournisseur de services. Cette autorité CA envoie des certificats auxiliaires. Les serveurs du réseau sont autorisés à migrer librement entre autorités CA régionales du même fournisseur de services.
Signé par	Autorité CA de fournisseur de services
Période de validité	20 ans
Longueur du module	1024, 1536, 2048
Extensions	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=0)

Le nom de l'entreprise dans le champ d'organisation (O) peut être différent du nom de l'entreprise dans le champ de nom courant (CN).

Certificat de centre KDC

Ce certificat DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat d'autorité CA radicale de fournisseur de services, le certificat d'autorité CA de fournisseur de services, le certificat facultatif d'autorité CA du système local et les certificats auxiliaires (p. ex. Les certificats de centre KDC).

Le certificat de centre KDC DOIT inclure le nom subjectAltName d'authentification PKINIT du secteur Kerberos comme spécifié dans le 8.2.3.4.1/J.170 concernant le certificat de centre de distribution de clés.

Tableau 11-15/J.192 – Certificat de centre KDC

Forme du nom du titulaire	C=<country> O=<Company Name> [OU=<Local System Name>] OU=<Company Name> Centre de distribution de clés CN=<Nom du serveur DNS>
Usage prévu	Ce certificat est envoyé soit par l'autorité CA de fournisseur de services ou par l'autorité CA du système local. Il sert à authentifier l'identité du centre KDC auprès des clients du protocole Kerberos pendant les échanges PKINIT. Ce certificat est transmis vers l'élément de services de portail à l'intérieur de la réponse PKINIT.
Signé par	Autorité CA de fournisseur de services ou l'autorité CA du système local
Période de validité	20 ans
Longueur du module	1024, 1536, 2048
Extensions	keyUsage[c,o](digitalSignature) authorityKeyIdentifier[n,m](KeyIdentifier=<subjectKeyIdentifier value from CA certificate>) subjectAltName[n,m] (voir Annexe C/J.170)

Certificat de serveur HTTPS

Ce certificat DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat d'autorité CA radicale de fournisseur de services, le certificat d'autorité CA de fournisseur de services, le certificat facultatif d'autorité CA du système local et les certificats auxiliaires (p. ex. les certificats de centre KDC).

Tableau 11-16/J.192 – Certificat de serveur HTTPS

Forme du nom du titulaire	C=<country> O=<Company Name> [OU=<Local System Name>] OU=<Company Name> Serveur HTTPS CN=<Nom du serveur DNS>
Usage prévu	Ce certificat est envoyé soit par l'autorité CA de fournisseur de services ou par l'autorité CA du système local. Il sert à authentifier l'identité du serveur HTTPS auprès des clients http pour la session de protocole TLS pendant la préconfiguration. Ce certificat est transmis à l'élément de services de portail à l'intérieur du message de certificat de serveur TLS.
Signé par	Autorité CA de fournisseur de services ou l'autorité CA du système local
Période de validité	20 ans
Longueur du module	1024, 1536, 2048
Extensions	keyUsage[c,m](digitalSignature, keyEncipherment, dataEncipherment), extendedKeyUsage[n,m] (id-kp-serverAuth), authorityKeyIdentifier [n,m]

11.3.4.2.3 Validation de certificat

La validation de certificat IPCable2Home implique la validation d'une chaîne de certificats liés depuis les certificats d'entité terminale jusqu'à la racine valide. Par exemple, la signature figurant sur le certificat d'élément de services de portail est vérifiée avec le certificat d'autorité CA de constructeur puis la signature figurant sur le certificat d'autorité CA de constructeur est vérifiée avec le certificat d'autorité CA radicale de constructeur. Le certificat d'autorité CA radicale de constructeur est autosigné et reçu à partir d'une source autorisée d'une façon sécurisée. La clé publique présente dans le certificat d'autorité CA radicale de constructeur sert à valider la signature portée sur le même certificat.

Les règles exactes pour la validation de la chaîne de certificats DOIVENT être pleinement conformes au document [RFC 3280], où elles sont désignées par le terme de *validation de chemin de certificat*. En général, les certificats [UIT-T X.509] prennent en charge un ensemble de règles souples afin de déterminer si le nom de l'émetteur d'un certificat correspond au nom du titulaire d'un autre. Les règles sont telles que deux champs de nom PEUVENT être déclarés en correspondance bien qu'une comparaison binaire des deux champs de nom n'indique pas de correspondance. Le document [RFC 3280] recommande que les autorités de certification interdisent le codage des champs de nom, de façon qu'une implémentation puisse déclarer une correspondance ou une non-correspondance au moyen d'une simple comparaison binaire. La sécurité IPCable2Home suit la présente Recommandation. En conséquence, le champ codé en règles DER tbsCertificate.issuer d'un certificat IPCable2Home DOIT être une correspondance exacte du champ codé en règles DER tbsCertificate.subject de son certificat d'émetteur. Une implémentation PEUT comparer un nom d'émetteur à un nom de titulaire en exécutant une comparaison binaire des champs codés en règles DER tbsCertificate.issuer et tbsCertificate.subject.

La validation des périodes de validité pour l'intégration n'est pas vérifiée et n'est pas mise en œuvre intentionnellement, ce qui est conforme aux normes en vigueur. Au moment de l'émission, la date de début de validité de tout certificat d'entité terminale DOIT être identique ou postérieure à la date de début de la période de validité du certificat de l'autorité CA émettrice. Après qu'un certificat d'autorité CA a été renouvelé, les dates de début des certificats d'entité terminale PEUVENT être antérieures à la date de début du certificat de l'autorité CA émettrice. La date de fin de validité des certificats d'entité terminale peut être antérieure, identique, ou postérieure à la date de fin de validité pour l'autorité CA émettrice, comme spécifié dans les tableaux de certificat IPCable2Home.

11.3.4.2.3.1 Validation de la chaîne de constructeur et vérification de la racine

Le centre KDC validera la chaîne de certificats liés du constructeur. Habituellement, le premier certificat de la chaîne n'est pas explicitement inclus dans la chaîne de certificats qui est émise sur le câble. Lorsque le certificat d'autorité CA radicale de constructeur est explicitement inclus dans la transmission, il DOIT déjà être connu du vérificateur avant le moment de vérifier ce certificat. Le certificat d'autorité CA radicale de constructeur émis sur le câble NE DOIT PAS contenir de modification de certificat, à l'exception possible du numéro de série du certificat, de sa période de validité et de la valeur de sa signature. Si des changements autres que le numéro de série du certificat, sa période de validité et sa valeur de signature existent dans le certificat d'autorité CA radicale de constructeur qui a été transmis sur le câble par rapport au certificat connu d'autorité CA radicale de constructeur, le centre KDC effectuant la comparaison DOIT échouer à la vérification du certificat.

11.3.4.2.3.2 Validation de la chaîne de vérification de code et vérification de la racine

Un serveur administratif peut vérifier la validité de la chaîne de vérification de code avant de commencer le processus de téléchargement de logiciel. Pour plus de détails, voir ci-dessous le § 11.8: Téléchargement sécurisé de logiciel pour le dispositif PS.

11.3.4.2.3.3 Validation de la chaîne de fournisseur de services et vérification de la racine

L'élément de services de portail DOIT valider la chaîne des certificats liés de fournisseur de services. Habituellement, le premier certificat de la chaîne n'est pas explicitement inclus dans la chaîne de certificats qui est émise sur le câble. Lorsque le certificat d'autorité CA radicale de fournisseur de services est explicitement inclus dans le câble, il DOIT déjà être connu par le vérificateur avant le moment de vérifier ce certificat. Le certificat d'autorité CA radicale de fournisseur de services NE DOIT PAS contenir de modification au certificat, à l'exception possible du numéro de série du certificat, de sa période de validité et de sa valeur de signature. Si des changements autres que le numéro de série du certificat, sa période de validité et sa valeur de signature existent dans le certificat d'autorité CA radicale de fournisseur de services qui a été transmis sur le câble par rapport au certificat connu d'autorité CA radicale de fournisseur de services, l'élément de services de portail effectuant la comparaison DOIT échouer à la vérification du certificat.

11.3.4.2.4 Révocation de certificat

La révocation de certificat est hors du domaine d'application de la présente Recommandation.

11.4 Messagerie de gestion sécurisée envoyée au dispositif PS

L'algorithme de sécurité servant à lancer la messagerie de gestion SNMP dépend du mode de préconfiguration de l'élément de services de portail (voir § 5.5). Dans le modèle IPCable2Home, il y a trois modes de préconfiguration: le mode de préconfiguration DHCP, le mode de préconfiguration SNMP et le mode inactif. Le mode de préconfiguration DHCP comporte des sous-modes additionnels qui permettent de savoir s'il est configuré en mode d'accès NmAccess ou en mode de coexistence. Le mode de préconfiguration SNMP exige la version SNMPv3 pour la messagerie de gestion.

Les paragraphes ci-après décrivent les algorithmes de sécurité et les exigences nécessaires pour initialiser la messagerie de gestion SNMP fondée sur le mode de préconfiguration de l'élément de services de portail, lequel DOIT prendre en charge les algorithmes de sécurité SNMPv3 spécifiés dans les § 11.4.4.1.2 et 11.4.4.2.

11.4.1 Messagerie de gestion sécurisée: objectifs

Les messages de gestion sécurisée comprennent les objectifs suivants:

- offrir des options afin de chiffrer les messages de gestion de réseau envoyés au dispositif PS;
- offrir des options afin d'authentifier les messages de gestion de réseau envoyés au dispositif PS;
- si possible, offrir une sécurité de messagerie de gestion n'exigeant pas l'implémentation de protocoles additionnels;
- offrir des directives et les exigences minimales relatives aux algorithmes de chiffrement et d'authentification.

11.4.2 Messagerie de gestion sécurisée: directives de conception du système

Référence	Directives de conception du système de sécurité
SEC3	Les messages de gestion de réseau entre la tête du réseau câblé et le dispositif PS peuvent être authentifiés et (facultativement) chiffrés afin de protéger contre une surveillance et une prise de contrôle illicites.

11.4.3 Messagerie de gestion sécurisée: description du système

La messagerie du protocole SNMP de gestion est envoyée au dispositif PS à partir du réseau des câblo-opérateurs. Le protocole SNMP est adopté dans les produits de l'industrie du câble depuis plusieurs années. Le bureau administratif du câblo-opérateur peut prendre en charge les versions SNMPv1, v2 ou v3. Le dispositif PS est tenu de prendre en charge la messagerie de gestion dans les trois versions du protocole SNMP. Aucune sécurité proprement dite n'est intégrée dans les versions SNMPv1 ou v2. La version SNMPv3 offre les algorithmes d'authentification et de chiffrement de base qui sont définis dans les documents [RFC 3410], [RFC 3415] et [RFC 3584] et le modèle IPCable2Home spécifie l'utilisation de la sécurité définie par ces documents RFC. La version SNMPv3 ne spécifie pas comment les clés sont réglées de façon à lancer les processus de chiffrement et d'authentification: certains détails permettant de produire et d'établir un échange de clés sont donc spécifiés. Ces détails sont énumérés dans le paragraphe suivant.

11.4.4 Messagerie de gestion sécurisée: exigences

11.4.4.1 Algorithmes de sécurité pour le protocole SNMP en mode de préconfiguration DHCP

En mode de préconfiguration DHCP, l'élément de services de portail peut être configuré en mode d'accès NmAccess ou en mode de coexistence. En mode de coexistence, l'élément de services de portail peut être configuré pour la messagerie de gestion en protocole SNMPv1, SNMPv2, et/ou SNMPv3.

11.4.4.1.1 Mode d'accès NmAccess

Si l'élément de services de portail est préconfiguré en mode DHCP avec le mode d'accès NmAccess, la gestion de réseau par protocole SNMP située dans l'élément de services de portail n'utilise pas la version SNMPv3 et n'a donc pas besoin de lancer les fonctions de sécurité SNMPv3. L'initialisation de la liaison de gestion SNMPv1/v2 est définie dans le § 6.3.3.1.

11.4.4.1.2 Mode de coexistence

Si l'élément de services de portail est en mode de préconfiguration DHCP et en mode de coexistence et si le protocole de la messagerie de gestion est déterminé comme étant en version SNMPv3 (voir § 6.3.3.1), alors l'élément de services de portail DOIT utiliser les fonctions de sécurité SNMPv3 spécifiées par le document [RFC 3414]. Le dispositif PS DOIT prendre en charge l'authentification SNMPv3 et la confidentialité SNMPv3. Le câblo-opérateur est fortement encouragé à activer en permanence l'authentification par protocole SNMPv3. L'utilisation de la confidentialité par protocole SNMPv3 est recommandée si le câblo-opérateur peut manipuler le surcroît de charge pour le chiffrement.

Afin d'établir des clés SNMPv3 en mode de préconfiguration DHCP, toutes les interfaces en protocole SNMP du modèle IPCable2Home DOIVENT utiliser la procédure SNMPv3 d'initialisation et de changements de clé comme défini dans le § 2.2 de la spécification DOCSIS 1.1 concernant l'interface avec les systèmes d'exploitation [ANSI/SCTE 23-3 2005] (remplacer les termes "CM" par "élément de services de portail" et "conforme au modèle DOCSIS 1.1" par "conforme au modèle IPCable2Home").

Afin de prendre en charge l'initialisation et les changements de clé SNMPv3 en mode de préconfiguration DHCP, l'élément de services de portail DOIT également être capable de recevoir des éléments TLV de types 34, 34.1 et 34.2, comme défini dans le § B.C.1.2.8 de la spécification DOCSIS 1.1 concernant l'interface radioélectrique [Annexe B de la Rec. J.112] et d'implémenter le mécanisme de changement de clé spécifié dans le document [RFC 2786], qui comprend l'objet de base MIB usmDHKickstartTable.

11.4.4.1.3 Initialisation de clé SNMPv3

Pour chacun d'un maximum de cinq noms de sécurité différents, l'autorité ultime (CHAdministrator) produit une paire de nombres. Tout d'abord, l'autorité CHAdministrator produit un nombre aléatoire Rm.

Puis l'autorité CH Administrator fait appel à l'équation de Diffie-Helman afin de convertir Rm en nombre public z. L'équation est la suivante:

$$z = g \text{ ^ } Rm \text{ MOD } p$$

où g est extrait de l'ensemble de paramètres de Diffie-Helman et où p est le nombre premier extrait de ces paramètres.

Le fichier de configuration du dispositif PS est créé de façon à inclure la paire (nom de sécurité, nombre public). Le dispositif PS DOIT prendre en charge un minimum de cinq paires. Par exemple:

TLV de type 34.1 (nom de sécurité de démarrage SNMPv3) = CHAdministrator

TLV de type 34.2 (nombre public de démarrage SNMPv3) = z

Le dispositif PS DOIT prendre en charge les entrées dans le modèle VACM définies dans le § 6.3.3.1.4.5. Seules les entrées VACM spécifiées par le nom de sécurité correspondant dans le fichier de configuration du dispositif PS DOIVENT être actives.

Pendant le processus d'amorçage du dispositif PS, les valeurs ci-dessus (nom de sécurité, nombre public) DOIVENT être incluses dans la table usmDHKickstartTable.

A ce point:

usmDHKickstartMgrpublic.1 = "z" (chaîne d'octets)

usmDHKickstartSecurityName.1 = "CHAdministrator"

Quand l'objet usmDHKickstartMgrpublic.n est établi avec une valeur valide pendant l'inscription, une rangée correspondante est créée dans la table usmUserTable avec les valeurs suivantes:

usmUserEngineID: localEngineID

usmUserName: valeur usmDHKickstartSecurityName.n

usmuserSecurityName: valeur usmDHKickstartSecurityName.n

usmUserCloneFrom: ZeroDotZero

usmUserAuthProtocol: usmHMACMD5AuthProtocol [RFC 2104]

usmuserAuthKeyChange: (valeur déduite de la valeur établie)

usmUserOwnAuthKeyChange: (valeur déduite de la valeur établie)

usmUserPrivProtocol: usmDESPrivProtocol

usmUserPrivKeyChange: (valeur déduite de la valeur établie)

usmUserOwnPrivKeyChange: (valeur déduite de la valeur établie)

usmUserPublic

usmUserStorageType: permanent

usmUserStatus: active

NOTE – Pour les entrées (PS) dhKickstarts dans la table usmUserTable, "permanent" signifie qu'elles DOIVENT être écrites mais non supprimées et ne sont pas sauvegardées après un réamorçage.

Après que le dispositif PS a achevé l'initialisation (ce qui est indiqué par une valeur égale à '1' (succès) de l'objet cabhPsDevProvState):

1) le dispositif PS produit un nombre aléatoire xa pour chaque rangée remplie dans la table usmDHKickstartTable qui a un nom usmDHKickstartSecurityName et une entrée usmDHKickstartMgrPublic de longueur différente de zéro;

2) le dispositif PS fait appel à l'équation de Diffie-Helman afin de convertir xa en nombre public c (pour chaque rangée identifiée ci-dessus).

$$C = g \text{ ^ } xa \text{ MOD } p$$

où g est extrait de l'ensemble de paramètres de Diffie-Helman et p est le nombre premier extrait de ces paramètres.

A ce point:

usmDHKickstartMyPublic.1 = "c" (chaîne d'octets)

usmDHKickstartMgrPublic.1 = "z" (chaîne d'octets)

usmDHKickstartSecurityName.1 = "CHAdministrator"

3) le dispositif PS calcule un secret partagé sk où sk = z ^xa mod p;

4) le dispositif PS fait appel à sk afin de calculer la clé de confidentialité et la clé d'authentification pour chaque rangée de la table usmDHKickstartTable et règle les valeurs dans la table usmUserTable.

Comme spécifié dans le document [RFC 2786], la clé de confidentialité et la clé d'authentification pour le nom d'utilisateur associé, "CHAdministrator" dans ce cas, sont déduites de sk par application de la fonction de calcul de clé PBKDF2 définie dans PKCS#5 v2.0.

clé de confidentialité ← PBKDF2(salt = 0xd1310ba6,
iterationCount = 500,
keyLength = 16,
prf = id-hmacWithSHA1) [RFC 2104]

clé d'authentification ← PBKDF2(salt = 0x98dfb5ac,
iterationCount = 500,
keyLength = 16 (usmHMACMD5AuthProtocol) [RFC 2104],
prf = id-hmacWithSHA1) [RFC 2104]

A ce point, le dispositif PS (portail CMP) a achevé son processus d'initialisation SNMPv3 et DOIT permettre un niveau d'accès approprié à un nom de sécurité valide avec la clé d'authentification et/ou de confidentialité correcte.

Le dispositif PS DOIT correctement remplir les tables appropriées avec les clés comme spécifié par les documents RFC se rapportant à la version SNMPv3 et [RFC 2786].

5) Ce qui suit décrit le processus auquel le gestionnaire fait appel afin de calculer la clé d'authentification et la clé de confidentialité uniques du dispositif PS.

Le gestionnaire SNMP accède au contenu de la table usmDHKickstartTable au moyen du nom de sécurité de l'objet 'dhKickstart' sans authentification.

Le dispositif PS DOIT offrir des entrées préinstallées dans les tables des modèles USM et VACM afin de créer correctement l'utilisateur 'dhKickstart' de niveau de sécurité noAuthNoPriv qui a l'accès en lecture seule à système groupe et usmDHkickstartTable.

Si le dispositif PS est en mode de coexistence et est configuré de façon à utiliser SNMPv3 la spécification de groupe pour la vue dhKickstart DOIT être mise en œuvre comme suit:

dhKickstart Group

vacmGroupName 'dhKickstart'

vacmAccessContextPrefix ''

vacmAccessSecurityModel 3 (USM)

vacmAccessSecurityLevel NoAuthNoPriv

vacmAccessContextMatch exact

vacmAccessReadViewName 'dhKickstartView'

vacmAccessWriteViewName ''

vacmAccessNotifyViewName ''

vacmAccessStorageType permanent

vacmAccessStatus active

La vue de modèle VACM pour la vue dhKickstart DOIT être implémentée comme suit:

dhKickstartView subtree 1.3.6.1.2.1.1 (Groupe de Système) et 1.3.6.1.3.101.1.2.1 (usmDHkickstartTable)

Le gestionnaire SNMP obtient la valeur du nombre usmDHKickstartMypublic du dispositif PS associé au nom de sécurité pour lequel le gestionnaire souhaite calculer les clés d'authentification et de confidentialité. Au moyen du nombre aléatoire privé, le gestionnaire peut calculer le secret partagé à codage DH. A partir de ce secret partagé, le gestionnaire peut calculer les clés opérationnelles d'authentification et de confidentialité pour le nom de sécurité que le gestionnaire va utiliser afin de communiquer avec le dispositif PS.

11.4.4.1.4 Changements de clé à codage Diffie-Helman

Le dispositif PS DOIT prendre en charge le mécanisme de changement de clé spécifié dans le paragraphe ci-dessus ainsi que dans le document [RFC 2786].

11.4.4.2 Algorithmes de sécurité pour le protocole SNMPv3 en mode de préconfiguration SNMP

Si l'élément de services de portail est en mode de préconfiguration SNMP, la gestion de réseau par protocole SNMP dans l'élément de services de portail DOIT exploiter la version SNMPv3 avec la sécurité spécifiée par le document [RFC 3414]. Le dispositif PS DOIT prendre en charge l'authentification SNMPv3 et la confidentialité SNMPv3. Le câblo-opérateur est fortement encouragé à activer en permanence l'authentification SNMPv3. L'utilisation de la confidentialité par protocole SNMPv3 est recommandée si le câblo-opérateur peut manipuler le surcroît de charge pour le chiffrement. Afin d'établir des clés SNMPv3 en mode de préconfiguration SNMP, le dispositif PS DOIT utiliser la gestion de clé SNMPv3 cerbérisée comme spécifié dans le § 11.4.4.2.1.

11.4.4.2.1 Protocole SNMPv3 cerbérisé

Le profil de gestion de clé cerbérisée propre au protocole SNMPv3 DOIT être suivi comme défini dans le § 6.5.4/J.170.

11.4.4.2.2 Algorithmes de chiffrement SNMPv3

Les identificateurs de transformation du chiffrement pour la gestion de clé SNMPv3 cerbérisée DOIVENT être suivis comme défini dans le § 6.3.1/J.170.

11.4.4.2.3 Algorithmes d'authentification SNMPv3

Les algorithmes d'authentification pour la gestion de clé SNMPv3 cerbérisée DOIVENT être suivis comme défini dans le § 6.3.2/J.170.

11.4.4.2.4 Identificateurs d'automate SNMPv3

Etant donné que le gestionnaire et le client du protocole SNMP DOIVENT vérifier que les identificateurs d'automate SNMPv3 contenus dans les messages de demande et de réponse AP sont fondés sur le nom de mandant de système NMS approprié qui est indiqué dans le ticket [Rec. UIT-T J.170], les règles suivantes sont utilisées afin de produire les identificateurs d'automate SNMPv3:

Règle 1: l'identificateur d'automate SNMPv3 DOIT suivre le format défini dans le document [RFC 3411], c'est-à-dire que le premier bit est réglé à 1 (un) et que la valeur appropriée est utilisée pour les quatre premiers octets [RFC 3411];

Règle 2: le cinquième octet DOIT être la valeur 4 (quatre) afin d'indiquer que les octets suivants, jusqu'à 27, sont à considérer comme du texte et sont définis comme suit:

- les caractères du nom de mandant de système NMS DOIVENT être utilisés pour les octets d'identificateur d'automate à partir du 6^{e} octet;
- la séquence d'octets indiquant le nom de mandant de système NMS DOIT être suivie par un octet unique et est considérée comme une valeur hexadécimale de 8 bits. Chaque valeur unique identifie un automate SNMP particulier dans le dispositif (élément ou serveur de système NMS). La valeur 0 (zéro) NE DOIT PAS être utilisée;
- la chaîne de texte qui commence au 6^{e} octet DOIT se terminer par un caractère vide.

NOTE – D'autres formats sont possibles en suivant l'approche du document [RFC 3411]. Le choix ci-dessus, cependant, est destiné à réduire la complexité d'implémentation qui serait requise si toutes les approches du document [RFC 3411] étaient permises.

11.4.4.2.5 Remplissage de la table usmUserTable

Les réglages de sécurité SNMPv3 pour le câblo-opérateur "CHAdministrator" en tant qu'utilisateur sont définis dans le § 6.3.3.1.4.5, "Exigences relatives au modèle de contrôle d'accès fondé sur le point de vue (VACM)". L'administrateur CHAdministrator est l'autorité ultime pour la gestion de l'élément de services de portail. D'autres utilisateurs peuvent également être définis. Dans le présent paragraphe, un utilisateur du modèle USM est défini précisément pour le processus de préconfiguration. En particulier, il est défini de façon à permettre de spécifier un récepteur de notification pour les messages cabhPsDevProvEnrollTrap et cabhPsDevInitTrap que le dispositif PS est tenu d'envoyer pendant le processus de préconfiguration (voir le Tableau 13-1, "Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration DHCP", étape CHPSWMD-11; le Tableau 13-3, "Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration SNMP", étape CHPSWMS-11 et étape CHPSWMS-13; ainsi que le § 13.4.3, "Messages INFORM d'enrôlement de préconfiguration/de préconfiguration terminée)".

Les paramètres msgSecurityParameters contenus dans les messages SNMPv3 transportent un champ msgUserName qui spécifie l'utilisateur au compte duquel le message est actuellement échangé et dont les informations de sécurité produisent les champs msgAuthenticationParameters et msgPrivacyParameters. Pour que l'automate SNMP d'un élément IPCable2Home traite ces messages, les informations nécessaires sont appelées à être introduites dans la table usmUserTable [RFC 3414] pour l'automate de l'élément.

La table usmUserTable DOIT être remplie avec les informations suivantes dans l'élément de services de portail juste après que le message de réponse AP a été reçu:

- usmUserEngineID: l'identificateur d'automate SNMP local comme défini dans le § 11.4.4.2.4, Identificateurs d'automate SNMPv3

- usmUserName: CHAdministratorxx:xx:xx:xx:xx:xx, où xx:xx:xx:xx:xx:xx est l'adresse matérielle de réseau WAN-Man du dispositif
- usmUserSecurityName: CHAdministratorxx:xx:xx:xx:xx:xx, où xx:xx:xx:xx:xx:xx est l'adresse matérielle de réseau WAN-Man du dispositif
- usmUserCloneFrom: 0.0
- usmUserAuthProtocol: indique le protocole d'authentification choisi pour l'utilisateur, à partir du message de réponse AP
- usmUserAuthKeyChange: valeur par défaut ""
- usmUserOwnAuthKeyChange: valeur par défaut ""
- usmUserPrivProtocol: indique le protocole de chiffrement choisi pour l'utilisateur, à partir du message de réponse AP
- usmUserPrivKeyChange: valeur par défaut ""
- usmUserOwnPrivKeyChange: valeur par défaut ""
- usmUserPublic: valeur par défaut ""
- usmUserStorageType: permanent
- usmUserStatus: active

De nouveaux utilisateurs SNMPv3 PEUVENT être créés par clonage avec la norme SNMPv3, comme défini dans [RFC 3414].

La table de sécurité du modèle VACM selon le groupe [RFC 3415] DOIT être remplie avec les informations suivantes dans le dispositif PS juste après réception du message de réponse AP:

- vacmSecurityModel: 3(usm)
- vacmSecurityName: CHAdministratorxx:xx:xx:xx:xx:xx
- vacmGroupName: CHAdministratorSNMP
- vacmSecurityToGroupStatus: active

La table d'accès au modèle VACM [RFC 3415] DOIT être remplie avec les informations suivantes, associées à la table vacmSecurityToGroupTable définie ci-dessus, dans le dispositif PS juste après la réception du message de réponse AP:

- vacmAccessContentPrefix: ""
- vacmAccessSecurityModel: 3(usm)
- vacmAccessSecurityLevel: AuthNoPriv
- vacmAccessContextMatch: exact(1)
- vacmAccessReadViewName: CHAdministratorView
- vacmAccessWriteViewName: CHAdministratorView
- vacmAccessNotifyViewName: CHAdministratorNotifyView
- vacmAccessStorageType: permanent
- vacmAccessStatus: active

Sept rangées de l'arbre de vues du modèle VACM [RFC 3415] DOIVENT être remplies avec les informations suivantes dans le dispositif PS juste après la réception du message de réponse AP:

- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: cabhPsDevProvEnrollTrap
- vacmViewTreeFamilyType: inclus
- vacmViewTreeFamilyMask: ""

- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: cabhPsDevBase
- vacmViewTreeFamilyType: inclus
- vacmViewTreeFamilyMask: ""
- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: docsDevSoftware
- vacmViewTreeFamilyType: inclus
- vacmViewTreeFamilyMask: ""
- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: cabhPsDevInitTrap
- vacmViewTreeFamilyType: inclus
- vacmViewTreeFamily Mask: ""
- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: cabhPsDevBase
- vacmViewTreeFamilyType: inclus
- vacmViewTreeFamily Mask: ""
- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: docsDevEventTable
- vacmViewTreeFamilyType: inclus
- vacmViewTreeFamily Mask: ""
- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: cabhPsDevProv
- vacmViewTreeFamilyType: inclus
- vacmViewTreeFamily Mask: ""

11.5 Qualité CQoS dans le dispositif PS

La qualité CQoS est un pont transparent de qualité de service entre le modèle IPCablecom et les liaisons de réseau local à réseau local. Les messages de qualité DQoS du modèle IPCablecom entre l'adaptateur MTA et le système CMTS, le serveur CMS ou le modem CM sont sécurisés par la spécification de sécurité IPCablecom. Il n'est pas prévu dans le domaine d'application du modèle IPCable2Home d'augmenter la sécurité des messages IPCablecom. La messagerie de qualité de service des liaisons de réseau local à réseau local dans le modèle IPCable2Home domestique n'est pas sécurisée car le risque d'attaques à domicile est considéré comme extrêmement faible. Etant donné qu'il n'y a aucune exigence de sécurité pour que l'élément de services de portail sécurise les messages CQoS issus du côté réseau régional, il n'y a aucune dépendance vis-à-vis des serveurs administratifs pour assurer cette fonction.

11.6 Pare-feu dans le dispositif PS

Depuis des dizaines d'années, les questions de sécurité constituent un problème majeur pour les compagnies fondées sur des réseaux. Il y a maintenant une prise de conscience croissante des problèmes de sécurité et de confidentialité pour les utilisateurs domestiques dont le câblo-modem est constamment sous tension. Etant donné que l'abonné moyen peut manquer de certaines connaissances techniques ou, même si ce n'est pas le cas, peut manquer de temps pour garder ses ordinateurs personnels dans le créneau supérieur du fonctionnement sécurisé, un pare-feu est

devenu une première ligne de défense nécessaire pour protéger les ordinateurs et autres dispositifs IP de réseau local qui en ont besoin au domicile.

11.6.1 Objectifs et hypothèses de pare-feu IPCable2Home

Objectifs

- Offrir au câblo-opérateur une configuration normalisée et interopérable pour le pare-feu.
- Offrir au câblo-opérateur un ensemble minimal de fonctionnalités requises pour le pare-feu.
- Permettre de surveiller les événements de pare-feu au moyen du mécanisme de messagerie de signalisation des événements.
- Protéger le réseau domestique et les dispositifs IP de réseau local de ce réseau contre le trafic indésirable de réseau régional à réseau local.
- Protéger l'hybride HFC contre le trafic indésirable de réseau local à réseau régional.
- Protéger le dispositif PS contre les attaques et le trafic considérés comme indésirables par le câblo-opérateur.
- Garantir que le pare-feu va traiter les paquets à des débits suffisants pour que le filtrage de paquets n'introduise pas un étranglement de la performance, sans tenir compte de la complexité ou de la taille de l'ensemble de règles.
- Garantir la prise en charge d'applications identifiées par le pare-feu pour des scénarios spécifiés.
- Offrir au câblo-opérateur la capacité de surveiller et de changer les règles utilisées par le pare-feu.
- Garantir que les configurations de sécurité appropriées (par exemple règles et politiques de filtrage) existent dans le système de pare-feu.
- Identifier les types d'attaques que le pare-feu va journaliser et spécifier le journal de telle sorte que l'opérateur puisse voir ce journal selon les besoins.
- Prendre en charge le modèle IPCablecom par le pare-feu.
- Signaler en temps réel à l'administrateur d'importants événements définis.
- Offrir un ensemble de règles par défaut du constructeur afin d'assurer de façon cohérente des réinitialisations complètes du pare-feu.

Hypothèses

- Le pare-feu traite tous les paquets à destination ou en provenance du réseau local conformément à la politique actuelle sans tenir compte du mode d'adressage: par conversion CAT ou par transfert (par exemple le mode d'adressage n'a aucun effet sur les opérations du pare-feu).
- Le pare-feu commence à fonctionner immédiatement après le message de préconfiguration terminée, sans tenir compte du mode de préconfiguration.
- Le protocole SNMP, en particulier la messagerie SNMP dirigée vers le portail de gestion IPCable2Home (portail CMP), peut servir à configurer les ensembles de règles du pare-feu IPCable2Home. Ainsi, l'ensemble de règles est représenté, extérieurement, comme une collection d'objets de base MIB.
- Des objets de base MIB commandent les actions de journalisation effectuées par le pare-feu.
- Le pare-feu appliquera les règles et politiques de filtrage conjointement avec la vérification des adresses converties qui sont connues de la fonction CAT dans le dispositif PS.

11.6.2 Pare-feu: directives de conception du système

Les directives de conception du système de pare-feu énumérées dans le Tableau 11-17 ont guidé les spécifications de pare-feu IPCable2Home.

Tableau 11-17/J.192 – Sécurité IPCable2Home: directives de conception du système

Référence	Directives de conception du système de sécurité
SEC4	Le pare-feu acceptera les fichiers de configuration dans un langage et un format normalisés. (Note)
SEC5	Le câblo-opérateur possédera la capacité de gérer à distance les produits conformes de pare-feu par fichier de configuration ou par commandes SNMP.
SEC6	Le pare-feu conforme comportera un ensemble par défaut de règles pour un ensemble minimal prévu de fonctionnalités.
SEC7	Ce niveau offre la prise en charge nécessaire du modèle IPCablecom par le pare-feu.
SEC8	Un ensemble minimal d'exigences sera imposé aux capacités de filtrage du pare-feu en termes de paquets, de ports, d'adresses IP, de serveur ToD, etc.
SEC9	Une interface de journalisation détaillée des événements de pare-feu permettra au câblo-opérateur de surveiller et de réexaminer l'activité de pare-feu comme configurée.
SEC10	Le pare-feu prendra en charge les applications d'usage courant dans des scénarios spécifiques.
SEC11	Le pare-feu protégera les réseaux locaux et régionaux à l'encontre d'attaques courantes dans le réseau.
SEC12	La gestion des événements et les ensembles de règles pour le pare-feu seront définis en détail par la base MIB de sécurité.
NOTE – Les exigences relatives au fichier de configuration du pare-feu sont définies dans le § 7.4, "Fonction de services de portail – Configuration globale des services de portail (BPSC)".	

11.6.3 Pare-feu: description du système

En principe, les pare-feu sont construits au moyen d'une combinaison des composants suivants: filtrage de paquets (PF, *packet filter*), filtrage de paquets d'après l'état (SPF, *stateful packet filtering*), passerelle de couche Application (ALG, *application layer gateway*) et serveur mandataire propre à l'application (ASP, *application specific proxy*). Un module de filtrage de paquets est probablement le composant de pare-feu le plus commun parce qu'il détermine quels flux de paquets sont bloqués et quels flux sont autorisés à franchir le pare-feu. Chaque décision concernant un paquet individuel est fondée sur des informations de configuration statique (l'ensemble de règles) configurées dans les mécanismes de filtrage du pare-feu (politique) de façon que le paquet soit autorisé ou refusé, sur la base de l'inspection des champs d'en-tête de paquet: adresses IP d'origine et de destination, numéros de port d'origine et de destination du protocole, type de protocole, etc. Selon le niveau de sécurité recherché, un grand nombre de filtres peuvent avoir besoin d'être configurés dans un pare-feu. Le câblo-opérateur aura besoin de mettre en balance la complexité de l'ensemble de règles et les besoins des clients. La présente Recommandation essaye de spécifier un ensemble abondant de filtres de configuration, gérés par les objets de base MIB, de façon que les divers types de services (protocoles et applications) puissent être individuellement configurés, si nécessaire.

Un module de filtrage de paquets d'après l'état (SPF) fait appel à des informations d'état cumulées à partir de paquets qui appartiennent à la même connexion lors de la prise de décisions d'abandon de paquet. Le module SPF différencie entre différents protocoles et manipule correctement chaque

connexion de protocole. Le module SPF mémorise et utilise des informations trouvées dans les en-têtes de couche Réseau et de couche Transport du paquet.

Une passerelle de couche Application (ALG) est un composant qui connaît la façon d'extraire les informations requises pour suivre la connexion à partir de la couche Application du paquet. Comme certains protocoles incorporent des informations de commande de connexion dans la couche Application, le filtre SPF incorporera des passerelles ALG afin d'exécuter le suivi de la connexion. La passerelle ALG spécifique (par exemple FTP-ALG, IPSec-ALG) est requise pour le traitement de chacun des protocoles requis afin de prendre en charge le modèle IPCable2Home. Par exemple, le protocole FTP en mode actif comprend le numéro de port du protocole TCP qui sera utilisé ultérieurement pour le transfert de données. Donc, il est tenu d'utiliser une passerelle de type FTP-ALG à suivre l'état de toutes les connexions FTP. Voir l'Annexe D pour de plus amples informations sur les exigences relatives aux passerelles ALG.

Un pare-feu mandataire propre à l'application (ASP) filtre, sur la base du protocole de couche Application, des caractéristiques uniques ou des messages spécifiquement réservés à des protocoles de type client/serveur. L'utilisation de mandataires ASP peut apporter des avantages en terme de sécurité. Tout d'abord, il est possible d'ajouter des listes de contrôle d'accès à des protocoles exigeant que des utilisateurs ou des systèmes offrent un certain niveau d'authentification avant que l'accès soit accordé. Non seulement propre à chaque protocole, un mandataire ASP comprend le protocole et peut être configuré de façon à bloquer seulement des sous-sections du protocole. Le mandataire ASP permet le fonctionnement d'applications incompatibles avec la conversion NAT quand le service de portail doit fonctionner dans un de ses deux modes d'acheminement transparent: C-NAT ou C-NAPT. Par exemple, un mandataire ASP du protocole FTP peut être configuré de façon à bloquer le trafic à partir d'utilisateurs non authentifiés, tout en accordant aux utilisateurs authentifiés un accès sélectif aux commandes "put" (mettre) et "get" (obtenir), selon le sens d'émission de ces commandes.

La combinaison particulière, dans un produit de pare-feu donné, de filtres de paquet, de passerelles SPF ALG et de mandataires ASP, constitue un compromis entre performance et niveau de sécurité. En principe, étant un mécanisme de couche Réseau, les filtres de paquets tendent à donner une meilleure performance que les passerelles ALG/mandataires ASP, qui sont des mécanismes de couche Application. Une solution de compromis de plus en plus courante consiste à utiliser le filtrage des paquets d'après l'état (SPF), où les informations d'état cumulées à partir de paquets qui appartiennent à la même connexion sont conservées et utilisées dans la prise de décision d'abandon de paquet.

Aussi bien les modules SPF que les mandataires ASP comportent un filtrage conforme à la politique de sécurité afin d'obtenir le niveau de sécurité recherché pour un site. Cependant, alors que la politique de sécurité détermine les services autorisés et la façon dont ils sont utilisés de part et d'autre du pare-feu, la politique de sécurité n'explicite pas la configuration spécifique de ce pare-feu. L'ensemble de règles est exprimé sous forme lisible à l'œil, puis est interprété par le pare-feu et mise en œuvre dans la politique de filtrage selon le langage interne du pare-feu. Les filtres inspectent chaque paquet et déterminent ceux que le pare-feu réexpédie et ceux qu'il rejette.

La Figure 11-3 ci-dessous est un diagramme de haut niveau du pare-feu avec les rôles des divers composants de pare-feu cités en référence par la présente Recommandation.

NOTE – Ce diagramme n'indique aucune architecture ou implémentation technique spécifique. Il s'agit seulement d'une référence logique.

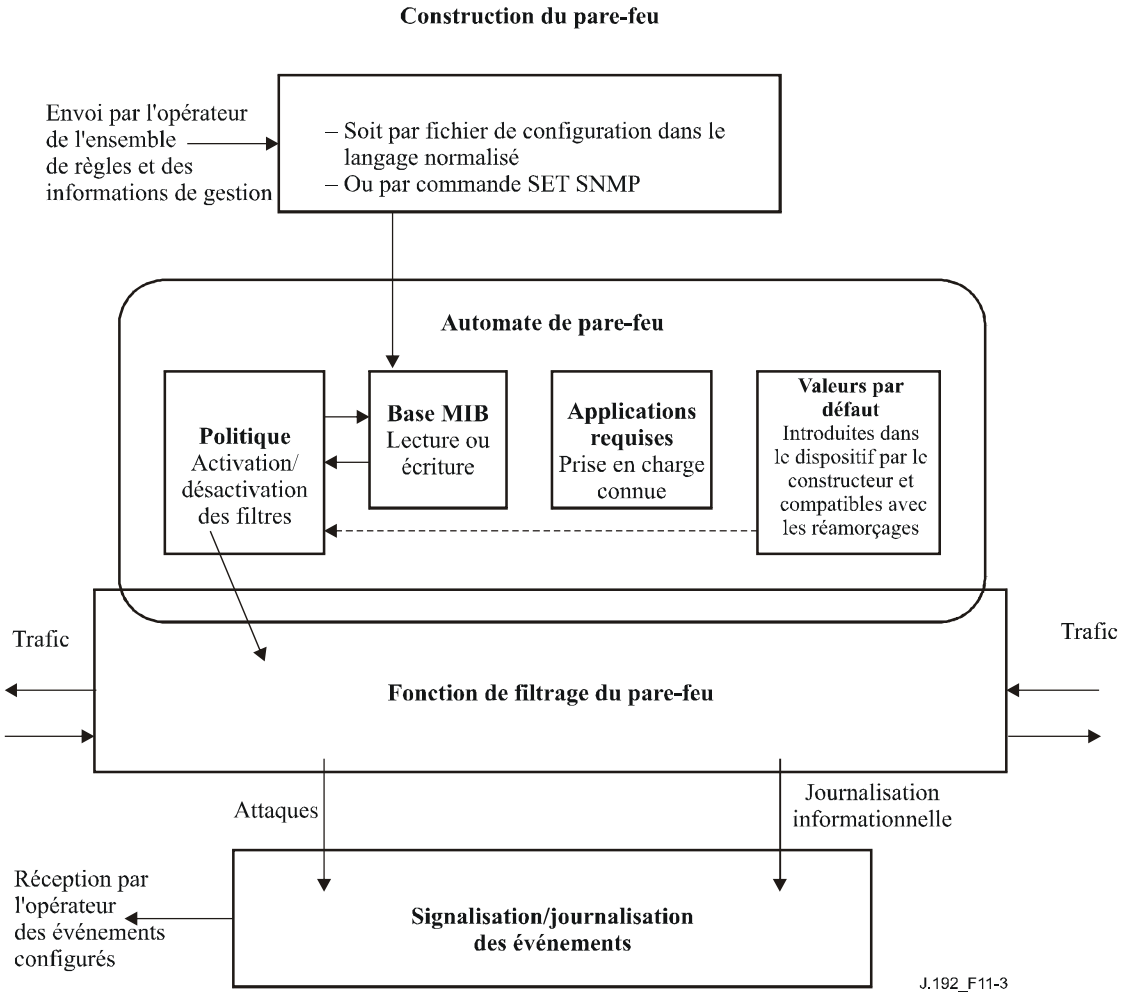


Figure 11-3/J.192 – Référence logique de pare-feu

11.6.4 Pare-feu: exigences

11.6.4.1 Langage du fichier de configuration pour le pare-feu

Un ensemble de règles choisies par le câblo-opérateur peut être configuré dans le pare-feu par un fichier de configuration du dispositif PS ou par téléchargement du fichier de configuration du pare-feu. Dans le présent paragraphe, le terme *fichier de configuration* désigne soit le fichier de configuration du dispositif PS ou le fichier de configuration du pare-feu. Le langage et le format du fichier de configuration contenant l'ensemble de règles applicable à un produit particulier de pare-feu sont définis, .

Le dispositif PS DOIT être capable de recevoir et d'interpréter un fichier de configuration du pare-feu construit au moyen d'éléments TLV formatés comme décrit dans le § 7.4.4.1: "Format du fichier de configuration: exigences". A l'intérieur du pare-feu, le compilateur convertit le langage de politique en format interne, propre au vendeur. Le nuplet TLV de type 28 DOIT servir à tous les objets de base MIB de pare-feu. Le langage du fichier de configuration du dispositif PS et du fichier de configuration du pare-feu est le même. Les exigences relatives au traitement du fichier de configuration du pare-feu sont définies dans le § 7.

11.6.4.2 Configuration du pare-feu

Le dispositif PS prend en charge – mais l'opérateur n'est pas tenu d'utiliser – la gestion à distance des fonctions de pare-feu. Le pare-feu contenu dans le dispositif PS DOIT accepter les ensembles de règles configurés en bloc au moyen des fichiers spécifiés de configuration du dispositif PS ou du

pare-feu, ainsi que les ensembles de règles configurés individuellement au moyen de commandes SET du protocole SNMP. Le dispositif PS NE DOIT PAS activer le pare-feu lors que la valeur de l'objet cabhPsDevProvState est égale à inProgress(2). Quand un fichier de configuration est utilisé afin de configurer des ensembles de règles après achèvement du téléchargement et du traitement du fichier de configuration, c'est-à-dire lorsqu cabhPsDevProvState = pass(1), les règles de pare-feu extraites de ce fichier de configuration DOIVENT être immédiatement appliquées et disponibles pour utilisation dans le dispositif PS sans réamorçage de celui-ci.

Si le dispositif PS ne peut pas traiter le fichier de configuration pour une raison ou une autre, c'est-à-dire si cabhPsDevProvState = fail(3), le dispositif PS DOIT utiliser les règles existantes de la table de filtrage du pare-feu qui sont indiquées par l'objet cabhSec2FwPolicySelection.

11.6.4.3 Politique de pare-feu et ensembles de règles

La politique de pare-feu commande au pare-feu de filtrer le trafic sur la base de règles particulières. La politique accepte les ensembles de règles à appliquer par la fonction de filtrage car celle-ci, qui n'est qu'un ensemble de capacités, n'a aucune signification par elle-même. Les capacités de filtrage par pare-feu, combinées avec la politique de pare-feu, offrent une protection par pare-feu pour le réseau local. Les filtres du pare-feu examinent activement chaque paquet ou chaque connexion en fonction de la politique afin d'appliquer les deux actions autorisées: permettre ou refuser.

Le modèle IPCable2Home définit trois composants comme informations d'entrée dans la politique de pare-feu, selon la configuration:

- les règles générales de comportement – qui sont les règles de comportement attendues pour autoriser ou refuser des flux de trafic. Ces règles s'appliquent toujours à moins qu'il n'y ait une exception écrite dans l'ensemble de règles IPCable2Home fixées par défaut à l'usine ou dans l'ensemble de règles configuré;
- l'ensemble de règles IPCable2Home fixées par défaut à l'usine – contenant les règles par défaut de filtrage par le pare-feu fixées à l'usine et utilisées en tant qu'exceptions aux règles générales de comportement. Ces règles peuvent également être utilisées conjointement avec l'ensemble de règles configuré;
- l'ensemble de règles configurées – contenant les règles configurées qui sont utilisées comme exceptions aux règles générales de comportement. Ces règles peuvent également être utilisées conjointement avec l'ensemble de règles IPCable2Home fixées par défaut à l'usine.

Les règles générales de comportement, l'ensemble de règles IPCable2Home fixées par défaut à l'usine et l'ensemble de règles configurées s'appliquent au trafic d'ouverture de session et non au trafic de réponse.

Le dispositif PS peut recevoir du trafic pour l'adaptateur MTA du modèle IPCablecom. Donc, il convient d'examiner rapidement la prise en charge requise pour l'adaptateur MTA. La prise en charge du modèle IPCablecom, décrite dans le § 11.6.4.4, comporte l'ensemble de règles par défaut fixées à l'usine plus les protocoles requis afin d'activer la messagerie IPCablecom à travers le pare-feu. L'Annexe D indique également quels ports doivent être ouverts pour l'adaptateur MTA. La prise en charge du modèle IPCablecom permet la préconfiguration, la gestion et les services à travers le pare-feu.

11.6.4.3.1 Politique de pare-feu et secteurs d'adresses

Le concept de secteurs d'adressage IP est défini dans la présente Recommandation pour les adresses IP de réseau régional et de réseau local. Bien que le dispositif PS soit considéré comme faisant partie du réseau local, les paquets en provenance ou à destination du dispositif PS ne sont pas désignés par le terme de *trafic de réseau local* aux fins du filtrage par pare-feu. En revanche, c'est l'adresse IP spécifique du dispositif PS qui est recherchée. Les paquets en provenance ou à destination du dispositif PS sont indiqués par l'utilisation de l'adresse IP du réseau WAN-Man, par

l'adresse IP du routeur-serveur PS ou par l'adresse IP fixe 192.168.0.1 (qui peut être ou ne pas être la même que l'adresse IP de l'interface PS/routeur-serveur). En conséquence, le pare-feu va distinguer le trafic à destination et en provenance du dispositif PS, dans l'ensemble de règles fixées par défaut à l'usine et dans l'ensemble de règles configurées. Le comportement du pare-feu est indépendant des secteurs d'adressage définis dans le § 5.1.3. Les règles de pare-feu ne sont pas affectées par le mode de traitement primaire des paquets ni par le mode d'adresses de réseau régional.

11.6.4.3.2 Comportement général du pare-feu

Le pare-feu contenu dans le dispositif PS est tenu de filtrer le trafic sur la base des règles générales de comportement spécifiées. Ces règles sont spécifiées afin d'offrir un niveau de référence du comportement de filtrage par le pare-feu dans le dispositif PS. Le comportement général s'applique, à moins qu'une exception ne soit définie dans l'ensemble de règles par défaut ou de règles configurées. Les états définis pour les règles générales de comportement sont de permettre ou de refuser le trafic. Avec les règles générales de comportement installées, le câblo-opérateur peut s'attendre que le dispositif PS se comportera toujours de façon normalisée en ce qui concerne le trafic de filtrage. Le dispositif PS DOIT appliquer à un paquet les règles générales de comportement lors du filtrage par le pare-feu comme spécifié dans le Tableau 11-18 ci-dessous sur les règles de comportement général du pare-feu, à moins que le pare-feu ne soit configuré de façon à utiliser une autre règle écrite dans l'ensemble de règles fixées par défaut à l'usine (cabhSec2FwFactoryDefaultFilterTable, [voir le § E.5]) ou dans l'ensemble de règles configurées (docsDevFilterIPTable).

Le pare-feu effectue le filtrage du côté réseau local au moyen de filtres de paquets du côté réseau local (LPF, *LAN side packet filter*) et du côté réseau régional au moyen de filtres de paquets du côté réseau régional (WPF, *WAN side packet filter*). Le comportement par défaut est spécifié en termes de filtres LPF et WPF. Voir au § 11.6.4.6.1 une description détaillée de l'architecture du pare-feu.

Tableau 11-18/J.192 – Règles de comportement général du pare-feu

Dispositif source	Adresse IP de destination	Règles de comportement général, WPF	Règles de comportement général, LPF
Tout dispositif de réseau régional	Adresse IP d'interface PS WAN-Man	Refuser tous trafics	N/A
	Adresse IP d'interface PS WAN-Data	Refuser tous trafics	N/A
	Toute adresse IP de réseau local (mode de transfert)	Refuser tous trafics	Autoriser tous trafics
Adresse IP d'interface PS WAN-Man OU PS WAN-Data	Toute adresse IP de réseau régional	Autoriser tous trafics	N/A
	Toute adresse IP de réseau local	N/A	Refuser tous trafics
Adresse IP d'interface PS/routeur-serveur OU 192.168.0.1	Toute adresse IP de réseau régional	Refuser tous trafics	N/A
	Toute adresse IP de réseau local	N/A	Autoriser tous trafics

Tableau 11-18/J.192 – Règles de comportement général du pare-feu

Dispositif source	Adresse IP de destination	Règles de comportement général, WPF	Règles de comportement général, LPF
Tout dispositif de réseau local	Adresse IP d'interface PS/routeur-serveur ou 192.168.0.1	N/A	Autoriser tous trafics
	Adresse IP d'interface PS WAN-Man ou PS WAN-Data	N/A	Refuser tous trafics
	Toute adresse IP de réseau régional	Autoriser tous trafics	Autoriser tous trafics
N/A: non applicable. L'instance de trafic ne traverse pas l'interface.			

11.6.4.3.3 Ensemble de règles fixées par défaut à l'usine

L'ensemble de règles fixées par défaut à l'usine définit un ensemble de règles de filtrage à appliquer quand l'option d'ensemble de règles par défaut de l'objet cabhSec2FwPolicySelection est sélectionnée. L'ensemble de règles IPCable2Home fixées par défaut à l'usine DOIT être codé physiquement dans le dispositif PS au moment de la fabrication. Le dispositif PS DOIT utiliser l'ensemble de règles IPCable2Home fixées par défaut à l'usine quand l'objet cabhSec2FwPolicySelection est réglé à la valeur factoryDefault(1) ou factoryDefaultAndConfiguredRuleset(3). Le Tableau 11-19 spécifie l'ensemble de règles fixées par défaut à l'usine. Les deux secteurs d'adresses (LAN-Trans et LAN-Pass) sont traités de la même façon pour l'ensemble de règles fixées par défaut à l'usine et sont étiquetés en tant qu'adresses IP de réseau local. Le pare-feu DOIT être en mesure de rechercher des adresses dans la table de mappage des conversions CAT afin d'appliquer une politique fondée sur l'adresse IP réelle du dispositif de serveur local. Ce Tableau fonde ses informations sur l'ouverture de session, et non pas sur le trafic autorisé. L'ensemble de règles fixées par défaut à l'usine du pare-feu DOIT donc être implémenté pour l'ouverture de session et non pas pour le trafic renvoyé en réponse à une session autorisée. Le trafic renvoyé sur requête de l'initiateur est interprété comme contenant des informations d'état pour une session et le pare-feu va vérifier l'état de la session après vérification des politiques afin de garantir qu'un paquet n'est pas refusé alors qu'il fait partie d'une session ouverte.

Tableau 11-19/J.192 – Politique de pare-feu IPCable2Home par défaut fixée à l'usine

Dispositif source	Adresse IP de destination	Règles de comportement général, WPF	Règles de comportement général, LPF	Liste des protocoles de filtrage en cas d'exception (numéro de règle)
Tout dispositif IP de réseau régional	Adresse IP d'interface PS WAN-Man	Refuser tous trafics	N/A	Autoriser ICMP (1) Autoriser SNMP (2,3)
	Adresse IP d'interface PS WAN-Data	Refuser tous trafics	N/A	Autoriser ICMP (15)
	Adresse IP d'interface PS/routeur-serveur ou 192.168.0.1	Refuser tous trafics	N/A	Néant
	Toute adresse IP de réseau local (mode de transfert)	Refuser tous trafics	Autoriser tous trafics	Autoriser ICMP (4)

Tableau 11-19/J.192 – Politique de pare-feu IPCable2Home par défaut fixée à l'usine

Dispositif source	Adresse IP de destination	Règles de comportement général, WPF	Règles de comportement général, LPF	Liste des protocoles de filtrage en cas d'exception (numéro de règle)
Adresse IP d'interface PS WAN-Man ou PS WAN-Data	Toute adresse IP de réseau régional	Autoriser tous trafics	N/A	Néant
	Toute adresse IP de réseau local	N/A	Refuser tous trafics	Autoriser ICMP (5,16)
Adresse IP d'interface PS/routeur-serveur ou 192.168.0.1	Toute adresse IP de réseau régional	Refuser tous trafics	N/A	Néant
	Toute adresse IP de réseau local	N/A	Autoriser tous trafics	Néant
Tout dispositif de réseau local	Adresse IP d'interface PS/routeur-serveur ou 192.168.0.1	N/A	Autoriser tous trafics	Néant
	Adresse IP d'interface PS WAN-Man ou WAN-Data	N/A	Refuser tous trafics	Autoriser ICMP (6,17)
	Toute adresse IP de réseau régional	Autoriser tous trafics	Autoriser tous trafics	Refuser Syslog (13,14)

L'ensemble de règles fixées par défaut à l'usine pour le pare-feu IPCable2Home, énuméré dans le Tableau 11-20, DOIT être implémenté dans l'objet de base MIB cabhSec2FwFactoryDefaultFilterTable. Les en-têtes de colonne correspondent aux objets de base MIB définis dans la base MIB de sécurité IPCable2Home mais comme les noms d'objet sont plutôt longs, seule la partie variable du nom d'objet est utilisée dans le tableau ci-dessous. Les règles qui incluent l'adresse IP de l'interface PS WAN-Data sont énumérées à partir de l'indice de Tableau 15, car le câblo-opérateur peut, s'il le souhaite, préconfigurer une ou plusieurs adresses IP du réseau WAN-Data dans le dispositif PS. Ce tableau sera correctement rempli lorsque le dispositif PS effectuera une préconfiguration selon la façon dont le câblo-opérateur aura configuré les adresses IP.

Tableau 11-20/J.192 – Règles de pare-feu fixées par défaut à l'usine

Index de tableau	Com-mande	IfIndex	sens	Saddr	Smask	Daddr	Dmask	Protocole	SourcePortLow	SourcePortHigh	DestPortLow	DestPortHigh	Continue
1	Autoriser	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Man	(255.255.255.255)	1	0	65535	0	65535	true
2	Autoriser	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Man	(255.255.255.255)	6	0	65535	161	161	true
3	Autoriser	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Man	(255.255.255.255)	17	0	65535	161	161	true
4	Autoriser	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	LAN IP (0.0.0.0)	(0.0.0.0)	1	0	65535	0	65535	true
5	Autoriser	255	2	PS WAN-Man	(255.255.255.255)	LAN IP (0.0.0.0)	(0.0.0.0)	1	0	65535	0	65535	true
6	Autoriser	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Man	(255.255.255.255)	1	0	65535	0	65535	true
7	Refuser	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	6	0	65535	88	88	true
8	Refuser	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	17	0	65535	88	88	true
9	Refuser	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	6	0	65535	749	749	true
10	Refuser	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	17	0	65535	749	749	true
11	Refuser	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	6	0	65535	1293	1293	true
12	Refuser	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	17	0	65535	1293	1293	true
13	Refuser	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	6	0	65535	514	514	true
14	Refuser	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	17	0	65535	514	514	true
15	Autoriser	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Data	(255.255.255.255)	1	0	65535	0	65535	true
16	Autoriser	255	2	PS WAN-Data	(255.255.255.255)	LAN IP (0.0.0.0)	(0.0.0.0)	1	0	65535	0	65535	true
17 §	Autoriser	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Data	(255.255.255.255)	1	0	65535	0	65535	true

Le câblo-opérateur peut configurer le dispositif PS avec tout ensemble de règles de pare-feu au moyen d'un fichier de configuration ou d'une commande SET du protocole SNMP. Quand un câblo-opérateur envoie des règles au dispositif PS, ces règles sont désignées par le terme d'ensemble de règles configurées. Le dispositif PS DOIT mémoriser les règles configurées dans la table docsDevFilterIpTable [RFC 2669] et mémoriser toutes les informations de planification, concernant d'éventuelles règles particulières, dans les objets de base MIB définis par IPCable2Home dans la table cabhSec2FwFiltreScheduleTable (voir le § E.5). L'ensemble des règles configurées n'est actif pour le filtrage par le pare-feu que si celui-ci est activé et que la sélection de politique est réglée à la valeur configuredRuleset(2) ou factoryDefaultAndConfiguredRuleset(3). L'ensemble de règles configurées peut être supprimé de la table docsDevFilterIpTable par réglage de la valeur de l'objet cabhSec2FwClearPreviousRuleset à true(1).

11.6.4.3.4 Ensemble de règles configurées

La politique de filtrage par le pare-feu IPCable2Home peut être configurée par création de règles de filtrage dans la table docsDevFilterIpTable et/ou cabhSec2FwLocalFilterIpTable (voir § 11.6.4.9.3). Ces règles de filtrage sont considérées comme étant l'ensemble de règles configurées. Les règles de filtrage définies dans l'ensemble de règles configurées sont utilisées comme exceptions aux règles générales de comportement. L'ensemble des règles configurées peut également être utilisé conjointement avec l'ensemble des règles fixées par défaut à l'usine. Quand cela est effectué, les règles de filtrage définies dans l'ensemble de règles configurées sont utilisées comme exceptions, à la fois aux règles générales de comportement et à l'ensemble de règles fixées par défaut à l'usine.

Les deux tables docsDevFilterIpTable et cabhSec2FwLocalFilterIpTable ont des capacités similaires de configuration des règles de filtrage. L'existence de ces deux tables de filtrage facilite la gestion de l'ensemble de règles configurées. Par exemple, la table docsDevFilterIpTable peut servir à définir des règles génériques de filtrage qui s'appliquent à de multiples dispositifs et la table cabhSec2FwLocalFilterIpTable peut servir à définir des règles de filtrage locales ou propres au client qui s'appliquent seulement à ces dispositifs. L'opérateur peut également permettre aux clients de configurer leur propres règles de filtrage dans la table cabhSec2FwLocalFilterIpTable.

L'objet de base MIB cabhSec2FwPolicySelection permet à l'opérateur de sélectionner quel(s) ensemble(s) de règles de filtrage est ou sont actifs (voir § 11.6.4.9.1). Si les tables docsDevFilterIpTable et cabhSec2FwLocalFilterIpTable sont simultanément actives, il est possible qu'une règle de filtrage conflictuelle puisse exister dans chaque table. Par exemple, une certaine règle de filtrage indique une action d'autorisation alors que l'autre indique une action de refus pour le même paquet trouvé concordant. Pour la résolution des conflits entre ces deux tables, l'objet de base MIB cabhSec2FwPolicyConfiguredRulesetPriority sert à déterminer la règle de filtrage prioritaire. Concernant les conflits entre règles de filtrage qui peuvent exister entre l'ensemble de règles configurées, l'ensemble de règles fixées par défaut à l'usine et les règles générales de comportement, le dispositif PS DOIT toujours donner priorité à l'ensemble de règles configurées.

Quand une entrée de règle de filtrage de pare-feu est créée dans la table docsDevFilterIpTable ou dans la table cabhSec2FwLocalFilterIpTable et s'applique à une unique adresse IP de réseau local qui est dynamiquement assignée par le dispositif PS (serveur CDS), le dispositif PS DOIT créer une réservation de location pour cette adresse IP. Cela garantit que l'adresse IP du dispositif de réseau local qui est appliquée par l'entrée de règle de filtrage de pare-feu ne changera pas lors d'un renouvellement de location. Une entrée de règle de filtrage de pare-feu qui s'applique à une unique adresse IP d'origine ou de destination possède la valeur de masque de sous-réseau réglée à 255.255.255.255.

Le dispositif PS DOIT déterminer si l'unique adresse IP d'origine et/ou de destination de l'entrée de règle de filtrage de pare-feu est dynamiquement assignée par le serveur CDS, p. ex. en la recherchant dans la table cabhCdpLanAddrTable. Si une entrée correspondante existe dans cette table avec la valeur de l'objet cabhCdpLanAddrMethod égale à soit dynamicActive(4) ou dynamicInactive(3), alors le dispositif PS DOIT remplacer cette entrée par une autre qui représente une réservation de location pour cette adresse IP dans la table, c'est-à-dire par une entrée où la valeur de l'objet cabhCdpLanAddrMethod est réglé soit à la valeur psReservationActive(6) ou à la valeur psReservationInactive(5), selon le cas. Si une entrée correspondante n'existe pas dans la table cabhCdpLanAddrTable, alors le dispositif PS NE DOIT PAS créer de réservation de location pour cette adresse IP. Dans ce cas, il est possible que l'adresse IP soit statiquement assignée au dispositif IP de réseau local.

Quand une entrée de règle de filtrage de pare-feu est supprimée de la table docsDevFilterIpTable ou de la table cabhSec2FwLocalFilterIpTable qui s'applique à une unique adresse IP de réseau local dynamiquement assignée par le dispositif PS (CDS), le dispositif PS DOIT supprimer la réservation correspondante de location d'adresse IIP qui a été créée en interne (identifiée par

cabhCdpLanAddrMethod=psReservationActive(6)) de la table cabhCdpLanAddrTable tant qu'il n'y a pas d'entrée de zone DMZ correspondante dans la table cabhCapMappingTable qui l'exige.

11.6.4.4.4 Prise en charge du modèle IPCablecom

Si le câblo-opérateur déploie le modèle IPCablecom, le pare-feu peut avoir besoin de communiquer le trafic à destination et en provenance de l'adaptateur MTA, selon la configuration du réseau et du dispositif. S'ils exploitent un réseau IPCablecom, les protocoles définis par la série des Recommandations relatives au modèle IPCablecom NE DOIVENT PAS être interrompus par le pare-feu. Le câblo-opérateur peut avoir besoin de configurer le pare-feu avec d'éventuelles règles additionnelles afin de garantir que le modèle IPCablecom sera activé par le pare-feu. Le Tableau 11-21 ci-après est une liste de spécifications qui exigent un port unique concernant la communication avec l'adaptateur MTA. Cependant, il ne s'agit pas d'une liste détaillée de toutes les spécifications IPCablecom.

Tableau 11-21/J.192 – Spécifications IPCablecom 1.x applicables au pare-feu IPCable2Home

Description	Spécification
Spécification des codecs audio/vidéo	[Rec. UIT-T J.161]
Spécification de la qualité de service dynamique	[Rec. UIT-T J.163]
Spécification du protocole de signalisation d'appel fourni par le réseau	[Rec. UIT-T J.162]
Spécification de la préconfiguration d'adaptateur MTA	[Rec. UIT-T J.167]
Spécification de sécurité	[Rec. UIT-T J.170]
Spécification du mécanisme d'événement de gestion	[Rec. UIT-T J.164]
Spécification du protocole de serveur audio	[Rec. UIT-T J.175]
Spécification de la signalisation du serveur distant de gestion d'appel	[Rec. UIT-T J.178]

La liste des protocoles IPCablecom requis par l'adaptateur MTA a été extraite des spécifications indiquées. Les numéros de port attribués par l'autorité IANA afin d'ouvrir les ports requis par les protocoles IPCablecom spécifiés par le pare-feu sont énumérés dans l'Annexe D, "Applications par conversion CAT et pare-feu". Les protocoles définis par le modèleIPCablecom sont les suivants:

- préconfiguration: SNMPv3, DHCP, DNS, TFTP, SYSLOG
- flux média: RTP, RTCP
- qualité de service: RSVP
- sécurité: Kerberos, IPSec
- signalisation d'appel réseau: MGCP, SDP

NOTE – Le protocole SDP n'exige aucun port spécifique.

{texte informatif:

11.6.4.5 Prise en charge du service de zone DMZ et du service UPnP de connexion IP par réseau régional

Les mappages de portail CAP concernant la zone DMZ et la connexion IP de réseau régional UPnP (UWIC) permettent au trafic non sollicité qui est issu d'un réseau régional de traverser la fonction de portail CAP du dispositif PS (par conversion NAPT). Afin de prendre cela en charge, le dispositif PS a besoin de créer des règles de filtrage de pare-feu qui correspondent aux entrées DMZ et UWIC dans la table de mappage du portail CAP et qui permettent à ce trafic de passer.

Quand une application de réseau local conforme au modèle UPnP configure un mappage de port dans la table cabhCapMappingTable, l'objet de base MIB cabhCapMappingMethod a une valeur égale à UPnP(3) (voir § 8.3.4.9). Pour chaque entrée dans la table cabhCapMappingTable avec une

valeur d'objet de base MIB cabhCapMappingMethod égale à UPnP(3), le dispositif PS DOIT créer une règle de filtrage de pare-feu correspondante qui permet au trafic non sollicité de passer du réseau régional au réseau local. Quand une entrée dans la table cabhCapMappingTable avec une valeur d'objet de base MIB cabhCapMappingMethod égale à UPnP(3) est supprimée, le dispositif PS DOIT supprimer la règle correspondante de filtrage de pare-feu.

Une entrée de zone DMZ dans la table cabhCapMappingTable a les valeurs de port de réseau régional et de port de réseau local réglées à zéro (voir § 8.3.3.2). Pour chaque entrée de zone DMZ dans la table cabhCapMappingTable, le dispositif PS DOIT créer une règle correspondante de filtrage de pare-feu qui permet au trafic non sollicité de passer du réseau régional au réseau local. Quand une entrée de zone DMZ dans la table cabhCapMappingTable est supprimée, le dispositif PS DOIT supprimer la règle correspondante de filtrage de pare-feu.

}

11.6.4.6 Filtrage par pare-feu

Le présent paragraphe spécifie les exigences relatives au composant de filtrage de paquets par le pare-feu. Le filtre de paquets spécifié examine les paquets individuels et détermine s'il y a lieu de permettre ou de refuser leur passage dans le pare-feu. Plus précisément, le filtre de paquets inspecte les champs d'en-tête de paquet et rend des décisions paquet par paquet sur la base du contenu de ces champs et de l'ensemble de règles configurées.

11.6.4.6.1 Ensemble minimal de capacités de filtrage

Dans le cadre du modèle IPCable2Home, une simple conversion NAT ou un simple filtre de paquets n'est pas suffisant. Afin d'offrir une solution flexible et sûre, le pare-feu DOIT implémenter un mandataire propre à l'application (ASP) ou un filtrage de paquets d'après l'état (SPF). De plus, des exigences spécifiques pour ces techniques de filtrage sont nécessaires afin d'offrir un niveau suffisant de produits essayables, fiables et interopérables pour l'industrie du câble. Le composant ASP/SPF du pare-feu commande le flux de trafic associé aux protocoles de couche Application qui ne peuvent pas être régis effectivement et en transparence par un filtrage statique. Les mécanismes de filtrage examineront les applications qui sont dynamiquement établies lors de sessions en protocole IP, TCP, UDP, ou ICMP. L'activité relative aux ports, aux adresses IP et à la planification est gérée comme étant associée à une "session" dans le pare-feu. Egalement, le mandataire propre à l'application permet le fonctionnement d'applications incompatibles avec la conversion NAT quand le service de portail doit fonctionner dans un de ses deux modes d'acheminement transparent: C-NAT ou C-NAPT.

Sans tenir compte du type de pare-feu qui est implémenté, le dispositif PS pare-feu DOIT être compatible avec la session et capable de suivre des informations sur une paire d'adresses IP (origine et destination) en conjonction avec la politique actuelle pour l'adresse IP spécifiée. Une session consiste en un appariement d'adresses IP à la demande. Cette demande comprend la mise en correspondance de la requête avec la politique autorisée pour cette session, qui comporte l'adresse IP, le port de l'application et ses limitations de trafic.

L'architecture de filtrage des paquets dans le pare-feu spécifie des filtres de paquets distincts du côté régional et du côté local du dispositif PS. Le filtre de paquets du côté réseau régional examine, à l'interface avec le réseau régional les paquets qui proviennent du domaine régional, du domaine local, ou des composants internes du dispositif PS. Le filtre de paquets du côté réseau local examine, aux interfaces avec le côté résultant d'un réseau local, les paquets qui proviennent du domaine local, du domaine régional, ou des composants internes du dispositif PS. Des règles distinctes peuvent être appliquées aux filtres de paquets du côté régional et du côté local.

Les composants du dispositif PS sont localisés en fonction du pare-feu comme représenté dans la Figure 11-4. Les paquets reçus par le dispositif PS en provenance du domaine régional ou du domaine local sont filtrés dans le pare-feu avant qu'ils atteignent l'un quelconque des composants du

dispositif PS autres que le pare-feu (portails CDP, CNP, CSP, CQP, CMP et CAP à l'exception de la commutation USFS). De la même façon, les paquets à transmettre par le dispositif PS vers le domaine régional ou vers le domaine local traverseront des composants autres que le pare-feu avant d'atteindre les filtres WPF ou LPF.

Les filtres WPF et LPF agissent également sur les paquets issus des composants internes du dispositif PS. Ces paquets sont filtrés par les filtres WPF et LPF avant d'être réexpédiés, respectivement, vers le domaine régional ou vers le domaine local.

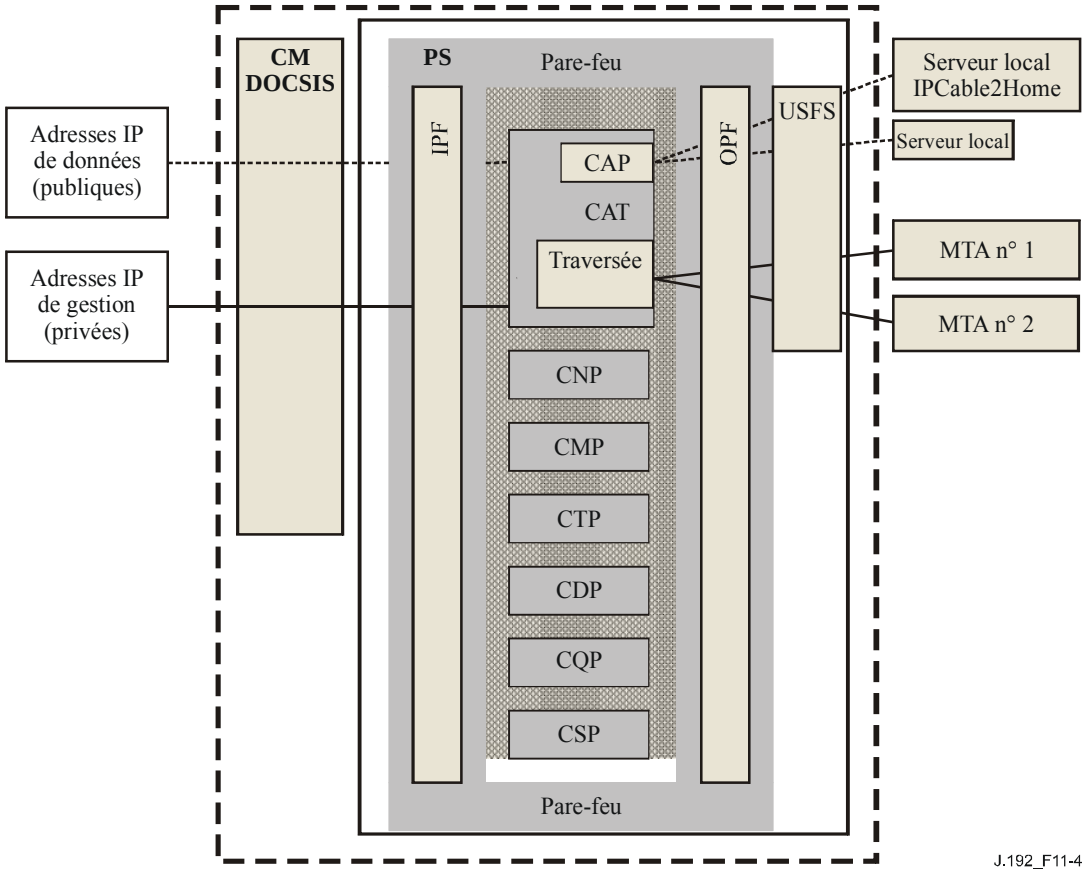


Figure 11-4/J.192 – Fonctionnalité de pare-feu à l'intérieur du dispositif PS

Les définitions de filtrage suivantes sont utilisées:

- AUTORISER signifie "laisser passer le paquet";
- REFUSER signifie "abandonner le paquet".

Les filtres WPF et LPF du pare-feu DOIVENT manifester le comportement suivant:

- le pare-feu DOIT filtrer le trafic sur la base de la politique définie par le modèle IPCable2Home comme indiqué dans le § 11.6.4.3: "Ensemble de règles fixées par défaut à l'usine", lorsqu'il n'existe pas de règle explicite à suivre afin de vérifier un paquet;
- le pare-feu DOIT refuser les paquets réexécutés à partir du réseau local ou WAN;
- le pare-feu DOIT créer un "état" pour tous les paquets autorisés ouvrant une session. Soit un paquet sera accepté parce qu'il y a une règle statique afin de permettre les paquets possédant ces critères, soit il y aura un état impliquant qu'un paquet sera autorisé par suite d'une session dont l'ouverture a été autorisée;

- le pare-feu NE DEVRAIT PAS autoriser de trafic TCP sortant avant d'avoir établi une session en protocole TCP (c'est-à-dire avant d'avoir effectué un dialogue TCP à trois correspondants);
- les paquets ayant une seule des options IP ci-après: lSRR (route à origine et à journalisation indéterminées), SSRR (route à origine et journalisation déterminées), RR (routage de journalisation) DOIVENT être refusés.

Il y a de nombreux types d'attaques dans le réseau que le pare-feu peut filtrer. De nombreuses méthodes et de nombreux utilitaires servent à attaquer divers dispositifs dans un réseau. La liste est très longue et change plus rapidement que tout document actuellement publié ne peut s'en prévaloir. La présente Recommandation signale, pour étude de sécurité générale, certaines des attaques les plus connues. Le pare-feu DEVRAIT protéger contre l'exploration des ports ou du réseau local lancée à partir d'un réseau local ou WAN. Le pare-feu DEVRAIT protéger contre les déversements de paquets et contre les paquets mal formés. Le pare-feu DEVRAIT protéger contre la liste ci-dessous d'attaques par refus de service: "Ping of Death", "Teardrop", "Bonk", "Nestea", "SYN Flood", "LAND Attack", "IP Spoofing", "Smurf Attack", "WinNuke" et contre toute messagerie à haute fréquence émise par des dispositifs IP de réseau local, comme les messages BP_Init ou DISCOVER du protocole DHCP.

11.6.4.6.2 Critères de filtrage

Le comportement par défaut est de refuser le trafic lancé à partir d'adresses IP de réseau régional, de l'adresse IP de l'interface PS WAN-Man, ou de l'adresse IP de l'interface PS/routeur-serveur. Les ensembles de règles sont donc construits de façon à permettre un trafic particulier pour ces adresses. Le comportement par défaut est de permettre un trafic à partir des adresses IP de réseau local sauf réglage de refus explicite. Donc, les ensembles de règles sont construits de façon à refuser tout trafic particulier vers ces adresses. Le présent paragraphe ne spécifie pas toutes les capacités de filtrage prévues, mais énumère un ensemble minimal de critères qui est développé par les objets de base MIB spécifiés. Les filtres de paquets entrants et de paquets sortants DOIVENT examiner le trafic afin de déterminer si une règle autorisera ce trafic sur la base des critères de filtrages suivants:

- adresse IP d'origine;
- adresse IP de destination;
- protocole IP ("de prochain niveau"); par exemple TCP, UDP, ICMP, IPSec AH, IPSec ESP;
- ports d'origine et de destination en protocole TCP ou UDP;
- informations de début de connexion pour paquets TCP (c'est-à-dire absence de bit ACK) pour suivi de session;
- suivi de numéro séquentiel pour les sessions.

Les données de paquet ci-dessus sont utilisées comme critères pour la mise en correspondance des paquets entrants avec une règle spécifique et donc pour l'obtention d'une décision de filtrage spécifique (autoriser/refuser). Le pare-feu DOIT vérifier l'adresse IP d'origine et de destination afin de déterminer si une règle quelconque s'applique à cette adresse. Si l'ensemble de règles interdit actuellement le trafic de réexpédition à destination ou à partir d'une adresse IP, le pare-feu DOIT refuser le paquet, à moins qu'il n'y ait lieu de le transmettre en raison de son état.

NOTE – Le filtrage en fonction de la politique actuelle comprend d'autres exigences relatives au filtrage qui doivent être appliquées mais qui ne sont pas considérées comme faisant partie des critères de filtrages intégrés.

11.6.4.6.3 Architecture de filtrage

Le filtre de paquets du pare-feu sera en mesure de filtrer le trafic en assurant un filtrage distinct pour le trafic issu du réseau régional, du réseau local ou du dispositif PS. Ce pare-feu DOIT:

- filtrer, à l'interface WAN, les paquets qui proviennent d'un côté ou de l'autre de cette interface. Les règles de filtrage du côté réseau régional du dispositif PS sont identifiées par la valeur d'indice d'interface 1 (un) et s'appliquent à tout trafic à destination et en provenance du réseau régional;
- filtrer, à l'interface avec le côté résultant des interfaces avec un réseau local, valeur d'indice ifIndex 255, les paquets qui proviennent d'un côté ou de l'autre de cette interface;
- filtrer les paquets provenant de l'intérieur du dispositif PS et allant vers le réseau local ou vers le réseau régional;
- n'appliquer les filtres que s'ils sont actuellement activés;
- appliquer le filtrage de paquets avant l'exécution de tout traitement par mandataire ASP ou par filtre SPF;
- appliquer le filtrage aux paquets que le dispositif PS reçoit avant de transmettre de tels paquets à l'un quelconque des autres composants du dispositif PS que le pare-feu. Cependant, comme celui-ci n'est pas tenu d'être en mesure de filtrer le trafic de réseau local à réseau local, le trafic issu du côté réseau local et reçu par le dispositif PS rencontre la fonction de commutation USFS avant de rencontrer le filtre LPF.

Le filtre WPF DOIT manifester le comportement général suivant:

- filtrer comme défini au § 11.6.4.3;
- refuser tous les paquets qui entrent dans le dispositif PS à partir du réseau régional et qui ont des adresses d'origine qui appartiennent aux secteurs d'adresse de réseau LAN-Pass ou LAN-Trans;
- refuser tous les paquets ayant des adresses d'origine diffusées ou multidiffusées.

Le filtre LPF DOIT manifester le comportement général suivant:

- filtrer comme défini au § 11.6.4.3;
- rejeter tous les paquets ayant des adresses d'origine diffusées ou multidiffusées.

11.6.4.7 Signalisation des événements de pare-feu

Les informations provenant du pare-feu sont critiques pour la gestion et la surveillance périodiques, ainsi que pour la fourniture des événements appropriés concernant des attaques spécifiées. Les événements produits par le pare-feu peuvent servir à la détection d'intrusion, pour les attaques par refus de service (DoS, *denial of service*) et pour les éventuels dérangements ou journaux associés au système de pare-feu. L'analyse des journaux peut être tout à fait malaisée s'il y a de grandes quantités de données à trier. Egalement, si de trop nombreux événements sont envoyés au câblo-opérateur, ces événements pourraient resserrer la largeur de bande, car il peut y avoir de nombreux pare-feu envoyant des événements au système NMS situé dans les bureaux administratifs du câblo-opérateur. Celui-ci aura besoin de déterminer les éléments qu'il souhaite activer afin de surveiller le pare-feu et la fréquence à laquelle il voudrait recevoir les événements. L'activation de la signalisation des événements est distincte de l'activation de l'ensemble des règles applicables aux critères de filtrage par pare-feu. Quand les objets MIB d'activation d'événement de pare-feu ont été réglés de façon à activer le pare-feu de façon à suivre des types d'événement définis, le pare-feu va journaliser et envoyer les messages événementiels spécifiés comme défini dans le présent paragraphe et dans l'Annexe B.

Chacun des événements spécifiés peut être activé ou désactivé par le câblo-opérateur en réglant un objet de base MIB du protocole SNMP par un fichier de configuration ou par une requête SET (mise à jour) du protocole SNMP. Il est recommandé que le protocole SNMPv3 soit utilisé afin de sécuriser les messages SNMP contenant des informations de pare-feu.

11.6.4.7.1 Evénements de pare-feu

Les événements de pare-feu permettent à un câblo-opérateur d'évaluer à distance le niveau d'activité de piratage et les modifications apportées au pare-feu d'après des éléments de services de portail spécifiques. La production d'événements est fondée: sur les modifications de gestion apportées à l'ensemble de règles, sur les événements détectés par le pare-feu tel qu'activé par l'ensemble de règles, ou sur les événements de protocole TFTP/HTTP fondés sur un téléchargement. Les événements de protocole TFTP/HTTP fondés sur un téléchargement de pare-feu DOIVENT être envoyés comme défini par l'Annexe B.

Le pare-feu DOIT être capable de journaliser les types d'événement suivants:

TYPE 1: le type 1 DOIT journaliser toutes les tentatives de traverser le pare-feu, issues des deux clients LAN et WAN, qui violent la politique de sécurité quand ce type est activé par l'objet cabhSec2FwEventEnable de base MIB. Ce type journalise toutes les tentatives de connexion qui sont abandonnées en raison d'une violation de politique. Une attaque est définie comme étant des paquets (c'est-à-dire que chaque paquet est compté comme une attaque) qui essayent de traverser le pare-feu et qui violent la politique actuelle. Si ce type est activé et si le seuil est atteint, le dispositif PS DOIT immédiatement envoyer l'événement 80010201;

TYPE 2: le type 2 DOIT journaliser les tentatives d'attaque par refus de service identifiées, quand ce type est activé, par l'objet cabhSec2FwEventEnable de base MIB. Une attaque de type 2 est définie comme toute tentative qui est considérée comme interrompant un service, comme le déversement de paquets dupliqués (c'est-à-dire que 10 paquets sont comptés comme une seule tentative), ou comme le déversement de paquets mal formés, ou comme des tentatives prohibées de connexion de partir du même serveur local pendant un certain nombre de fois. Si ce type est activé et si le seuil est atteint, le dispositif PS DOIT immédiatement envoyer l'événement 80010202;

TYPE 3: le type 3 DOIT journaliser toutes les modifications aux objets de base MIB cabhSec2FwPolicyFileURL ou cabhSec2FwPolicyFileCurrentVersion ou cabhSec2FwEnable quand ce type est activé, apportées par l'objet cabhSec2FwEventEnable de base MIB. Le suivi des modifications apportées à la configuration de pare-feu offre au câblo-opérateur un utile retour d'informations aux fins du débogage. Si ce type est activé et si le seuil est atteint, le dispositif PS DOIT immédiatement envoyer l'événement 80010203;

TYPE 4: le type 4 DOIT journaliser toutes les tentatives infructueuses de modifier les objets de base MIB cabhSec2FwPolicyFileURL et cabhSec2FwEnable quand ce type est activé, effectuées par l'objet cabhSec2FwEventEnable de base MIB. Si ce type est activé et si le seuil est atteint, le dispositif PS DOIT immédiatement envoyer l'événement 80010204;

TYPE 5: le type 5 DOIT journaliser les paquets autorisés entrant à partir du réseau régional quand ce type est activé, par l'objet cabhSec2FwEventEnable de base MIB. Ce type permet au câblo-opérateur de surveiller le trafic dans un scénario où il y a des signes de détection d'intrusion ou d'attaques par refus de service (DOS) à partir du réseau régional. Si ce type est activé et si le seuil est atteint, le dispositif PS DOIT immédiatement envoyer l'événement 80010205;

TYPE 6: le type 6 DOIT journaliser les paquets autorisés sortant du réseau local quand ce type est activé, par l'objet cabhSec2FwEventEnable de base MIB. Ce type permet au câblo-opérateur de surveiller le trafic dans un scénario où il y a des signes d'attaques provenant d'un réseau local résidentiel en traversant le réseau régional. Si ce type est activé et si le seuil est atteint, le dispositif PS DOIT immédiatement envoyer l'événement 80010206.

Les types d'événement pour IPCable2Home ne sont définis qu'aux fins de la surveillance. C'est à chaque câblo-opérateur qu'il appartient d'évaluer et d'exécuter toute réponse nécessaire aux anomalies détectées et signalées par le pare-feu.

11.6.4.7.2 Journaux de pare-feu

Les informations de journalisation du pare-feu DOIVENT être enregistrées dans le dispositif PS pour chaque type de journal activé, comme spécifié dans le § 11.6.4.7.1. Pour chaque type d'événement activé, le dispositif PS DOIT journaliser les informations spécifiées dans la table cabhSec2FwLogTable chaque fois que le décompte d'événements atteint le seuil spécifié dans l'intervalle d'enregistrement. Le décompte d'événements, le seuil et l'intervalle sont définis pour chaque type d'événement dans la table cabhSec2FwEventCommandTable (cabhSec2FwEventCount, cabhSec2FwEventThreshold et cabhSec2FwEventInterval au § 11.6.4.9.2). Tout événement journalisé dans la table cabhSec2FwLogTable DOIT également être journalisé dans la table docsDevEventTable, à condition que les contraintes additionnelles de ralentissement d'admission soient observées pour la table docsDevEventTable spécifiée au § 6.3.3.2.4.8.

Si la table de journalisation est pleine, le dispositif PS DOIT supprimer la plus ancienne entrée et ajouter la nouvelle. Si la table cabhSec2FwEventThreshold n'est pas réglée à zéro, si la table cabhSec2FwEventEnable est activée et si la table cabhSec2FwEventInterval n'est pas réglée à zéro, le dispositif PS DOIT continuer à journaliser les événements du type activé. Une fois que l'objet cabhSec2FwEventLogReset est réglé à 1 afin de supprimer le journal et que l'objet cabhSec2FwEventEnable est activé, l'objet cabhSec2FwEventCount DOIT commencer à compter à partir de zéro.

Le dispositif PS, au minimum, DOIT prendre en charge la journalisation de 40 entrées dans la table de journalisation du pare-feu (cabhSec2FwLogTable). Si un type d'événement est activé, le dispositif PS DOIT journaliser les informations requises par le type d'événement au rythme minimal de 1 événement toutes les 5 secondes, même en situation d'attaque. On suppose que le dispositif PS ne va pas consommer la majorité de ses ressources de calcul en journalisation de sorte que, quand des attaques se produisent, le dispositif PS DEVRAIT être capable de communiquer le trafic à un débit normal et de fonctionner normalement par ailleurs.

La journalisation peut poser différents problèmes si elle n'est pas effectuée correctement. La journalisation de tous les événements et paquets peut rendre le journal complexe, long et difficile à comprendre. Il est difficile d'effectuer un tri parmi de nombreuses informations afin de rechercher un élément particulier. Si la journalisation est limitée à quelques types d'événements seulement, elle ne va pas offrir assez d'informations au câblo-opérateur pour qu'il puisse déboguer des intrusions ou détecter des attaques. Noter que les journaux peuvent être analysés s'ils ne sont pas chiffrés. Un pirate peut utiliser des informations de journalisation afin de prendre connaissance des divers services fonctionnant dans le dispositif PS ou dans les dispositifs du serveur local.

Le modèle IPCable2Home exige qu'un ensemble particulier d'informations soit journalisé pour chaque type d'événement qui est activé. La fonction de journalisation DOIT journaliser les paquets de chaque type conformément aux règles applicables à ce type d'événement. L'exigence relative à la date et à l'heure implique que la date et l'heure seront aussi précises que la dernière mise à jour de l'horloge du dispositif PS pendant la séquence de préconfiguration.

La table cabhSec2FwLogTable pour les types d'événement 1, 2, 5 et 6 DOIT enregistrer les informations suivantes pour chaque occurrence, sauf spécification contraire:

- numéro d'événement – DOIT être mémorisé comme défini dans l'Annexe B, une seule fois, au début du journal;
- priorité d'événement – DOIT être mémorisée comme défini dans l'Annexe B, une seule fois, au début du journal;
- date et heure – quand l'événement s'est produit:
  - DOIT consister des quatre chiffres de l'année, du mois et du jour;
  - DOIT consister de l'heure, de la minute et de la seconde;

- protocole – le protocole indiqué dans le champ d'en-tête IP (1 = ICMP; 2 = IGMP; 6 = TCP; 17 = UDP);
- adresse IP d'origine;
- adresse IP de destination;
- port d'origine (TCP et UDP);
- port de destination (TCP et UDP);
- type de message (ICMP) – Le document [RFC 2474] définit le protocole ICMP et, quand le pare-feu bloque un paquet ICMP, le journal DOIT afficher un nombre indiquant de quel type de message ICMP il s'agissait. 0 – Réponse d'écho, 3 – Destination inatteignable, 4 Extinction de l'origine, 5 – Réacheminement, 8 – demande d'écho, 9 – Signalement du routeur, 10 – Sollicitation du routeur, 11 – Dépassement d'heure, 12 – Problème de paramètre, 13 – Demande de marqueur temporel, 14 – Réponse à la demande de marqueur temporel, 15 – Demande d'informations, 16 – Réponse à la demande d'informations, 17 Demande de masque d'adresse, 18 – Réponse à la demande de masque d'adresse;
- comptage de réexécutions – si les données qui sont mémorisées constituent une attaque par réexécution, le pare-feu NE DEVRAIT PAS enregistrer chaque occurrence de l'attaque. Cependant, le pare-feu DEVRAIT enregistrer le nombre d'occurrences jusqu'à la valeur de seuil fixée pour le type spécifique;
- nom de la table de filtrage concordante (le cas échéant) – quand l'événement se produit en raison d'une concordance de paquet avec une entrée de table de règles de filtrage, le nom de cette table de filtrage (docsDevFilterIpTable, cabhSec2FwFactoryDefaultFilterTable, ou cabhSec2FwLocalFilterIpTable) DOIT être fourni;
- indice de la table de filtrage concordante (le cas échéant) – quand l'événement se produit en raison d'une concordance de paquet avec une entrée de table de règles de filtrage, l'indice de cette table de filtrage DOIT être fourni;
- description du filtre concordant (le cas échéant) – quand l'événement se produit en raison d'une concordance de paquet avec une entrée de table de règles de filtrage, la description du filtre DOIT être fournie.

La table cabhSec2FwLogTable pour le type d'événement 3 DOIT enregistrer les informations suivantes pour chaque occurrence sauf spécification contraire:

- le numéro d'événement DOIT être mémorisé comme défini dans l'Annexe B, une seule fois, au début du journal;
- la priorité d'événement DOIT être mémorisée comme défini dans l'Annexe B, une seule fois, au début du journal;
- la date et l'heure où l'événement s'est produit:
  - DOIVENT consister des quatre chiffres de l'année, du mois et du jour;
  - DOIVENT consister de l'heure, de la minute et de la seconde;
- l'adresse IP d'origine;
- l'objet de base MIB modifié.

La table cabhSec2FwLogTable pour le type d'événement 4 DOIT enregistrer les informations suivantes pour chaque occurrence sauf spécification contraire:

- le numéro d'événement DOIT être mémorisé comme défini dans l'Annexe B, une seule fois, au début du journal;
- priorité d'événement DOIT être mémorisé comme défini dans l'Annexe B, une seule fois, au début du journal;

- la date et l'heure où l'événement s'est produit:
  - DOIVENT consister des quatre chiffres de l'année, du mois et du jour;
  - DOIVENT consister de l'heure, de la minute et de la seconde;
- l'adresse IP d'origine;
- l'objet de base MIB dont la modification a été tentée.

11.6.4.8 Applications traversant le pare-feu

Dans le cadre de l'ensemble minimal de capacités, le pare-feu DOIT être capable de permettre à des applications spécifiées, comme définies par l'Annexe D, de traverser le dispositif PS afin d'atteindre leur destination prévue. Le pare-feu applique l'ensemble de règles actuel à la politique afin de garantir que les ouvertures correctes sont créées afin de prendre en charge le trafic spécifique entre les réseaux locaux et régionaux, ainsi qu'à destination et en provenance du dispositif PS lui-même. Le dispositif PS NE DOIT PAS limiter le nombre de sessions ou de connexions à prendre en charge simultanément, sauf spécification contraire dans l'Annexe D, Applications passant par la conversion CAT et le pare-feu.

La politique de pare-feu est appliquée au trafic lorsque celui-ci essaye de traverser le pare-feu. Les paquets sont d'abord traités dans le pare-feu puis sont envoyés au dispositif PS pour traitement complémentaire, ou sont envoyés à leur destination sur le réseau régional ou LAN. La politique est appliquée aux adresses IP d'origine et de destination, aux ports et à l'heure locale. L'Annexe D énumère les exigences et fournit de plus amples détails.

11.6.4.9 Objets de base MIB de pare-feu

Les objets de base MIB de pare-feu se composent de trois groupements généraux:

1) un ensemble servant à gérer la configuration de pare-feu;
2) un ensemble servant à surveiller et à journaliser les événements;
3) un ensemble servant à gérer les ensembles de règles eux-mêmes.

Les exigences relatives aux objets de base MIB de pare-feu DOIVENT être utilisées en conjonction avec le document sur la base MIB de sécurité [voir § E.5].

11.6.4.9.1 Objets de base MIB de gestion d'ensemble de règles de pare-feu

Les objets suivants de gestion du pare-feu DOIVENT être implémentés dans le dispositif PS:

cabhSec2FwPolicyFileURL – cet objet contient le nom du fichier de l'ensemble de règles de la politique et l'adresse IP du serveur TFTP ou HTTPS contenant le fichier de l'ensemble de règles de la politique, en format d'adresse URL du protocole TFTP ou HTTPS. Le téléchargement d'un fichier de l'ensemble de règles de la politique est déclenché quand la valeur servant à mettre à jour (SET) cette base MIB est différente de la valeur contenue dans l'objet cabhSec2FwPolicySuccessfulFileURL de base MIB. Voir § 7.4.4.2.3, "Déclencheur du fichier de configuration du pare-feu".

Si le téléchargement du fichier de configuration du pare-feu n'a pas réussi, le dispositif PS NE DOIT PAS mettre à jour l'objet cabhSec2FwPolicySuccessfulFileURL de base MIB avec la même valeur que l'objet cabhSec2FwPolicyFileURL de base MIB. En tout état de cause, l'objet cabhSec2FwPolicyFileURL de base MIB DOIT contenir la valeur mise à jour (SET) soit par le fichier de configuration du dispositif PS ou par une requête SET (mise à jour) du protocole SNMP. Quand le dispositif PS est réinitialisé, l'objet cabhSec2FwPolicyFileURL de base MIB DOIT être rempli avec sa valeur par défaut.

cabhSec2FwPolicySuccessfulFileURL – cet objet contient le nom du fichier de l'ensemble de règles de la politique et l'adresse IP du serveur TFTP qui contenait le fichier de l'ensemble de règles de la politique, en format d'URL du protocole TFTP ou HTTPS, qui a servi à déclencher le dernier

téléchargement réussi. Si un téléchargement réussi ne s'est pas encore produit, cette base MIB devrait avoir une valeur "néant".

cabhSec2FwPolicyFileHash – cet objet définit le condensé de codage SHA-1 pour le fichier de l'ensemble de règles correspondant.

cabhSec2FwPolicyFileOperStatus – cet objet contient l'état opérationnel du téléchargement du fichier de configuration du pare-feu et DOIT contenir les trois états suivants:

- inProgress(1) – indique qu'un téléchargement du fichier de configuration du pare-feu est en cours d'exécution;
- complete(2) – indique que le fichier de configuration du pare-feu a téléchargé avec succès;
- failed(3) – indique que la dernière tentative de téléchargement du fichier de configuration du pare-feu a échoué.

cabhSec2FwPolicyFileCurrentVersion – cet objet est une étiquette établie par le câblo-opérateur qui peut servir à suivre diverses versions des ensembles de règles configurées. Une fois l'étiquette réglée puis modifiée en même temps que les règles configurées, cette étiquette peut ne plus refléter précisément la version des règles configurées qui s'appliquent au dispositif. Cet objet DOIT contenir la chaîne "null" s'il n'a jamais été configuré.

cabhSec2FwEnable – cet objet permet l'activation et la désactivation du pare-feu. Si cet objet est réglé à "désactiver", le pare-feu DOIT être complètement désactivé. Si cet objet est réglé à "activer", le pare-feu DOIT être activé immédiatement, sans réamorçage du dispositif PS.

cabhSec2FwClearPreviousRuleset – cet objet permet à l'opérateur d'effacer les entrées de règle de filtrage dans la table docsDevFilterIpTable.

cabhSec2FwPolicySelection – Cet objet permet la sélection de la politique de filtrage comme défini par les options suivantes:

- factoryDefault (1) – indique que le pare-feu utilise les réglages fixés par défaut à l'usine qui sont définis au § 11.6.4.3.3. Si l'objet de base MIB cabhSec2FwPolicySelection est réglé à la valeur factoryDefault(1), alors le pare-feu filtre en fonction de l'ensemble de règles fixées par défaut à l'usine indiqué dans la table cabhSec2FwFactoryDefaultFilterTable.
- configuredRulesetBoth (2) – indique que le pare-feu utilise l'ensemble de règles configurées défini à la fois par la table docsDevFilterIpTable et par la table cabhSec2FwLocalFilterIpTable. Si l'objet de base MIB cabhSec2FwPolicySelection est réglé à la valeur configuredRulesetBoth(2),alors le pare-feu filtre en fonction des règles de filtrage définies à la fois par la table docsDevFilterIpTable et par la table cabhSec2FwLocalFilterIpTable.
- factoryDefaultAndConfiguredRulesetBoth (3) – indique que le pare-feu utilise l'ensemble de règles fixées par défaut à l'usine et l'ensemble de règles configurées défini à la fois par la table docsDevFilterIpTable et par la table cabhSec2FwLocalFilterIpTable. Si l'objet de base MIB cabhSec2FwPolicySelection est réglé à la valeur factoryDefaultAndConfiguredRulesetBoth (3), le dispositif PS DOIT filtrer en fonction de l'ensemble de règles fixées par défaut à l'usine spécifié par le modèle IPCable2Home dans la table cabhSec2FwFactoryDefaultFilterTable et en fonction des règles de filtrage définies à la fois par la table docsDevFilterIpTable et par la table cabhSec2FwLocalFilterIpTable.
- configuredRulesetDocsDevFilterIpTable (4) – indique que le pare-feu utilise l'ensemble de règles configurées défini par la table docsDevFilterIpTable. Si l'objet de base MIB cabhSec2FwPolicySelection est réglé à la valeur configuredRulesetDocsDevFilterIpTable (4), alors le pare-feu filtre en fonction de l'ensemble de règles configurées indiqué dans la table docsDevFilterIpTable.

- configuredRulesetCabhSec2FwLocalFilterIpTable (5) – indique que le pare-feu utilise l'ensemble de règles configurées défini par la table cabhSec2FwLocalFilterIpTable. Si l'objet de base MIB cabhSec2FwPolicySelection est réglé à la valeur configuredRulesetDocsDevFilterIpTable (5), alors le pare-feu filtre en fonction de l'ensemble de règles configurées indiqué dans la table cabhSec2FwLocalFilterIpTable.
- factoryDefaultAndConfiguredRulesetDocsDevFilterIpTable (6) – indique que le pare-feu utilise l'ensemble de règles fixées par défaut à l'usine et l'ensemble de règles configurées défini par la table docsDevFilterIpTable. Si l'objet de base MIB cabhSec2FwPolicySelection est réglé à la valeur factoryDefaultAndConfiguredRulesetDocsDevFilterIpTable (6), le dispositif PS DOIT filtrer en fonction de l'ensemble de règles fixées par défaut à l'usine spécifié par le modèle IPCable2Home dans la table cabhSec2FwFactoryDefaultFilterTable et en fonction de l'ensemble de règles configurées spécifié dans la table docsDevFilterIpTable.
- factoryDefaultAndConfiguredRulesetCabhSec2FwLocalFilterIpTable (7) – indique que le pare-feu utilise l'ensemble de règles fixées par défaut à l'usine et l'ensemble de règles configurées défini par la table cabhSec2FwLocalFilterIpTable. Si l'objet de base MIB cabhSec2FwPolicySelection est réglé à la valeur factoryDefaultAndConfiguredRulesetCabhSec2FwLocalFilterIpTable (7), le dispositif PS DOIT filtrer en fonction de l'ensemble de règles fixées par défaut à l'usine spécifié par le modèle IPCable2Home dans la table cabhSec2FwFactoryDefaultFilterTable et en fonction de l'ensemble de règles configurées spécifié dans la table cabhSec2FwLocalFilterIpTable.

cabhSec2FwEventSetToFactory – cet objet permet à l'opérateur de supprimer tous les événements actuellement inscrits dans la table d'événements. Le dispositif PS DOIT immédiatement supprimer l'objet cabhSec2FwEventControlTable si cet objet est réglé à "true".

cabhSec2FwEventLastSetToFactory – cet objet signale la dernière fois que la table d'événements a été réinitialisée.

cabhSec2FwConfiguredRulesetPriority – cet objet définit, dans l'ensemble de règles configurées, la règle de filtrage qui a priorité quand un conflit existe entre une règle de filtrage figurant dans la table docsDevFilterIpTable et une règle de filtrage figurant dans la table cabhSec2FwLocalFilterIpTable, comme indiqué par les options suivantes:

- docsDevFilterIpTable (1) – indique que les règles de filtrage figurant dans la table docsDevFilterIpTable ont priorité sur tous les filtres contradictoires qui peuvent exister dans la table cabhSec2FwLocalFilterIpTable;
- cabhSec2FwLocalFilterIpTable (2) – indique que les règles de filtrage figurant dans la table cabhSec2FwLocalFilterIpTable ont priorité sur tous les filtres contradictoires qui peuvent exister dans la table docsDevFilterIpTable.

cabhSec2FwClearLocalRuleset – cet objet permet à l'opérateur d'effacer les entrées de règle de filtrage dans la table cabhSec2FwLocalFilterIpTable.

11.6.4.9.2 Objets de base MIB pour événements de pare-feu

Les objets d'événement de pare-feu suivants DOIVENT être implémentés dans le dispositif PS, comme défini dans la base MIB de sécurité. Ils sont inclus dans l'objet cabhSec2FwEventControlTable:

cabhSec2FwEventType – cet objet attribue le type d'événement que la table doit suivre. Les types d'événement sont définis dans le § 11.6.4.7.1.

cabhSec2FwEventEnable – cet objet active ou désactive le comptage et la journalisation d'événements de pare-feu selon le type attribué dans l'objet cabhSec2FwEventType. Les exigences de journalisation sont définies dans le paragraphe concernant les données de journal (voir

§ 11.6.4.7.2). Cet objet n'est qu'un commutateur par tout ou rien. Si la valeur d'activation change, le dispositif PS DOIT immédiatement envoyer l'événement approprié (8001010x). Si cette valeur est activée, le pare-feu DOIT journaliser les occurrences dans l'objet cabhSec2FwLog. Le pare-feu NE DOIT PAS compter, envoyer des événements, ou collecter des données de journalisation afin de répondre à des attaques quand l'objet cabhSec2FwEventEnable est désactivé. Valeur par défaut = "False".

cabhSec2FwEventThreshold – cet objet indique le nombre d'attaques à compter avant d'envoyer l'événement approprié par type tel qu'attribué dans l'objet cabhSec2FwEventType. Si la valeur est réglée à zéro, le pare-feu NE DOIT PAS compter, envoyer des événements, ou collecter des données de journalisation pour ce type. Par défaut = 0.

cabhSec2FwEventInterval – cet objet indique l'intervalle temporel en heures afin de compter et de journaliser les occurrences d'un type d'événement de pare-feu tel qu'attribué dans l'objet cabhSec2FwEventType. Cet intervalle temporel s'applique aussi longtemps que l'objet cabhSec2FwEventThreshold n'est pas atteint. Si l'objet cabhSec2FwEventInterval de base MIB a une valeur égale à zéro, il n'y a aucun intervalle attribué et le dispositif PS NE DOIT PAS compter, envoyer, ou journaliser des événements. Par défaut = 0.

cabhSec2FwEventCount – cet objet indique le décompte actuel des attaques jusqu'à la valeur de l'objet cabhSec2FwEventThreshold par type tel qu'attribué par l'objet cabhSec2FwEventType. Le pare-feu DOIT commencer à compter les attaques à partir de zéro chaque fois que l'objet cabhSec2FwEventEnable de base MIB est activé, ou que l'objet cabhSec2FwEventInterval est terminé, ou que l'objet cabhSec2FwEventCount a une valeur égale à celle de l'objet cabhSec2FwEventThreshold. Si le nombre d'attaques comptées dans l'objet cabhSec2FwEventCount a une valeur égale au seuil fixé dans l'objet cabhSec2FwEventThreshold avant la fin de l'intervalle temporel défini par l'objet cabhSec2FwEventInterval, le dispositif PS DOIT immédiatement envoyer l'événement approprié (8001020x). Par défaut = 0.

cabhSec2FwEventLogReset – le réglage de cet objet à la valeur "true" réinitialise la table de journalisation pour le type spécifié d'événement. La lecture de cet objet renvoie toujours la valeur "false". Par défaut = "false".

cabhSec2FwEventLogLastReset – cet objet signale la dernière fois que le journal a été réinitialisé.

11.6.4.9.3 Objets de base MIB de politique de pare-feu

Les objets de base MIB de politique de pare-feu permettent au câblo-opérateur de configurer les règles qui seront utilisées par le pare-feu afin de filtrer le trafic. Le câblo-opérateur peut créer tout ensemble de règles configurées nécessaire pour filtrer le trafic traversant le pare-feu dans le dispositif PS. Les objets de base MIB d'ensemble de règles configurées pour la politique de filtrage par pare-feu sont fondés sur l'ensemble minimal d'exigences de filtrage. La capacité de filtrage du pare-feu est semblable aux filtres définis dans les objets de base MIB de câblo-modem de l'industrie du câble, spécifiés dans [RFC 2669]. Donc, le modèle IPCable2Home a adopté certains des objets de filtrage déjà définis dans [RFC 2669] et a ajouté dans la base MIB de sécurité certains objets de base MIB spécifiques du pare-feu.

Dans [RFC 2669], l'objet docsDevFilterIpTable offre les propriétés de filtrage de base. L'objet docsDevFilterIpTable contient une séquence d'objets de base MIB docsDevFilterIpEntry. Chaque rangée de cette table décrit les règles associées à des adresses IP qui sont ensuite comparées aux paquets IP traversant le pare-feu. Le gabarit comprend les adresses IP d'origine et de destination (et leurs masques associés), le protocole de niveau supérieur (par exemple TCP, UDP), ainsi que les étendues des ports d'origine et de destination. La table cabhSec2FwLocalFilterIpTable est similaire à la table docsDevFilterIpTable et peut également servir à définir les propriétés de filtrage. Les deux tables docsDevFilterIpTable et cabhSec2FwLocalFilterIp constituent le cœur de l'implémentation de la politique pour l'ensemble des règles configurées. C'est dans ces tables de base MIB que la politique de l'ensemble des règles configurées est définie et construite.

Le modèle IPCable2Home définit une extension de l'objet docsDevFilterIpTable, cabhSec2FwFilterScheduleTable, qui offre des attributs de filtrage pour l'instant de début, l'instant de fin et le jour de la semaine selon les entrées de filtrage contenues dans la table docsDevFilterIpTable. Ces attributs existent également dans la table cabhSec2FwLocalFilterIpTable et permettent d'appliquer une règle ou un filtre selon le jour de la semaine (dimanche, lundi, mardi, mercredi, jeudi, vendredi, ou samedi), entre un instant de début et un instant de fin. Par exemple, un parent peut demander que les communications soient refusées entre le réseau régional et l'ordinateur d'un enfant du lundi au vendredi, entre 21 h et 7 h ainsi que le samedi et le dimanche, entre 22 h et 8 h. La table cabhSec2FwFilterScheduleTable fournit également un attribut descriptif qui peut être utilisé pour placer des observations/remarques qui aident à déterminer à quelle fin l'entrée de filtre est utilisée. Les entrées de règle de filtrage dans la table docsDevFilterIpTable DOIVENT toujours être appliquées si leurs objets de base MIB cabhSec2FwFilterScheduleTables associés ont les valeurs suivantes:

- cabhSec2FwFilterScheduleStartTime = 0;
- cabhSec2FwFilterScheduleEndTime = 2359;
- cabhSec2FwFilterScheduleDOW = 0xFE.

Les entrées de règle de filtrage dans la table cabhSec2FwLocalFilterIpTable DOIVENT toujours être appliquées si leur objets de base MIB ont les valeurs suivantes:

- cabhSec2FwLocalFilterStartTime = 0;
- cabhSec2FwLocalFilterEndTime = 2359;
- cabhSec2FwLocalFilterDOW = 0xFE.

La combinaison de filtres définie dans [RFC 2669] et dans la base MIB de sécurité permet de créer des règles quelconques sur la base d'une combinaison quelconque d'adresse IP d'origine, d'adresse IP de destination, de port d'origine, de port de destination, d'heure locale et de jour de la semaine.

S'il n'y a pas de correspondance quand le dispositif PS est en train de comparer chaque paquet entrant ou sortant aux règles contenues dans les tables docsDevFilterIpTable, cabhSec2FwLocalFilterIpTable ou cabhSec2FwFactoryDefaultFilterTable, alors le dispositif PS DOIT appliquer les règles générales de comportement et l'ensemble minimal de capacités et d'architecture de pare-feu, comme défini dans les § 11.6.4.3.1 et 11.6.4.3.3. Le fanion docsDevFilterIpDefault défini dans [RFC 2669] DOIT être ignoré.

Les objets de base MIB suivants DOIVENT être implémentés à partir de [RFC 2669] afin de créer la version IPCable2Home de la table docsDevFilterIpTable. Sauf indication contraire dans ce paragraphe, la fonctionnalité est conforme à [RFC 2669]:

- docsDevFilterIpTable >>DocsDevFilterIpEntry
  - **docsDevFilterIpIndex**
    - conformément à [RFC 2669], le filtre ayant l'indice le moins élevé est toujours appliqué, c'est-à-dire que le filtre est vérifié; puis le dispositif PS DOIT continuer la vérification des filtres et appliquer le filtre d'indice le plus élevé en cas de conflits.
  - **docsDevFilterIpStatus**
  - **docsDevFilterIpControl**
    - Le dispositif PS DOIT ignorer le réglage (3) pour la politique; le modèle IPCable2Home n'utilise pas la table de politique.
  - **docsDevFilterIpIfIndex**
    - cet objet DOIT utiliser une valeur par défaut de 255 (côté résultant des interfaces avec le réseau local);

- le dispositif PS DOIT prendre en charge les valeurs 1 (un) pour les filtres du côté régional du dispositif PS et 255 (l'interface avec le côté résultant des interfaces avec le réseau local) pour les filtres du côté local du dispositif PS.

– **docsDevFilterIpDirection**
  - dans le modèle IPCable2Home, cette valeur représente le sens par rapport à l'indice docsDevFilterIpIfIndex dans la règle particulière considérée, c'est-à-dire que le dispositif PS DOIT représenter le sens du trafic (du réseau régional au réseau local, réciproquement ou dans les deux sens) par rapport à l'indice d'interface indiqué. Les valeurs d'indice d'interface attribuées par le vendeur DOIVENT suivre la même règle d'application du sens. Par exemple, le modèle IPCable2Home attribue le nombre 255 au côté résultant de l'interface avec le réseau local. Dans ce cas, le dispositif PS verra le trafic issu du réseau régional avec l'indice d'interface 255 comme tout le trafic issu du réseau local et allant vers le dispositif PS ou traversant celui-ci; et il verra le trafic issu du réseau local avec l'indice d'interface 255 comme tout le trafic allant vers le réseau local en provenance du dispositif PS ou traversant celui-ci.

– **docsDevFilterIpBroadcast**
  - On suppose que cet objet aura toujours la valeur par défaut "false". Donc, la règle s'appliquera à tout le trafic.

– **docsDevFilterIpSaddr**

– **docsDevFilterIpSmask**

– **docsDevFilterIpDaddr**

– **docsDevFilterIpDmask**

– **docsDevFilterIpProtocol**

– **docsDevFilterIpSourcePortLow**

– **docsDevFilterIpSourcePortHigh**

– **docsDevFilterIpDestPortLow**

– **docsDevFilterIpDestPortHigh**

– **docsDevFilterIpMatches**
  - Etant donné que des règles de filtrage sont appliquées au trafic d'ouverture de session, cet objet DOIT au minimum compter le nombre de fois que ce filtre est trouvé en concordance lorsqu'une ouverture de session est tentée.

– **docsDevFilterIpTos**
  - Cet objet peut être ignoré, sa fonction n'est pas requise.

– **docsDevFilterIpTosMask**
  - Cet objet peut être ignoré, sa fonction n'est pas requise.

– **docsDevFilterIpContinue**
  - Cet objet DOIT toujours être réglé à "true" de sorte que le dispositif PS continuera la vérification des filtres jusqu'à ce que tous les filtres aient été vérifiés. Contrairement au document RFC 2669, cet objet NE DOIT PAS déclencher de rejet avant que tous les filtres aient été vérifiés et qu'il n'y ait plus aucun autre filtre exigeant que le paquet soit accepté.

– **docsDevFilterIpPolicyId**
  - Cet objet peut être ignoré, sa fonction n'est pas requise.

De plus, le pare-feu DOIT prendre en charge les objets de base MIB suivants comme spécifié dans le document sur la base MIB de sécurité:

- **cabhSec2FwFilterScheduleStartTime**
- **cabhSec2FwFilterScheduleEndTime**
- **cabhSec2FwFilterScheduleDOW**
- **cabhSec2FwFilterScheduleDescr**
- **cabhSec2FwLocalFilterIpTable**

11.6.4.9.4 Objets de base MIB de l'ensemble de règles fixées par défaut à l'usine pour le pare-feu

Les objets de base MIB de l'ensemble de règles fixées par défaut à l'usine pour le pare-feu IPCable2Home permettent au câblo-opérateur de voir les règles IPCable2Home fixées par défaut à l'usine, qui sont des exceptions aux règles générales, ou au comportement général du pare-feu comme défini dans les Tableaux 11-18 et 11-19. Pour de plus amples informations sur les objets de base MIB de l'ensemble de règles par défaut utilisé pour le filtrage, voir dans la base MIB de sécurité la description de l'objet cabhSec2FwFactoryDefaultFilterTable et ses entrées.

11.7 Objets additionnels de base MIB de sécurité dans le dispositif PS

Les objets de base MIB de pare-feu sont décrits dans le paragraphe relatif au pare-feu (voir § 11.6). Le présent paragraphe décrit les autres objets de base MIB de sécurité requis. Les objets de base MIB de sécurité sont définis plus en détail et DOIVENT être pris en charge comme défini dans l'Annexe A.

11.7.1 Objets de base MIB de téléchargement sécurisé de logiciel

Le téléchargement sécurisé de logiciel suit les capacités créées par l'Annexe B/J.112 et, en tant que tels, les objets de base MIB peuvent être réutilisés dans le dispositif PS exactement comme le câblo-modem fait appel à eux. L'infrastructure PKI du modèle IPCable2Home est définie séparément et donc certaines des bases MIB de certificat DOIVENT être utilisées comme défini par IPCable2Home et non par les bases MIB de la Rec. UIT-T J.112, comme actuellement indiqué dans le projet [draft-ietf-ipcdn-bpiplus-mib-05].

Le dispositif PS autonome DOIT prendre en charge les objets de base MIB suivants comme défini dans le document CL-SP-MIB-CLABDEF-I03-030411 [voir § E.6]:

- **clabCVCRootCACert** – autorité CA radicale de vérification de code servant à la validation des certificats CVC;
- **clabCVCCACert** – autorité CA de vérification de code servant à la validation des certificats CVC;
- **clabMfgCACert** – certificat d'autorité CA de constructeur servant à mémoriser le certificat CA du constructeur.

Le dispositif PS autonome DOIT prendre en charge les objets de base MIB de téléchargement de logiciel suivants, définis dans le projet [draft-ietf-ipcdn-bpiplus-mib-05]:

- **docsBpi2CodeDownloadGroup** – collection d'objets qui offrent une prise en charge authentifiée du téléchargement de logiciel. Les valeurs de l'objet docsBpi2CodeDownloadGroup sont les suivantes:
  - **docsBpi2CodeDownloadStatusCode** – cet objet indique le résultat de la plus récente vérification du certificat CVC du fichier de configuration, de la plus récente vérification du certificat CVC du protocole SNMP, ou de la plus récente vérification du fichier de code;
  - **docsBpi2CodeDownloadStatusString** – informations complémentaires au code d'état;

– **docsBpi2CodeMfgOrgName** – nom d'organisation du constructeur de dispositif;
– **docsBpi2CodeMfgCodeAccessStart** – valeur actuelle de l'objet codeAccessStart du constructeur du dispositif, rapportée au temps moyen de Greenwich (GMT);
– **docsBpi2CodeMfgCvcAccessStart** – valeur actuelle de l'objet cvcAccessStart du constructeur du dispositif, rapportée au temps moyen de Greenwich (GMT);
– **docsBpi2CodeCoSignerOrgName** – nom d'organisation du cosignataire;
– **docsBpi2CodeCoSignerCodeAccessStart** – valeur actuelle de l'objet codeAccessStart du cosignataire, rapportée au temps moyen de Greenwich (GMT);
– **docsBpi2CodeCoSignerCvcAccessStart** – valeur actuelle de l'objet cvcAccessStart du cosignataire, rapportée au temps moyen de Greenwich (GMT);
– **docsBpi2CodeCvcUpdate** – déclenche la vérification par le dispositif du certificat CVC et la mise à jour de la valeur cvcAccessStart.

11.7.2 Objets de base MIB de fichier de configuration de la sécurité

Le dispositif PS DOIT prendre en charge l'objet suivant de base MIB de téléchargement du fichier de configuration comme défini dans la base MIB de sécurité:

cabhPsDevProvConfigHash – hachage SHA-1 [FIPS 186] du contenu entier du fichier de configuration, considéré comme une chaîne d'octets.

11.7.3 Objets de base MIB de fournisseur de services de sécurité

Le dispositif PS DOIT prendre en charge l'objet suivant de base MIB d'authentification du fournisseur de services comme défini dans la base MIB de sécurité:

clabSrvcPrvdrRootCACert – autorité CA radicale de fournisseur de services servant à valider des certificats de dispositif sur le réseau du fournisseur de services.

11.7.4 Objets de base MIB de certificat du dispositif PS

Le dispositif PS DOIT prendre en charge l'objet suivant de base MIB de certificat du dispositif PS, comme défini dans la base MIB de sécurité:

cabhSecCertPsCert – certificat X.509 codé en règles DER du dispositif PS servant à fournir l'identité sécurisée du dispositif PS.

11.7.5 Objets de base MIB Kerberos

Les besoins du protocole Kerberos dans le modèle IPCable2Home constituent un sous-ensemble de la fonctionnalité requise par IPCablecom. Les objets de base MIB suivants sont requis pour IPCable2Home et le dispositif PS DOIT prendre en charge ces objets de base MIB, comme défini dans la base MIB de sécurité:

- **cabhSecKerbPKINITGracePeriod** – nombre de minutes avant l'expiration du ticket actuel, pendant lequel le dispositif PS peut lancer une demande de nouveau ticket auprès du centre KDC;
- **cabhSecKerbTGSGracePeriod** – nombre de minutes avant à l'expiration du ticket actuel pendant lequel le dispositif PS peut lancer une demande de nouveau ticket auprès du centre KDC;
- **cabhSecKerbUnsolicitedKeyMaxTimeout** – valeur de temporisation maximale pour l'échange de demande/réponse AP;
- **cabhSecKerbUnsolicitedKeyMaxRetries** – nombre maximal de réessais que le dispositif PS est autorisé à effectuer lors d'une tentative de négociation par demande/réponse AP.

11.8 Téléchargement sécurisé de logiciel pour le dispositif PS

11.8.1 Téléchargement sécurisé de logiciel: objectifs

Les objectifs du téléchargement sécurisé de logiciel sont les suivants:

- le câblo-opérateur peut sans danger charger du code dans le dispositif PS selon les besoins;
- le câblo-opérateur peut gérer des téléchargements sécurisés avec diverses politiques de configuration;
- la sécurité du téléchargement offrira l'intégrité, l'authentification et, si possible, le chiffrement;
- le dispositif PS ne téléchargera que les images appropriées au dispositif.

11.8.2 Téléchargement sécurisé de logiciel: directives de conception

Voir le Tableau 11-22.

Tableau 11-22/J.192 – Sécurité IPCable2Home: directives de conception du système

Référence	Directives
SEC13	Le câblo-opérateur possédera la capacité de télécharger en sécurité les images logicielles vers l'élément de services de portail.

11.8.3 Téléchargement sécurisé de logiciel: description du système

Le téléchargement sécurisé de logiciel garantit qu'une image logicielle ne peut être téléchargée dans le dispositif PS que si cette image est créée par le même constructeur. Il garantit également que l'image n'a pas été modifiée depuis que le constructeur a signé l'image de code. L'image peut également être signée par un laboratoire d'essais de certification (CTL, *certification testing laboratory*) agissant en tant que cosignataire, afin de garantir que l'image a été certifiée. Comme sécurité supplémentaire dans le processus de téléchargement, le câblo-opérateur peut (facultativement) signer toute image en tant que cosignataire afin de garantir que seules des images que le câblo-opérateur a approuvées seront chargées dans le dispositif PS. Le mécanisme de commande pour le téléchargement sécurisé de logiciel consiste à insérer les certificats de vérification de code (certificats CVC) dans le fichier de configuration qui correspondent aux certificats CVC contenus dans l'image de code à télécharger. Après que le dispositif PS a reçu le ou les certificats CVC dans le fichier de configuration, ce dispositif PS est activé afin de télécharger la nouvelle image de code sur déclenchement par le fichier de configuration, ou par une requête SET (mise à jour) du protocole SNMP.

11.8.4 Téléchargement sécurisé de logiciel: exigences

Un élément PS autonome DOIT être capable de télécharger une image logicielle afin de l'importer dans le réseau. Comme décrit dans le § 6.3.3.2.4.9, le téléchargement sécurisé de logiciel vers un dispositif PS intégré est régi par le câblo-modem. La nouvelle image logicielle permettra au câblo-opérateur d'améliorer la performance, d'intégrer de nouvelles fonctions et caractéristiques, de corriger des déficiences de conception et d'offrir un chemin de migration aux dispositifs IPCable2Home au fur et à mesure des évolutions de ce modèle. La capacité de téléchargement de logiciel DOIT permettre de changer la fonctionnalité de l'élément de services de portail sans qu'il soit nécessaire que le personnel du système câblé visite et configure physiquement chaque unité. Le processus de téléchargement sécurisé de logiciel par un dispositif PS autonome répond aux exigences primaires de système suivantes:

- le mécanisme utilisé pour le téléchargement de logiciel DOIT être le protocole de transfert de fichiers TFTP;

- le téléchargement de logiciel DOIT être lancé d'une des deux façons suivantes:
  1) par une commande SNMP de requête de mise à jour (SET) envoyée par le système NMS à l'objet docsDevSwAdminStatus;
  2) par le fichier de configuration de l'élément de services de portail.

  Si le nom de fichier de mise à jour logicielle dans le fichier de configuration ne correspond pas à l'image logicielle actuelle du dispositif, l'élément de services de portail DOIT demander le fichier spécifié par TFTP auprès du serveur de logiciel;
- l'élément de services de portail DOIT vérifier que l'image logicielle téléchargée lui est appropriée. Si l'image logicielle téléchargée est appropriée, l'élément de services de portail DOIT écrire cette nouvelle image logicielle dans une mémoire non volatile. Une fois que le transfert de fichiers est achevé avec succès, le dispositif DOIT se relancer lui-même avec la nouvelle image de code;
- si l'élément de services de portail n'est pas en mesure d'achever le transfert de fichiers pour une raison ou une autre, l'élément de services de portail DOIT rester capable d'accepter de nouveaux téléchargements de logiciel (sans interaction avec l'opérateur ou avec l'utilisateur), même si l'alimentation ou la connexité est interrompue entre les tentatives;
- l'élément de services de portail DOIT journaliser les échecs de téléchargement de logiciel et peut les signaler de manière asynchrone au gestionnaire du réseau;
- lorsque le logiciel a été amélioré de façon à répondre à une nouvelle version de la présente Recommandation, alors il est critique que ce logiciel DOIVE opérer avec la version précédente afin de permettre une transition graduelle des unités dans le réseau;
- l'élément de services de portail DOIT authentifier l'image logicielle téléchargée;
- l'élément de services de portail DOIT vérifier que le code téléchargé n'a pas été altéré par rapport à la forme originale dans laquelle il a été offert par la source habilitée;
- le processus de téléchargement de logiciel DOIT offrir à un câblo-opérateur des mécanismes de surclassement/sous-classement de la version de code des éléments IPCable2Home;
- le processus de téléchargement de logiciel DOIT offrir des options permettant à un câblo-opérateur d'imposer ses propres politiques de téléchargement;
- le constructeur du fichier de code DOIT appliquer une signature de vérification de code (CVS) à l'image du code et à tous les autres attributs authentifiés, comme défini dans la présente Recommandation pour la signature numérique de la structure PKCS # 7 appliquée au fichier de code; la clé privée servant à appliquer la signature DOIT être reliée à un certificat de clé publique qui remonte jusqu'au certificat CVC radical. La signature du constructeur authentifie l'origine et l'intégrité du fichier de code;
- un cosignataire (câblo-opérateur ou laboratoire CTL) peut contresigner le fichier de code en plus de la signature du constructeur;
- l'élément de services de portail DOIT être capable de traiter une signature numérique PKCS # 7 et un certificat UIT-T X.509 comme défini dans les § 11.8.4.1.1 et 11.3.4.1.1, respectivement;
- l'élément de services de portail DOIT être capable de mettre à jour le certificat d'autorité CA radicale de certificat CVC mémorisé dans le dispositif, une fois que ce certificat a été validé s'il figurait dans un fichier de code sous forme de nuplet TLV;
- l'élément de services de portail DOIT être capable de remplacer le ou les certificats d'autorité CA de constructeur mémorisés dans le dispositif, une fois que ce ou ces certificats ont été validés s'ils figuraient dans un fichier de code sous forme de nuplet TLV;

- l'élément de services de portail DOIT être capable de mettre à jour le certificat d'autorité CA de certificat CVC mémorisé dans le dispositif, une fois que ce certificat a été validé s'il figurait dans un fichier de code sous forme de nuplet TLV;
- l'élément de services de portail DOIT être capable de mettre à jour le certificat d'autorité CA radicale de fournisseur de services, mémorisé dans le dispositif, une fois que ce certificat a été validé s'il figurait dans un fichier de code sous forme de nuplet TLV.

Le téléchargement facultatif du certificat d'autorité CA radicale de fournisseur de services, du certificat d'autorité CA radicale de certificat CVC, du certificat d'autorité CA de certificat CVC, et/ou du certificat d'autorité CA de constructeur, en tant que partie du fichier de code, permet de distinguer clairement l'image de code et des autres paramètres contenus dans le fichier de téléchargement de code. Il est possible de changer le certificat d'autorité CA radicale de fournisseur de services, le certificat d'autorité CA radicale de certificat CVC, le certificat d'autorité CA de certificat CVC, et/ou le certificat d'autorité CA de constructeur, interprété par l'élément de services de portail, en insérant ces nouveaux certificats dans l'image de code. L'insertion du certificat CVC du constructeur et/ou d'un certificat CVC de cosignataire avec la signature CVS correspondante, permet à l'élément de services de portail de vérifier que l'image de code n'a pas été altérée depuis que le certificat d'autorité CA radicale de fournisseur de services, le certificat d'autorité CA radicale de certificat CVC, le certificat d'autorité CA de certificat CVC, et/ou le certificat d'autorité CA de constructeur, ou des paramètres SignedData, ont été annexés à l'image de code.

Un dispositif de passerelle résidentielle communiquant les plaintes IPCable2Home peut inclure un câblo-modem et l'élément de services de portail, comme entités distinctes ou intégrées selon la définition donnée dans le paragraphe relatif à l'architecture (voir le § 5).

- Si l'élément de services de portail est intégré avec un câblo-modem, l'image PS/CM DOIT être une seule image et le téléchargement de logiciel DOIT être effectué seulement par le câblo-modem.
- Si l'élément de services de portail est composé d'entités distinctes et autonomes, le téléchargement de logiciel pour les éléments IPCable2Home DOIT être effectué par l'élément de services de portail, comme décrit ci-dessous dans la présente spécification.

11.8.4.1 Structure du fichier de téléchargement de code pour le téléchargement sécurisé de logiciel

Pour le téléchargement sécurisé de logiciel, le fichier de téléchargement de code est construit au moyen d'une structure conforme au [RFC 2315] qui a été définie dans un format spécifique à utiliser avec des éléments de services de portail. Le fichier de code DOIT être conforme au [RFC 2315] et DOIT être codé selon les règles DER. Le fichier de code DOIT correspondre à la structure représentée dans le Tableau 11-23.

Quand des certificats sont téléchargés dans le cadre du fichier de code, ces certificats PEUVENT être contenus dans les champs spécifiés dans le Tableau 11-23 et être séparés de l'image de code réelle contenue dans le champ CodeImage.

Tableau 11-23/J.192 – Structure du fichier de code

Fichier de code	Description
PKCS #7 Digital Signature {	
ContentInfo	
ContentType	SignedData
SignedData ()	Valeur EXPLICITE du contenu des données signées: y compris la signature CVS et les signatures CVS conformes à la Rec. UIT-T X.509.
} fin de signature numérique [RFC 2315]	
SignedContent {	
Download Parameters {	Format de TLV obligatoire (de type 28). (La longueur est zéro s'il n'y a aucun sous-champ TLV).
MfgCACerts ()	Nuplet TLV facultatif pour un ou plusieurs certificats à codage DER dont chacun est formaté conformément au nuplet TLV de certificat d'autorité CA du constructeur (de type 17).
clabServProvRootCACert ()	Nuplet TLV facultatif pour un seul certificat à codage DER formaté conformément au nuplet TLV de certificat d'autorité CA radicale de fournisseur de services (de type 50).
clabCVCRootCACert ()	Nuplet TLV facultatif pour un seul certificat à codage DER formaté conformément au nuplet TLV de certificat d'autorité CA radicale de certificat CVC (de type 51).
clabCVCCACertificate ()	Nuplet TLV facultatif pour un seul certificat à codage DER formaté conformément au nuplet TLV de Certificat d'autorité CA de certificat CVC (de type 52).
}	
CodeImage ()	Image du code de mise à jour
} end SignedContent	

11.8.4.1.1 Données signées

Le fichier de téléchargement de code contiendra les informations avec un type de contenu de données signées [RFC 2315] comme représenté dans le Tableau 11-24. Tout en conservant la conformité à [RFC 2315], la structure utilisée a été réduite en terme de format afin de faciliter le traitement effectué par le dispositif PS afin de valider la signature. Les données signées [RFC 2315] DOIVENT être codées en règles DER et correspondre exactement à la structure représentée ci-dessous, à l'exception des éventuels changements d'ordre requis par le codage DER (par exemple l'ordre des attributs de type SET OF). L'élément de services de portail DEVRAIT ignorer la signature [RFC 2315] si les données signées [RFC 2315] ne correspondent pas à la structure codée en règles DER.

Tableau 11-24/J.192 – Données signées PKCS # 7

Champ PKCS #7	Description
Signed Data {	
version	1
digestAlgorithms	SHA-1
contentInfo	
contentType	Données (l'élément SignedContent est concaténé jusqu'à la fin de la structure PKCS # 7)
certificates {	
mfgCVC	(REQUIS pour tous les fichiers de code) (Note 1)
co-signerCVC	(FACULTATIF; requis pour cosignatures) (Note 2)
} *fin des certificats*	
signerInfos{	
MfgSignerInfo {	(REQUIS pour tous les fichiers de code)
version	1
issuerAndSerialNumber	
issuer	
countryName	Etats-Unis d'Amérique
organizationName	CableLabs
commonName	Autorité CA radicale de certificat CVC de CableLabs
serialNumber	<Numéro de série du certificat CVC du constructeur>
digestAlgorithm	SHA-1
authenticatedAttributes	
contentType	Données (type de contenu de l'élément signedContent)
signingTime	Temps UTC (GMT), AAMMJJhhmmssZ
messageDigest	(condensé du contenu en association avec les attributs authentifiés du signataire, comme défini dans [PKCS # 7])
digestEncryptionAlgorithm	Chiffrement rsa
encryptedDigest	
} *fin des infos de constr. signataire*	
CoSignerInfo {	(FACULTATIF; requis pour les cosignatures)
version	1
issuerAndSerialNumber	
issuer	
countryName	Etats-Unis d'Amérique
organizationName	CableLabs
commonName	Autorité CA de certificat CVC de CableLabs
serialNumber	<Numéro de série de certificat CVC de cosignataire>
digestAlgorithm	SHA-1
authenticatedAttributes	
contentType	Données (type de contenu de l'élément signedContent)

Tableau 11-24/J.192 – Données signées PKCS # 7

Champ PKCS #7	Description
signingTime	Temps UTC (GMT), AAMMJJhhmmssZ
messageDigest	(condensé du contenu en association avec les attributs authentifiés du signataire, comme défini dans [PKCS # 7])
digestEncryptionAlgorithm	Chiffrement rsa
encryptedDigest	
} *fin des infos de cosignataire*	
} *fin des infos de signataire*	
} *fin des données signées*	
NOTE 1 – Le certificat CVC du constructeur DOIT respecter le format spécifié dans le Tableau 11-9. NOTE 2 – Le certificat CVC du cosignataire DOIT respecter le format spécifié dans le Tableau 11-10 ou dans le Tableau 11-11 selon le type de cosignataire, qui peut être le laboratoire CTL ou le fournisseur de services, selon le cas.	

11.8.4.1.2 Contenu signé

Le champ de contenu signé du fichier de code contient l'image de code et le champ des paramètres de téléchargement, qui contient éventuellement les éléments facultatifs supplémentaires suivants:

- certificat d'autorité CA radicale de fournisseur de services;
- certificat d'autorité CA radicale de certificat CVC du laboratoire d'essais de certification (CTL);
- certificat d'autorité CA de certificat CVC du laboratoire CTL;
- certificat d'autorité CA de constructeur.

L'image de code finale est dans un format compatible avec l'élément de services de portail de destination. Afin de prendre en charge les exigences [RFC 2315] relatives à la signature, le code contenu est caractérisé comme étant des données, c'est-à-dire comme une simple chaîne d'octets. Le format de l'image de code finale n'est pas spécifié ici et sera défini par chaque constructeur conformément à ses exigences.

Chaque constructeur DEVRAIT construire son code avec des mécanismes supplémentaires qui vérifient qu'une image de code de mise à jour est compatible avec l'élément de services de portail de destination.

S'il est inclus dans le champ de contenu signé, un certificat est destiné à remplacer le certificat actuellement mémorisé dans l'élément de services de portail. Si le téléchargement et l'installation du code ont réussi, l'élément de services de portail DOIT remplacer son certificat actuellement mémorisé par le nouveau certificat reçu dans le champ de contenu signé, une fois le certificat validé. Ce nouveau certificat sera utilisé pour les vérifications subséquentes.

11.8.4.1.3 Clés de signature de code

La signature numérique [RFC 2315] fait appel à l'algorithme de chiffrement RSA [PKCS #1] avec hachage SHA-1 [FIPS 186]. L'élément de services de portail DOIT être capable de vérifier les signatures de fichier de code. L'exposant public est F_4 (65537 en décimal).

11.8.4.1.4 Certificat d'autorité CA de constructeur

Cet attribut est une chaîne contenant un certificat d'autorité CA X.509, comme défini dans [Rec. UIT-T X.509].

Type	Longueur	Valeur
17	Variable	Certificat d'autorité CA X.509 (notation ASN.1 codée en règles DER)

11.8.4.1.5 Certificat d'autorité CA radicale de fournisseur de services

Cet attribut est une chaîne contenant un certificat d'autorité CA radicale de fournisseur de services X.509, comme défini dans [Rec. UIT-T X.509]. Ce certificat doit être utilisé par l'élément de services de portail en mode de préconfiguration SNMP pour l'authentification mutuelle.

Type	Longueur	Valeur
50	Variable	Certificat d'autorité CA X.509 (notation ASN.1 codée en règles DER)

11.8.4.1.6 Certificat d'autorité CA radicale de certificat CVC

Cet attribut est une chaîne contenant un certificat d'autorité CA radicale de certificat CVC X.509 comme défini dans [Rec. UIT-T X.509]. Ce certificat doit être utilisé par l'élément PS autonome dans le processus de téléchargement sécurisé de logiciel.

Type	Longueur	Valeur
10	Variable	Certificat d'autorité CA X.509 (notation ASN.1 codée en règles DER)

11.8.4.1.7 Certificat d'autorité CA de certificat CVC

Cet attribut est une chaîne contenant un certificat d'autorité CA de certificat CVC X.509, comme défini dans [Rec. UIT-T X.509]. Ce certificat doit être utilisé par l'élément PS autonome dans le processus de téléchargement sécurisé de logiciel.

Type	Longueur	Valeur
52	Variable	Certificat d'autorité CA X.509 (notation ASN.1 codée en règles DER)

11.8.4.2 Format de certificat CVC pour le téléchargement sécurisé de logiciel

Pour le téléchargement sécurisé de logiciel, le format servant au certificat CVC est conforme à la Rec. UIT-T X.509. Cependant, la structure X.509 a été réduite afin de faciliter le traitement effectué par un élément de services de portail et de valider le certificat et d'extraire la clé publique servant à vérifier la signature CVS. Le certificat CVC DOIT être codé en règles DER et être conforme aux Tableaux 11-9, 11-10 et 11-11 selon le type de certificat CVC. L'élément de services de portail DEVRAIT rejeter le certificat CVC s'il ne correspond pas à la table correspondante.

11.8.4.2.1 Révocation de certificat

La présente Recommandation n'exige ni ne définit l'utilisation de listes de révocation de certificat (CRL). L'élément de services de portail n'est pas tenu de prendre en charge les listes CRL. Les opérateurs peuvent définir et utiliser des listes CRL afin de faciliter la gestion des fichiers de code qui leur sont offerts par les constructeurs. Cependant, il y a une méthode pour révoquer les certificats sur la base de la date de leur début de validité. Cette méthode exige qu'un certificat CVC mis à jour soit délivré à l'élément de services de portail avec une heure de début de validité mise à jour. Une fois que le certificat CVC est correctement validé, l'instant de début de validité X.509 va mettre à jour la valeur actuelle de l'objet cvcAccessStart dans l'élément de services de portail.

11.8.4.3 Contrôles d'accès de fichier de code

Pour le téléchargement sécurisé de logiciel, des valeurs de contrôle spéciales sont incluses dans le fichier de code pour que l'élément de services de portail les vérifie avant qu'il ne valide une image de code. Les conditions imposées aux valeurs de ces paramètres de contrôle DOIVENT être satisfaites avant que l'élément de services de portail valide le certificat CVC ou la signature CVS, et accepte l'image de code.

11.8.4.3.1 Noms d'organisation titulaire

L'élément de services de portail va reconnaître jusqu'à deux noms, à tout instant donné, qu'il considère comme un agent signataire de code habilité dans le champ de titulaire d'un fichier de code CVC:

- le constructeur du dispositif: le nom du constructeur contenu dans le champ de titulaire du certificat CVC du constructeur DOIT correspondre exactement au nom du constructeur mémorisé dans la mémoire non volatile de l'élément de services de portail par le constructeur. Un certificat CVC du constructeur DOIT toujours être inclus dans le fichier de code;
- un agent cosignataire: il est autorisé qu'une autre organisation habilitée cosigne les fichiers de code destinés au dispositif. Dans la plupart des cas, c'est le câblo-opérateur qui contrôle le domaine de fonctionnement actuel du dispositif. Le nom d'organisation du cosignataire est communiqué à l'élément de services de portail par un certificat CVC de cosignataire inséré dans le fichier de configuration lors de l'initialisation du processus de vérification de code de l'élément de services de portail. Le nom d'organisation du cosignataire figurant dans le champ de titulaire du certificat CVC de cosignataire DOIT correspondre exactement au nom d'organisation de cosignataire précédemment reçu dans le certificat CVC d'initialisation et mémorisé par l'élément de services de portail.

L'élément de services de portail PEUT comparer les noms d'organisation au moyen d'une comparaison binaire.

11.8.4.3.2 Contrôles variables dans le temps

Afin de réduire la probabilité qu'un élément de services de portail reçoive un précédent fichier de code par le biais d'une attaque par réexécution, les fichiers de code comprennent une valeur d'instant de signature contenue dans la structure PKCS #7 qui peut servir à indiquer l'instant auquel l'image de code a été signée. L'élément de services de portail DOIT conserver deux valeurs de temps UTC associées à chaque agent de signature de code. Un seul ensemble DOIT toujours être mémorisé et conservé pour le dispositif constructeur. De plus, si le fichier de code est cosigné, l'élément de services de portail DOIT également stocker et conserver un ensemble distinct de valeurs temporelles pour le cosignataire.

Ces valeurs servent à contrôler l'accès du fichier de code à l'élément de services de portail en contrôlant individuellement la validité de la signature CVS et du certificat CVC:

- codeAccessStart: valeur temporelle UTC de 12 octets, rapportée au temps moyen de Greenwich (GMT);
- cvcAccessStart: valeur temporelle UTC de 12 octets, rapportée au temps moyen de Greenwich (GMT).

Les valeurs de temps UTC incluses dans le certificat CVC DOIVENT être exprimées en temps GMT et DOIVENT inclure les secondes, c'est-à-dire qu'elles DOIVENT être exprimées dans le format suivant: AAMMJJhhmmssZ. Le champ d'année (AA) DOIT être interprété comme suit:

- lorsque AA est supérieur ou égal à 50, l'année doit être interprétée comme 19AA;
- lorsque AA est inférieur à 50, l'année doit être interprétée comme 20AA.

Ces valeurs seront toujours rapportées au temps moyen de Greenwich, de sorte que le caractère ASCII final (Z) peut être supprimé quand ces valeurs sont mémorisées par l'élément de services de portail comme objets codeAccessStart et cvcAccessStart.

L'élément de services de portail DOIT conserver chacune de ces valeurs temporelles dans un format qui contienne des informations et une précision temporelles équivalentes au format UTC à 12 caractères (c'est-à-dire AAMMDDhhmmss). L'élément de services de portail DOIT comparer précisément ces valeurs mémorisées aux valeurs de temps UTC délivrées à l'élément de services de

portail dans un certificat CVC. Ces exigences sont examinées ci-dessous dans la présente Recommandation.

Les valeurs des objets codeAccessStart et cvcAccessStart correspondant au constructeur de l'élément de services de portail NE DOIVENT PAS diminuer. La valeur des objets codeAccessStart et cvcAccessStart correspondant au cosignataire NE DOIVENT PAS diminuer aussi longtemps que le cosignataire ne change pas et que l'élément de services de portail conserve ces valeurs de contrôle variables dans le temps du cosignataire.

11.8.4.4 Initialisation de mise à jour de code

11.8.4.4.1 Initialisation du constructeur

Il appartient au constructeur d'installer correctement la version initiale de code dans l'élément de services de portail.

Afin de prendre en charge le téléchargement sécurisé de logiciel, les valeurs de contrôle variables dans le temps du constructeur DOIVENT être chargées dans la mémoire non volatile de l'élément de services de portail:

- nom d'organisation du constructeur de l'élément de services de portail;
- valeurs de contrôles variables dans le temps du constructeur:
  - valeur d'initialisation de l'objet codeAccessStart;
  - valeur d'initialisation de l'objet cvcAccessStart.

Le nom d'organisation du constructeur de l'élément de services de portail DOIT toujours être présent dans le dispositif. Le nom d'organisation du constructeur de l'élément de services de portail PEUT être mémorisé dans l'image de code du dispositif. Le nom de constructeur servant à la mise à jour du code n'est pas nécessairement le même que celui qui est utilisé dans le certificat d'autorité CA de constructeur.

Les valeurs de contrôles variables dans le temps, objets codeAccessStart et cvcAccessStart, DOIVENT être initialisées à un temps UTC compatible avec l'instant de début de validité du plus récent certificat CVC du constructeur. Ces valeurs variables dans le temps seront mises à jour périodiquement en période de fonctionnement normal au moyen des certificats CVC de constructeur qui sont reçus et vérifiés par l'élément de services de portail.

Le constructeur DOIT initialiser les certificats suivants dans la mémoire non volatile de l'élément PS autonome:

- certificat d'autorité CA radicale de fournisseur de services;
- certificat d'autorité CA radicale de certificat CVC;
- certificat d'autorité CA de certificat CVC;
- certificat d'autorité CA de constructeur;
- certificat d'élément de services de portail.

Le constructeur DOIT initialiser les certificats suivants dans la mémoire non volatile de l'élément PS intégré:

- certificat d'autorité CA radicale de fournisseur de services;
- certificat d'autorité CA de constructeur;
- certificat d'élément de services de portail.

11.8.4.4.2 Initialisation du réseau

Afin de prendre en charge la vérification de code, le fichier de configuration du dispositif PS est utilisé comme moyen authentifié permettant de lancer le processus de vérification de code. Dans le

fichier de configuration de l'élément de services de portail, l'élément de services de portail reçoit les réglages de configuration applicables à la vérification de mise à jour du code.

Le fichier de configuration DEVRAIT toujours inclure le certificat CVC le plus à jour qui soit applicable à l'élément de services de portail de destination. Quand le fichier de configuration sert à lancer une mise à jour du code, il DOIT inclure un certificat de vérification de code (CVC) afin de lancer l'acceptation, par l'élément de services de portail, des fichiers de code conformément à la présente Recommandation. Sans tenir compte de savoir si une mise à jour du code est requise, un certificat CVC inclus dans le fichier de configuration DOIT être traité par l'élément de services de portail. Un fichier de configuration PEUT contenir:

- aucun certificat CVC – l'élément de services de portail NE DOIT PAS accepter de fichier de code;
- un seul certificat CVC de constructeur – l'élément de services de portail DOIT vérifier que le certificat CVC de constructeur remonte jusqu'à la racine de certificat CVC avant d'accepter un fichier de code. Quand le fichier de configuration de l'élément de services de portail contient seulement un certificat CVC valide de constructeur, le dispositif va seulement exiger une signature de constructeur sur les fichiers de code. Dans ce cas, l'élément de services de portail NE DOIT PAS accepter de fichiers de code qui ont été cosignés;
- seulement un certificat CVC de cosignataire (câblo-opérateur ou CTL) – l'élément de services de portail DOIT vérifier que le cosignataire CV remonte jusqu'à la racine de certificat CVC avant d'accepter un fichier de code. Quand le fichier de configuration de l'élément de services de portail contient un certificat CVC valide de cosignataire, il sert à lancer le dispositif avec un cosignataire. Une fois validé, le nom d'organisation du titulaire du certificat CVC va devenir le cosignataire de code attribué à l'élément de services de portail. Afin qu'un élément de services de portail accepte ultérieurement une image de code, le cosignataire, en plus de constructeur du dispositif, DOIT avoir signé le fichier de code;
- à la fois un certificat CVC de constructeur et un certificat CVC de cosignataire – l'élément de services de portail DOIT vérifier que les deux certificats CVC remontent jusqu'à la racine de certificat CVC avant d'accepter un fichier de code.

Avant que l'élément de services de portail active sa capacité de mise à jour des fichiers de code dans le réseau, il DOIT recevoir un certificat CVC valide dans un fichier de configuration. En outre, quand le fichier de configuration de l'élément de services de portail ne contient pas de certificat CVC valide (ce qui signifie que sa capacité de mise à jour des fichiers de code a été désactivée) l'élément de services de portail DOIT rejeter toutes les informations contenues dans un certificat CVC délivré ultérieurement par un objet de base MIB docsBpi2CodeCvcUpdate du protocole SNMP.

Le nom d'organisation du constructeur de l'élément de services de portail et les valeurs de contrôles variables dans le temps du constructeur DOIVENT toujours être présents dans l'élément de services de portail. Si celui-ci est initialisé de façon à accepter un code cosigné par un signataire de code supplémentaire, le nom de l'organisation et les valeurs de contrôles variables dans le temps correspondantes DOIVENT être mémorisés et conservés pendant qu'ils sont opérationnels. De l'espace DOIT être attribué dans la mémoire de l'élément de services de portail pour les valeurs de contrôle de cosignataire suivantes:

- nom d'organisation de l'agent cosignataire;
- valeurs de contrôles variables dans le temps du cosignataire:
  - cvcAccessStart;
  - codeAccessStart.

L'ensemble de ces valeurs de constructeur DOIT être mémorisé dans la mémoire non volatile de l'élément de services de portail et NE DOIT PAS être perdu quand la source d'alimentation principale du dispositif est supprimée ou pendant un réamorçage.

Quand un cosignataire est attribué à l'élément de services de portail, l'ensemble de valeurs de certificat CVC du cosignataire DOIT être mémorisé dans la mémoire de l'élément de services de portail. Celui-ci PEUT conserver ces valeurs en mémoire non volatile, qui ne doit pas être perdue quand la source d'alimentation principale du dispositif est supprimée ou pendant un réamorçage. Cependant, lors de l'attribution d'un cosignataire à un élément de services de portail, le certificat CVC est toujours dans le fichier de configuration. L'élément de services de portail va donc toujours recevoir les valeurs de contrôle de cosignataire pendant la phase d'initialisation et ne sera pas tenu de stocker les valeurs de contrôle de cosignataire variables dans le temps quand l'alimentation principale est perdue ou pendant un processus de réamorçage.

11.8.4.4.3 Traitement de certificat CVC

Afin d'accélérer la livraison d'un certificat CVC mis à jour sans demander au dispositif PS de procéder à une mise à jour du code, le certificat CVC PEUT être délivré dans le fichier de configuration ou dans un message de commande SNMP de mise à jour (SET). Le format du certificat CVC est le même, qu'il soit dans un fichier de code, dans un fichier de configuration, ou dans un message SNMP.

11.8.4.4.3.1 Traitement du certificat CVC dans un fichier de configuration

Quand un certificat CVC est inclus dans le fichier de configuration, l'élément de services de portail DOIT vérifier ce certificat CVC avant d'accepter l'un quelconque des réglages de mise à jour de code qu'il contient. Dès réception du certificat CVC dans le fichier de configuration, l'élément de services de portail DOIT exécuter les étapes de validation et de procédure suivantes. Si l'un des essais de vérification suivants échoue, l'élément de services de portail DOIT immédiatement arrêter le processus de vérification du certificat CVC et journaliser l'erreur si applicable. Si le fichier de configuration du dispositif PS n'inclut pas de certificat CVC correctement validé, l'élément de services de portail NE DOIT PAS télécharger les fichiers de mise à jour de code, que ce téléchargement soit déclenché par le fichier de configuration du dispositif PS ou par l'objet de base MIB docsDevSwAdminStatus du protocole SNMP. En outre, si le fichier de configuration du dispositif PS ne contient pas de certificat CVC (de constructeur ou de cosignataire) correctement validé, l'élément de services de portail n'est pas tenu de traiter les certificats CVC délivrés ultérieurement au moyen de l'objet de base MIB docsBpi2CodeCvcUpdate du protocole SNMP et NE DOIT PAS accepter d'informations en provenance de ces certificats CVC (c'est-à-dire que l'élément de services de portail DOIT ignorer toutes les éventuelles requêtes SET du protocole SNMP envoyées à l'objet de base MIB docsBpi2CodeCvcUpdate du protocole SNMP.

Dès réception du certificat CVC dans un fichier de configuration, l'élément de services de portail DOIT:

1) vérifier que le certificat CVC est conforme à la structure et aux valeurs prescrites dans le § 11.3.4.2;
2) vérifier le nom d'organisation titulaire du certificat CVC:
    a) Si le certificat CVC est un certificat CVC de constructeur (de type 32) alors:
        i) si le nom d'organisation est identique au nom du constructeur du dispositif, alors c'est le certificat CVC du constructeur. Dans ce cas, l'élément de services de portail DOIT vérifier que l'instant de début de la validité du certificat CVC de constructeur est supérieur ou égal à la valeur cvcAccessStart du constructeur actuellement contenue dans l'élément de services de portail;
        ii) si le nom d'organisation n'est pas identique au nom du constructeur du dispositif, alors ce certificat CVC DOIT être rejeté et l'erreur être journalisée;

b) si le certificat CVC est un certificat CVC de cosignataire (de type 33) alors:

i) si le nom d'organisation est identique à celui du cosignataire de code actuel de l'élément de services de portail, alors c'est le certificat CVC du cosignataire actuel et l'élément de services de portail DOIT vérifier que l'instant de début de validité est supérieur ou égal à la valeur cvcAccessStart du cosignataire actuellement contenue dans l'élément de services de portail;

ii) si le nom d'organisation n'est pas identique au nom du cosignataire actuel alors, après que le certificat CVC a été validé (et que l'enregistrement est terminé), ce nom d'organisation titulaire va devenir le nouveau cosignataire de code de l'élément de services de portail, lequel NE DOIT PAS accepter de fichier de code à moins qu'il n'ait été signé par le constructeur et cosigné par ce cosignataire de code;

3) valider la signature de l'émetteur de certificat CVC au moyen de la clé publique d'autorité CA de certificat CVC du laboratoire CTL détenue par l'élément de services de portail;

4) valider la signature d'autorité CA de certificat CVC du laboratoire CTL au moyen de la clé publique d'autorité CA radicale de certificat CVC du laboratoire CTL détenue par l'élément de services de portail. La vérification de la signature authentifiera l'origine et validera la confiance dans les paramètres du certificat CVC;

5) mettre à jour la valeur actuelle de l'objet cvcAccessStart de l'élément de services de portail correspondant au nom d'organisation titulaire du certificat CVC (c'est-à-dire du constructeur ou du cosignataire) avec la valeur d'instant de début de validité extraite du certificat CVC validé. Si la valeur d'instant de début de validité est supérieure à la valeur actuelle de l'objet codeAccessStart de l'élément de services de portail, mettre à jour la valeur de l'objet codeAccessStart de l'élément de services de portail avec la valeur d'instant de début de validité. L'élément de services de portail DEVRAIT ignorer tous les résidus éventuels du certificat CVC de cosignataire.

11.8.4.4.3.2 Traitement du certificat CVC en protocole SNMP

L'élément de services de portail DOIT traiter les certificats CVC délivrés par protocole SNMP quand il a la capacité de mettre à jour les fichiers de code. Sinon, tous les certificats CVC délivrés par protocole SNMP DOIVENT être rejetés. Lorsqu'il valide le certificat CVC délivré par protocole SNMP, l'élément de services de portail DOIT exécuter les étapes de validation et de procédure suivantes:

NOTE – Si l'un quelconque des essais de vérification échoue, l'élément de services de portail DOIT immédiatement arrêter le processus de vérification du certificat CVC, journaliser l'erreur si applicable et supprimer tous les résidus du processus à cette étape.

L'élément de services de portail DOIT:

1) vérifier que le certificat CVC est conforme à la structure et aux valeurs prescrites dans le § 11.3.4.2.2.2;

2) vérifier le nom d'organisation titulaire du certificat CVC:

a) si le nom d'organisation est identique au nom du constructeur du dispositif, alors c'est le certificat CVC de constructeur. Dans ce cas, l'élément de services de portail DOIT vérifier que l'instant de début de la validité du certificat CVC de constructeur est supérieur à la valeur cvcAccessStart du constructeur actuellement contenue dans l'élément de services de portail;

b) si le nom d'organisation est identique à celui du cosignataire de code actuel de l'élément de services de portail, alors c'est un certificat CVC du cosignataire actuel et l'instant de début de validité DOIT être supérieur à la valeur cvcAccessStart du cosignataire actuellement contenue dans l'élément de services de portail;

c) si le nom d'organisation n'est pas identique au nom du constructeur du dispositif ou du cosignataire actuel, alors l'élément de services de portail DOIT immédiatement ignorer ce certificat CVC;

3) valider la signature de l'émetteur de certificat CVC au moyen de la clé publique d'autorité CA de certificat CVC du laboratoire CTL détenue par l'élément de services de portail;

4) valider la signature de l'émetteur de certificat CVC au moyen de la clé publique d'autorité CA radicale de certificat CVC du laboratoire CTL détenue par l'élément de services de portail. La vérification de la signature authentifiera le certificat et confirmera la confiance dans l'instant de début de validité du certificat CVC;

5) mettre à jour la valeur actuelle de l'objet cvcAccessStart du titulaire avec la valeur de l'instant de début de validité du certificat CVC. Si la valeur d'instant de début de validité est supérieure à la valeur actuelle de l'objet codeAccessStart de l'élément de services de portail, mettre à jour la valeur de l'objet codeAccessStart de l'élément de services de portail avec la valeur de début de validité.

11.8.4.5 Exigences relatives à la signature de code

11.8.4.5.1 Exigences relatives à l'autorité de certification (CA)

Les certificats de vérification de code (certificats CVC) sont signés et envoyés par l'autorité CA de certificat CVC du laboratoire d'essais de certification (CTL). Le certificat CVC DOIT être exactement comme spécifié dans le § 11.3.4.2.2.2, selon le type de certificat CVC.

Dans tout format en variante, toutes ces informations DOIVENT être conservées et le format original DOIT être reproduit; par exemple comme un entier de 32 bits différent de zéro avec une valeur d'entier égale à 0 représentant l'absence de signataire de code.

11.8.4.5.2 Exigences relatives au certificat CVC du constructeur

Afin de signer ses fichiers de code, le constructeur DOIT obtenir un certificat CVC valide à partir de l'autorité CA de certificat CVC de laboratoire CTL. Toutes les images de code fournies par le constructeur à un câblo-opérateur pour la mise à jour à distance d'un dispositif DOIVENT être signées conformément aux exigences définies dans la présente Recommandation. Lorsqu'il signe un fichier de code, un constructeur peut choisir de ne pas mettre à jour la valeur [RFC 2315] signingTime contenue dans les informations de signature du constructeur. La présente Recommandation exige que cette valeur [RFC 2315] signingTime soit égale ou supérieure à l'instant de début de validité du certificat CVC. Si le constructeur fait appel à une valeur signingTime égale à l'instant de début de validité du certificat CVC lorsqu'il signe une série de fichiers de code, ceux-ci peuvent être utilisés et réutilisés. Cela permet à un câblo-opérateur d'utiliser le fichier de code afin de surclasser/sous-classer la version de code pour les dispositifs de ce constructeur. Ces fichiers de code seront valides jusqu'à ce qu'un nouveau certificat CVC soit produit et reçu par l'élément de services de portail.

11.8.4.5.3 Exigences relatives au câblo-opérateur

Quand un câblo-opérateur reçoit des fichiers de code de mise à jour logicielle à partir d'un constructeur, ce câblo-opérateur va valider l'image de code au moyen de la clé publique d'autorité CA de certificat CVC du laboratoire CTL. Cela permettra au câblo-opérateur de vérifier que l'image de code est telle qu'elle a été construite par le constructeur habilité. Le câblo-opérateur peut revérifier le fichier de code à tout instant en répétant le processus.

Si un câblo-opérateur souhaite exercer l'option de cosignature de l'image de code destinée à un dispositif de son réseau, ce câblo-opérateur DOIT obtenir un certificat CVC valide à partir de l'autorité CA de certificat CVC de laboratoire CTL.

Lorsqu'il signe un fichier de code, le câblo-opérateur DOIT cosigner le contenu du fichier conformément à la norme de signature PKCS #7 et inclure son certificat CVC de câblo-opérateur comme défini dans le § 11.8.4.1.1. Le modèle IPCable2Home n'exige pas d'un câblo-opérateur qu'il cosigne les fichiers de code. Cependant, quand le câblo-opérateur suit toutes les règles définies dans la présente Recommandation pour préparer un fichier de code, l'élément de services de portail DOIT l'accepter.

11.8.4.6 Processus de déclenchement

Les téléchargements de code, sans tenir compte du mode de préconfiguration, peuvent être lancés pendant le processus de préconfiguration et d'enregistrement, au moyen d'un téléchargement initialisé par fichier de configuration, ou pendant le fonctionnement normal au moyen d'une commande de téléchargement initialisée par protocole SNMP. L'élément de services de portail DOIT prendre en charge les deux méthodes.

NOTE – Avant de déclencher un téléchargement sécurisé de logiciel, les informations de certificat CVC appropriées DOIVENT être incluses dans le fichier de configuration. Si l'opérateur décide d'utiliser le téléchargement lancé par protocole SNMP comme méthode de déclenchement d'un téléchargement sécurisé de logiciel, il est recommandé que les informations de certificat CVC soient toujours présentes dans le fichier de configuration, de façon qu'un élément de services de portail ait toujours les informations de certificat CVC initialisées quand nécessaire. Si l'opérateur décide d'utiliser le téléchargement initialisé par fichier de configuration comme méthode de déclenchement du téléchargement sécurisé de logiciel, les informations de certificat CVC doivent être présentes dans le fichier de configuration au moment où le dispositif est réamorcé afin d'obtenir le fichier de configuration qui va déclencher la mise à jour.

11.8.4.6.1 Téléchargement de logiciel initialisé par le protocole SNMP

A partir d'une station de gestion de réseau:

- mettre docsDevSwServer à l'adresse du serveur TFTP pour les mises à jour logicielles;
- mettre docsDevSwFilename au nom de chemin de fichier de l'image de mise à jour logicielle;
- mettre docsDevSwAdminStatus à Upgrade-from-mgt (mise à jour venant de la gestion). L'état docsDevSwAdminStatus DOIT persister au-delà des réinitialisations/réamorçages jusqu'à ce qu'il soit remplacé par une surécriture effectuée par un gestionnaire SNMP ou par le fichier de configuration de l'élément de services de portail.

L'état par défaut de l'objet docsDevSwAdminStatus DOIT être la valeur allowProvisioningUpgrade{2} jusqu'à ce qu'il soit remplacé en surécriture par la valeur ignoreProvisioningUpgrade{3} après une initialisation de mise à jour logicielle par protocole SNMP réussie, ou modifié autrement par la station de gestion. L'état docsDevSwOperStatus DOIT persister au-delà des réinitialisations afin de signaler le résultat de la dernière tentative de mise à jour logicielle.

Si un élément de services de portail subit une perte d'alimentation ou une réinitialisation pendant une mise à jour initialisée par SNMP, l'élément de services de portail DOIT reprendre la mise à jour sans exiger d'intervention manuelle et, quand l'élément de services de portail reprend le processus de mise à jour:

- docsDevSwAdminStatus DOIT être à la valeur Upgrade-from-mgt{1};
- docsDevSwFilename DOIT être le nom du fichier de l'image logicielle à mettre à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant l'image de mise à jour logicielle à mettre à jour;
- docsDevSwOperStatus DOIT être à la valeur inProgress{1};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui doit fonctionner dans le dispositif.

Si l'élément de services de portail atteint le nombre maximal de réessais (nombre maximal de réessais = 3) à la suite de multiples pertes d'alimentation ou réinitialisations pendant une mise à jour initialisée par SNMP, l'état de l'élément de services de portail DOIT adhérer aux exigences suivantes après avoir été enregistré:

- docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom du fichier du logiciel qui a échoué au processus de mise à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à jour;
- docsDevSwOperStatus DOIT être à la valeur other{5};
- docsDevSwCurrentVer DOIT être la version actuelle de logiciel qui doit fonctionner dans le dispositif.

Si un élément de services de portail atteint le nombre maximal de réessais TFTP par l'envoi d'un total de 16 réessais consécutifs, l'élément de services de portail DOIT se replier sur la dernière image connue qui fonctionnait, passer à un état opérationnel et adhérer aux exigences suivantes:

- docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom du fichier du logiciel qui a échoué au processus de mise à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à jour;
- docsDevSwOperStatus DOIT être à la valeur failed{4};
- docsDevSwCurrentVer DOIT être la version actuelle de logiciel qui doit fonctionner dans le dispositif.

Après que l'élément de services de portail a achevé la mise à jour logicielle sécurisée qui a été lancée par protocole SNMP, l'élément de services de portail DOIT réamorcer et devenir opérationnel avec l'image logicielle correcte. Quand le dispositif est opérationnel, il DOIT adhérer aux exigences suivantes:

- mettre son objet docsDevSwAdminStatus à la valeur ignoreProvisioningUpgrade{3};
- mettre son objet docsDevOperStatus à la valeur completeFromMgt{3};
- réamorcer.

L'élément de services de portail DOIT correctement utiliser la valeur ignoreProvisioningUpgrade afin d'ignorer la valeur de mise à jour logicielle qui peut être incluse dans le fichier de configuration de l'élément de services de portail. Celui-ci DOIT devenir opérationnel avec l'image logicielle correcte et DOIT adhérer aux exigences suivantes:

- docsDevSwAdminStatus DOIT être à la valeur ignoreProvisioningUpgrade{3};
- docsDevSwFilename PEUT être le nom du fichier du logiciel fonctionnant actuellement dans l'élément de services de portail;
- docsDevSwServer PEUT être l'adresse du serveur TFTP contenant le logiciel qui fonctionne actuellement dans l'élément de services de portail;
- docsDevSwOperStatus DOIT être à la valeur completeFromMgt{3};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui doit fonctionner dans l'élément de services de portail.

Si l'élément de services de portail télécharge correctement (ou détecte pendant le téléchargement), une image qui n'est pas destinée au dispositif, l'objet:

- docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};

- docsDevSwFilename DOIT être le nom du fichier du logiciel qui a échoué à la mise à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à jour;
- docsDevSwOperStatus DOIT être à la valeur other{5};
- docsDevSwCurrentVer DOIT être la version actuelle de logiciel qui doit fonctionner dans le dispositif.

Si l'élément de services de portail détermine que l'image téléchargée est endommagée ou corrompue, l'élément de services de portail DOIT ignorer l'image nouvellement téléchargée. L'élément de services de portail peut réessayer de télécharger si le nombre MAX de réessais de séquence TFTP n'a pas été atteint. Si l'élément de services de portail choisit de ne pas réessayer et que le nombre MAX de réessais de séquence TFTP n'ait pas été atteint, l'élément de services de portail DOIT se replier sur la dernière image connue qui fonctionnait et passer à un état opérationnel, produire les notifications d'événement appropriées comme spécifié dans le § 11.8.4.8 et adhérer aux exigences suivantes:

- DocsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom du fichier du logiciel qui a échoué à la mise à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à jour;
- docsDevSwOperStatus DOIT être à la valeur other{5};
- docsDevSwCurrentVer DOIT être la version actuelle de logiciel qui doit fonctionner dans le dispositif.

Si l'élément de services de portail détermine que l'image est endommagée ou corrompue, l'élément de services de portail DOIT ignorer l'image nouvellement téléchargée. L'élément de services de portail peut réessayer de télécharger la nouvelle image si le nombre MAX de réessais de séquence TFTP n'a pas été atteint. A la 16^{e} tentative de téléchargement de logiciel consécutive qui échoue, l'élément de services de portail DOIT se replier sur la dernière image connue qui fonctionnait et passer à un état opérationnel. Dans ce cas, l'élément de services de portail est tenu d'envoyer deux notifications: une afin de signaler que la limite MAX de réessais TFTP a été atteinte et une autre afin de signaler que l'image est endommagée. Immédiatement après que l'élément de services de portail a atteint l'état opérationnel, l'élément de services de portail DOIT adhérer aux exigences suivantes:

- docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom du fichier du logiciel qui a échoué à la mise à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à jour;
- docsDevSwOperStatus DOIT être à la valeur other{5};
- docsDevSwCurrentVer DOIT être la version actuelle de logiciel qui doit fonctionner dans le dispositif.

11.8.4.6.2 Téléchargement de logiciel initialisé par fichier de configuration

Le téléchargement de logiciel initalisé par fichier de configuration est déclenché dans un dispositif PS autonome par l'inclusion du paramètre de nom de fichier de mise à jour logicielle (TLV-9) ET du paramètre de serveur TFTP de mise à jour logicielle (TLV-21) dans son fichier de configuration PS. Un dispositif PS intégré DOIT ignorer les nuplets TLV-9 et TLV-21 s'ils sont présents dans son fichier de configuration car la mise à jour logicielle d'un dispositif PS intégré est commandée par le câblo-modem. Si le paramètre (TLV-9) de nom de fichier de configuration PS ET le paramètre (TLV-21) de serveur TFTP de mise à jour logicielle sont présents avec une valeur valide dans le fichier de configuration PS de l'élément de services de portail autonome ET si la valeur du

paramètre de nom de fichier de mise à jour logicielle (c'est-à-dire celle de l'objet docsDevSwFilename) ne correspond pas au nom du fichier d'image logicielle actuel, l'élément de services de portail DOIT demander le fichier spécifié au moyen du protocole TFTP, à partir du serveur dont l'adresse a été fournie dans le paramètre de serveur TFTP de mise à jour logicielle.

Si un élément PS de services de portail autonome reçoit un fichier de configuration PS dans lequel le paramètre TLV-9 de nom de fichier de configuration PS et le paramètre TLV-28 valuant l'objet docsDevSwFilename sont tous deux présents, ET si les valeurs de TLV-9 et de docsDevSwFilename sont différentes, l'élément PS DOIT rejeter le fichier de configuration PS, notifier un événement d'identificateur 73040102 (format/contenu de paramètre TLV invalide), préserver toutes les valeurs d'objet qui existaient avant la tentative de traitement de ce fichier de configuration erroné, et réinitialiser.

NOTE – L'adresse IP du serveur de logiciels est un paramètre distinct. S'il est présent, l'élément de services de portail DOIT essayer de télécharger le fichier spécifié à partir de ce serveur. S'il est absent, l'élément de services de portail DOIT essayer de télécharger le fichier spécifié à partir du serveur de fichiers de configuration.

Si l'élément de services de portail atteint le nombre maximal de réessais (nombre maximal de réessais = 3) à la suite de pertes d'alimentation ou réinitialisations multiples pendant une mise à jour initialisée par fichier de configuration, l'état de l'élément de services de portail DOIT adhérer aux exigences suivantes, après avoir été enregistré:

- docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom du fichier du logiciel qui a échoué au processus de mise à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à jour;
- docsDevSwOperStatus DOIT être à la valeur other{5};
- docsDevSwCurrentVer DOIT être la version actuelle de logiciel qui doit fonctionner dans le dispositif.

Si un élément de services de portail atteint le nombre maximal de réessais TFTP par l'envoi d'un total de 16 réessais consécutifs, l'élément de services de portail DOIT se replier sur la dernière image connue qui fonctionnait, passer à un état opérationnel et adhérer aux exigences suivantes:

- docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom du fichier du logiciel qui a échoué au processus de mise à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à jour;
- docsDevSwOperStatus DOIT être à la valeur failed{4};
- docsDevSwCurrentVer DOIT être la version actuelle de logiciel qui doit fonctionner dans le dispositif.

Après que l'élément de services de portail a achevé la mise à jour logicielle sécurisée qui a été initialisée par fichier de configuration, l'élément de services de portail DOIT réamorcer et devenir opérationnel avec l'image logicielle correcte. Après que l'élément de services de portail a été enregistré, l'objet:

- docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};
- docsDevSwFilename PEUT être le nom du fichier du logiciel fonctionnant actuellement dans le dispositif;
- docsDevSwServer PEUT être l'adresse du serveur TFTP contenant le logiciel qui fonctionne actuellement dans le dispositif;

- docsDevSwOperStatus DOIT être à la valeur completeFromProvisioning{2};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui doit fonctionner dans le dispositif.

11.8.4.7 Vérification de code

Pour un téléchargement sécurisé de logiciel, l'élément de services de portail DOIT exécuter les essais de vérification présentés dans le présent paragraphe. Si l'un des essais de vérification échoue, ou si une portion quelconque du fichier de code est rejetée à cause d'un format non valide, l'élément de services de portail DOIT immédiatement arrêter le processus de téléchargement, journaliser l'erreur si applicable, supprimer tous les résidus du processus jusqu'à cette étape et continuer de fonctionner avec son code existant.

Les essais de vérification suivants peuvent être effectués dans un ordre quelconque, pourvu que toutes les vérifications applicables présentées dans le présent paragraphe soient effectuées:

1) l'élément de services de portail DOIT valider les informations de signature du constructeur en vérifiant que la valeur [RFC 2315] signingTime est:
   a) égale ou supérieure à la valeur de l'objet codeAccessStart actuellement contenue dans l'élément de services de portail;
   b) égale ou supérieure à l'instant de début de validité du certificat CVC du constructeur;
   c) inférieure ou égale à la l'instant de fin de validité du certificat CVC du constructeur;
2) l'élément de services de portail DOIT valider le certificat CVC de constructeur en vérifiant que:
   a) le certificat CVC est exactement le même que spécifié dans le Tableau 11-8;
   b) le nom d'organisation titulaire du certificat CVC est identique au nom du constructeur actuellement mémorisé dans la mémoire de l'élément de services de portail;
   c) l'instant de début de validité du certificat CVC est égal ou supérieur à la valeur cvcAccessStart du constructeur actuellement contenue dans l'élément de services de portail;
3) l'élément de services de portail DOIT valider la signature du certificat au moyen de la clé publique d'autorité CA de certificat CVC du laboratoire CTL détenue par l'élément de services de portail. A son tour, la signature du certificat d'autorité CA de certificat CVC du laboratoire CTL est validée par la clé publique d'autorité CA radicale du certificat CVC du laboratoire CTL détenue par l'élément de services de portail. La vérification de la signature authentifiera l'origine de la clé publique de vérification de code (CVK) et confirmera la confiance dans la clé;
4) l'élément de services de portail DOIT vérifier la signature du fichier de code du constructeur:
   a) l'élément de services de portail DOIT exécuter un nouveau hachage SHA-1 sur le contenu signé. Si la valeur du condensé de message ne correspond pas au nouveau hachage, l'élément de services de portail DOIT considérer la signature figurant sur le fichier de code comme non valide;
   b) si la signature ne se vérifie pas, tous les composants du fichier de code (y compris l'image de code) et toutes les valeurs déduites du processus de vérification DOIVENT être rejetés et DEVRAIENT être immédiatement supprimés;
5) si la signature de constructeur est vérifiée et qu'un agent cosignataire signature soit requis:
   a) l'élément de services de portail DOIT valider les informations de signature du cosignataire en vérifiant que:
      i) les informations de signature du cosignataire sont incluses dans le fichier de code;

ii) la valeur de l'objet signingTime [RFC 2315] est égale ou supérieure à la valeur correspondante de l'objet codeAccessStart actuellement contenue dans l'élément de services de portail;

iii) la valeur de l'objet signingTime [RFC 2315] est égale ou supérieure à l'instant de début de validité du certificat CVC correspondant;

iv) la valeur de l'objet signingTime [RFC 2315] est inférieure ou égale à l'instant de fin de validité du certificat CVC correspondant;

b) l'élément de services de portail DOIT valider le certificat CVC de cosignataire en vérifiant que:

i) le nom d'organisation titulaire du certificat CVC est identique au nom d'organisation de cosignataire actuellement mémorisé dans la mémoire de l'élément de services de portail;

ii) le certificat CVC est exactement le même que spécifié dans le Tableau 11-9 ou 11-10, selon le type de cosignataire (laboratoire CTL ou fournisseur de services);

ii) l'instant de début de validité du certificat CVC est égal ou supérieur à la valeur de l'objet cvcAccessStart actuellement contenue dans l'élément de services de portail pour le nom d'organisation titulaire correspondant;

c) l'élément de services de portail DOIT valider la signature du certificat au moyen de la clé publique d'autorité CA de certificat CVC du laboratoire CTL détenue par l'élément de services de portail. A son tour, la signature du certificat d'autorité CA de certificat CVC du laboratoire CTL est validée par la clé publique d'autorité CA radicale du certificat CVC du laboratoire CTL détenue par l'élément de services de portail. La vérification de la signature authentifiera l'origine de la clé publique de vérification de code du cosignataire (CVK) et confirmera la confiance dans la clé;

d) l'élément de services de portail DOIT vérifier la signature du fichier de code du cosignataire;

e) l'élément de services de portail DOIT exécuter un nouveau hachage SHA-1 sur le contenu signé. Si la valeur du condensé de message ne correspond pas au nouveau hachage, l'élément de services de portail DOIT considérer la signature sur le fichier de code comme non valide;

f) si la signature ne se vérifie pas, tous les composants du fichier de code (y compris l'image de code) et toutes les valeurs déduites du processus de vérification DOIVENT être rejetés et DEVRAIENT être immédiatement supprimés;

6) si la signature du constructeur et (facultativement) celle du cosignataire sont vérifiées, l'image de code peut être considérée comme fiable et l'installation peut se poursuivre. Avant d'installer l'image de code, tous les autres composants du fichier de code et toutes les valeurs déduites du processus de vérification, à l'exception des valeurs signingTime [RFC 2315] et des valeurs de début de validité du certificat CVC, DEVRAIENT être immédiatement supprimés;

7) si l'installation de code échoue, l'élément de services de portail DOIT ignorer les valeurs de l'élément signingTime [RFC 2315] et les valeurs de début de validité de certificat CVC qu'il vient de recevoir dans le fichier de code;

8) quand l'installation de code est réussie, l'élément de services de portail DOIT mettre à jour les commandes variables dans le temps du constructeur avec les valeurs issues des informations de signature et de certificat CVC du constructeur:

a) mettre à jour la valeur actuelle de l'objet codeAccessStart avec la valeur de l'élément signingTime [RFC 2315];

b) mettre à jour la valeur actuelle de l'objet cvcAccessStart avec la valeur de début de validité du certificat CVC;

9) quand l'installation de code est réussie et que le fichier de code a été cosigné, l'élément de services de portail DOIT mettre à jour les commandes du cosignataire qui varient dans le temps avec les valeurs issues des informations de signature et de certificat CVC du cosignataire:

a) mettre à jour la valeur actuelle de l'objet codeAccessStart avec la valeur de l'élément signingTime [RFC 2315];

b) mettre à jour la valeur actuelle de l'objet cvcAccessStart avec la valeur de début de validité du certificat CVC.

11.8.4.8 Codes d'erreur

Des codes d'erreur sont définis afin de refléter les états d'échec possibles pendant le processus de vérification de code de téléchargement sécurisé de logiciel.

1) Commandes de fichier de code inappropriées:

a) le nom d'organisation titulaire du certificat CVC pour le constructeur ne correspond pas au nom de constructeur de l'élément de services de portail;

b) le nom d'organisation titulaire du certificat CVC pour l'agent cosignataire de code ne correspond pas à l'agent cosignataire de code actuel de l'élément de services de portail;

c) la valeur signingTime [RFC 2315] du constructeur est inférieure à la valeur codeAccessStart actuellement contenue dans l'élément de services de portail;

d) la valeur de l'instant de début de validité [RFC 2315] du constructeur est inférieure à la valeur de l'objet cvcAccessStart actuellement contenue dans l'élément de services de portail;

e) l'instant de début de validité du certificat CVC de constructeur est inférieur à la valeur de l'objet cvcAccessStart actuellement contenue dans l'élément de services de portail;

f) la valeur signingTime [RFC 2315] du constructeur est inférieure à l'instant de début de validité du certificat CVC;

g) l'extension d'utilisation de clé étendue est manquante ou est inappropriée dans le certificat CVC du constructeur;

h) la valeur signingTime [RFC 2315] du cosignataire est inférieure à la valeur codeAccessStart actuellement contenue dans l'élément de services de portail;

i) la valeur de l'instant de début de validité [RFC 2315] du cosignataire est inférieure à la valeur de l'objet cvcAccessStart actuellement contenue dans l'élément de services de portail;

j) l'instant de début de validité du certificat CVC de cosignataire est inférieur à la valeur de l'objet cvcAccessStart actuellement contenue dans l'élément de services de portail;

k) la valeur signingTime [RFC 2315] du cosignataire est inférieure à l'instant de début de validité du certificat CVC;

l) l'extension d'utilisation de clé étendue est manquante ou inappropriée dans le certificat CVC de cosignataire;

2) échec de validation du certificat CVC du constructeur du fichier de code;

3) échec de validation de la signature CVS du constructeur du fichier de code;

4) échec de validation du certificat CVC du cosignataire du fichier de code;

5) échec de validation de la signature CVS du cosignataire du fichier de code;

6) format de certificat CVC de fichier de configuration du dispositif PS inapproprié (par exemple attribut d'utilisation de clé manquant ou inapproprié);

7) échec de validation du certificat CVC d'un fichier de configuration;

8) format inapproprié du certificat CVC par protocole SNMP:

   a) le nom d'organisation titulaire du certificat CVC pour le constructeur ne correspond pas au nom du constructeur du dispositif;

   b) le nom d'organisation titulaire du certificat CVC pour l'agent cosignataire de code ne correspond pas à l'agent cosignataire de code actuel de l'élément de services de portail;

   c) l'instant de début de validité du certificat du certificat CVC est inférieur ou égal à la valeur correspondante de l'objet cvcAccessStart du titulaire actuellement contenue dans l'élément de services de portail;

   d) attribut d'utilisation de clé manquant ou inapproprié;

9) échec de validation du certificat CVC par protocole SNMP.

11.8.4.9 Repli du logiciel

Le repli du logiciel définit le processus de retrait de la version mise à jour du téléchargement d'image logicielle, donc de retour du dispositif IPCable2Home à son état antérieur exact.

Quand l'élément de services de portail reçoit un fichier de code avec un instant de signature qui est antérieur à l'instant de signature qu'il a dans sa mémoire, le dispositif DOIT mettre à jour sa mémoire interne avec la valeur reçue.

Etant donné que l'élément de services de portail n'acceptera pas de fichiers de code avec un instant de signature antérieur à cette valeur en mémoire interne afin de mettre à jour un dispositif avec un nouveau fichier de code sans refuser l'accès aux anciens fichiers de code, le signataire (par exemple le constructeur, le câblo-opérateur, le laboratoire CTL) peut choisir de ne pas mettre à jour l'instant de signature. De cette façon, de multiples fichiers de code ayant le même instant de signature de code permettent à un opérateur de replier librement une image de code de dispositif sur une version antérieure (c'est-à-dire jusqu'à ce que le certificat CVC soit mis à jour). Cela présente un certain nombre d'avantages pour le câblo-opérateur, mais ces avantages seront pesés au regard des risques d'attaque par réexécution d'un fichier de code.

Une autre approche consisterait à signer le précédent fichier de code avec un instant de signature égal à ou supérieur à l'instant de signature de la dernière mise à jour.

11.9 Sécurité du fichier de configuration du dispositif PS en mode de préconfiguration DHCP

11.9.1 Fichier de configuration de la sécurité: objectifs infrastructurels

Les objectifs de sécurisation du fichier de configuration sont les suivants:

- offrir un tunnel authentifié entre le dispositif PS client et le serveur HTTPS afin d'assurer que les fichiers de configuration sont sécurisés à partir du câblo-opérateur jusqu'au dispositif PS. Une vérification d'intégrité est automatiquement incluse quand un message est authentifié;
- réduire la possibilité d'interception illicite lors de la configuration du pare-feu et du dispositif PS, par chiffrement des fichiers de configuration en cours de transport;
- réduire le risque de téléchargement de fichier de configuration illicite vers le dispositif PS par une source illicite.

11.9.2 Fichier de configuration de la sécurité: directives de conception du système

Voir le Tableau 11-25.

Tableau 11-25/J.192 – Sécurité: directives de conception du système

Référence	Directives
SEC14	Le câblo-opérateur possédera la capacité d'authentifier et (facultativement) de chiffrer le transport de fichiers de configuration pour le dispositif PS ou le dispositif de pare-feu.

11.9.3 Fichier de configuration de la sécurité: description du système

En mode de préconfiguration DHCP, le câblo-opérateur peut choisir d'activer la sécurité pour le téléchargement du fichier de configuration. Dans ce paragraphe, le terme *fichier de configuration* renvoie au fichier de configuration du dispositif PS ou au fichier de configuration du pare-feu. La sécurité est assurée par l'ouverture d'une session de sécurité TLS entre le dispositif PS et le serveur HTTPS. Le modèle IPCable2Home exige que le dispositif PS comprenne cette option de sécurité et utilise la sécurité TLS dans la séquence de préconfiguration afin d'offrir une session sécurisée entre le serveur HTTPS et le dispositif PS aux fins de téléchargement du fichier de configuration du dispositif PS et du fichier de configuration du pare-feu, de façon fiable. La sécurité TLS offre l'authentification et le chiffrement pour la session, comme configurés par le câblo-opérateur. La session est fermée par l'envoi du message de préconfiguration achevé en tant que notification au système Syslog et/ou NMS. Le déclenchement, la gestion et le contenu du téléchargement du fichier de configuration restent conformes aux normes industrielles quand la sécurité TLS est située dans une couche inférieure au protocole HTTPS. Le modèle IPCable2Home spécifie les exigences relatives à une session de plainte en matière de sécurité TLS [RFC 2246]. Les options de sécurité TLS sont renforcées afin de créer un ensemble minimal de comportements d'interfonctionnement pour le dispositif PS. Le flux de préconfiguration avec protocole HTTP/TLS est décrit en détail dans le § 13.

Le protocole TLS offre un tunnel de transport chiffré et authentifié pour toute application située au-dessus de la couche TLS dans la pile du modèle ISO. Le protocole HTTP lui-même n'est pas affecté par le niveau de la couche TLS. Les couches indiquées en caractères italiques et soulignés dans la pile sont chiffrées pour un paquet de données normal du protocole TLS. Le protocole HTTP, qui normalement repose sur le protocole TCP, repose directement sur le protocole TLS. Voir le Tableau 11-26.

Tableau 11-26/J.192 – Chiffrement du protocole TLS

Fichier de configuration données (charge utile)
HTTP
TLS
TCP
IP
MAC
PHY

11.9.4 Fichier de configuration de la sécurité: exigences

Le dispositif PS DOIT implémenter le protocole de sécurité de la couche Transport (TLS) comme défini par [RFC 2246], Version 1.0 du protocole TLS, avec les exceptions énumérées dans la présente Recommandation. Les exceptions indiquées dans la présente Recommandation sont destinées à simplifier les exigences nécessaires aux fins de l'implémentation et des essais. Certaines de ces exceptions imposent un ensemble minimal d'exigences qui s'alignent déjà avec d'autres techniques utilisées dans l'industrie du câble. Les exigences ainsi imposées garantiront que le dispositif PS offre un niveau cohérent de performance pour les câblo-opérateurs. Le présent paragraphe contribue également à supprimer toute ambiguïté et définissent des processus qui ne sont pas définis dans les documents RFC mais qui sont requis aux fins du modèle IPCable2Home. Cela est particulièrement vrai en cas de traitement des échecs.

NOTE – L'algorithme de caractéristique de compression du protocole TLS ne sera pas utilisé.

La version 1.0 du protocole TLS (SSL3, TLSv1) DOIT être prise en charge. Les versions antérieures du protocole TLS NE DOIVENT PAS être prises en charge par le dispositif PS. Celui-ci DOIT ignorer les messages provenant du serveur s'il essaye d'utiliser de précédentes versions du protocole TLS.

11.9.4.1 Déclenchement du protocole TLS

Afin de déclencher un téléchargement sécurisé du fichier de configuration en mode de préconfiguration DHCP, le message ACK du protocole DHCP contiendra l'adresse IP du serveur HTTPS dans le champ "siaddr". Le message ACK du protocole DHCP va également contenir l'option 72 avec l'adresse IP du serveur HTTPS. S'il y a correspondance entre l'adresse IP contenue dans le champ "siaddr" et la première adresse IP contenue dans l'option 72, le dispositif PS DOIT établir une session de sécurité TLS avec le serveur HTTPS à l'adresse IP indiquée dans le message ACK, avant de demander le fichier de configuration. Le dispositif PS DOIT télécharger le fichier de configuration au moyen du protocole HTTP/TLS si la première adresse IP contenue dans l'option TLV 72 correspond à cette adresse IP dans le champ "siaddr" du message DHCP ACK. Si le dispositif PS ne reçoit pas de correspondance dans le message ACK du protocole DHCP, le dispositif PS NE DOIT PAS lancer de session de sécurité TLS, les exigences dans le présent paragraphe ne sont pas applicables et le dispositif PS client DOIT utiliser le mode de préconfiguration DHCP avec le processus de téléchargement TFTP spécifié. Le diagramme de fluence de préconfiguration et la table de description sont spécifiés dans le § 13. Si l'option 66 est incluse ainsi que l'option 72 et si l'adresse IP contenue dans l'option 72 correspond à l'adresse IP contenue dans le champ "siaddr", le dispositif PS DOIT lancer une session de sécurité TLS vers le serveur HTTPS et NE DOIT PAS lancer de téléchargement à partir du serveur TFTP indiqué dans l'option 66.

Si le dispositif PS reçoit les informations nécessaires pour lancer le téléchargement par protocole HTTPS d'un fichier de configuration du pare-feu comme spécifié dans le § 7, alors ce dispositif PS devra déterminer s'il a besoin de continuer ou d'ouvrir une session de protocole TLS avec un serveur HTTPS.

11.9.4.2 Conditions préalables à une session de protocole TLS

Avant d'établir une session de sécurité TLS, le dispositif PS client DOIT synchroniser son horloge avec le serveur TOD. Les détails sont spécifiés dans le § 13.

De plus, le dispositif PS client DOIT établir la connexion TCP/IP au serveur HTTPS avant d'envoyer le préappel "ClientHello" du protocole TLS. Une fois que le téléchargement du fichier de configuration est achevé, le dispositif PS DOIT fermer la connexion TCP/IP. Le dispositif PS client DOIT utiliser le port TCP #443 spécifié par les normes de l'autorité IANA afin de se connecter au serveur distant HTTP/TLS. Si le dispositif PS n'est pas en mesure d'établir correctement une connexion TCP/IP, il DOIT journaliser l'événement 68002000 puis relancer la préconfiguration

conformément à la procédure de réessai définie dans le § 7.4.4.2.4: "Fonctionnement après déclenchement", afin de traiter les réessais.

11.9.4.3 Messages TLS

Sauf indication contraire, tous les messages sont conformes à [RFC 2246].

11.9.4.3.1 ClientHello

Le dispositif PS client DOIT envoyer un préappel "ClientHello" au serveur distant HTTP/TLS afin de lancer la séquence de dialogue initial du protocole TLS. Après que le message ClientHello initial a été envoyé au serveur distant HTTP/TLS, si la session de protocole TLS n'est pas établie après 5 tentatives, avec 30 secondes autorisées pour chaque tentative, le dispositif PS DOIT échouer à la session et envoyer l'événement 68002100.

11.9.4.3.2 Traitement par le dispositif PS des messages de serveur distant

Le dispositif PS DOIT être capable de traiter les messages de serveur distant comme défini dans [RFC 2246], avec les exceptions suivantes:

- HelloRequest: le dispositif PS DOIT ignorer les messages HelloRequest issus d'un serveur distant. Cela empêche le dispositif PS de répondre à des demandes illégales issues de serveurs HTTPS. Le processus HTTP/TLS ne peut être lancé que si les options DHCP appropriées sont configurées par le câblo-opérateur. Cela implique que le protocole DHCP soit considéré comme fiable, bien qu'il ne soit pas sécurisé par IPCable2Home;
- ServerCertificate: le serveur HTTPS est censé envoyer son certificat de dispositif à l'élément PS dans le message ServerCertificate. En plus des exigences [RFC 2246] relatives à ce message, le dispositif PS client DOIT valider et vérifier le certificat de serveur HTTPS. Si l'authentification du certificat de serveur HTTPS échoue, la session de protocole TLS est considérée comme un échec et le dispositif PS DOIT envoyer l'événement 68002200 avec le code d'erreur défini dans [RFC 2246].

11.9.4.3.3 Message ClientCertificate

Lorsque cela est demandé par le serveur HTTPS, le dispositif PS DOIT envoyer son certificat d'élément de services de portail au serveur HTTPS, ainsi que le certificat CA du constructeur émetteur, dans le message Client Certificate. On suppose que le serveur HTTPS va valider et vérifier les certificats de client PS avant de procéder au dialogue initial. Si les certificats du dispositif PS ne sont pas correctement authentifiés par le serveur distant, le dispositif PS DOIT traiter le message d'alerte reçu comme une alerte fatale et envoyer l'événement 68002200 avec la valeur appropriée du code d'erreur, extraite de [RFC 2246], puis relancer la préconfiguration conformément à la procédure de réessai définie dans le § 7.4.4.2.4: "Fonctionnement après déclenchement".

11.9.4.4 Suites chiffrantes et compression en protocole TLS

Dans le message ClientHello, la suite chiffrante demandée DOIT être énumérée. La prise en charge de la suite chiffrante requise est un sous-ensemble de [RFC 2246] afin d'assurer la compatibilité avec la technique déjà utilisée dans l'industrie du câble. Le câblo-opérateur aura besoin de choisir l'algorithme approprié de chiffrement et d'authentification sur le serveur HTTPS afin de le communiquer au dispositif PS qui respecte le modèle de sécurité pour cet opérateur. Les suites chiffrantes requises dans la présente Recommandation sont un sous-ensemble de celles qui sont disponibles et le dispositif PS peut prendre en charge des suites chiffrantes additionnelles.

Les algorithmes cryptographiques suivants DOIVENT être pris en charge par le dispositif PS.

- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA

- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA.

La caractéristique de compression du protocole TLS n'est pas requise. Donc, le dispositif PS client DOIT utiliser la valeur "compressionMethod.null" en tant que type de compression.

11.9.4.5 Fermeture de session TLS

Si le dispositif PS est tenu de télécharger un fichier distinct de configuration du pare-feu immédiatement après que le fichier de configuration du dispositif PS a été téléchargé et si le fichier de configuration du pare-feu doit être téléchargé à partir du même serveur HTTPS que le fichier de configuration du dispositif PS l'a été, la session de protocole TLS est censée rester active. Le dispositif PS DOIT garantir que le protocole TLS et la session TCP/IP correspondante sont fermés dans chaque serveur HTTPS après que:

- le fichier de configuration du dispositif PS a été téléchargé, si et seulement s'il y n'a aucun fichier de configuration du pare-feu à télécharger à partir du même serveur HTTPS, immédiatement après que le fichier de configuration du dispositif PS a été traité;
- le fichier de configuration du pare-feu a été téléchargé et traité.

11.9.4.6 Evénements du protocole TLS

Le document [RFC 2246] définit un protocole d'alerte afin de manipuler les fermetures et les erreurs du protocole TLS. Les alertes et erreurs TLS DOIVENT être prises en charge et utilisées comme défini dans [RFC 2246], à l'exception de l'alerte de type "decompression_failure (30)" qui ne sera pas utilisée car la compression n'est pas prise en charge. Toutes les alertes TLS DOIVENT être mémorisées par le dispositif PS au moyen de l'événement 68002200 avec la valeur appropriée du code d'erreur définie dans [RFC 2246], insérée dans le champ <P1> de texte d'événement. Les erreurs associées aux certificats DOIVENT être traitées comme étant critiques car le dispositif PS repose sur l'authentification du serveur.

Si le dispositif PS client n'a pas reçu de message à partir du serveur distant HTTP/TLS en réponse à un quelconque message TLS émis après 5 tentatives, avec 30 secondes autorisées pour chaque tentative, la connexion TLS est considérée comme un échec et le dispositif PS DOIT envoyer l'événement 68002100.

11.9.4.7 Téléchargement et événements en protocole HTTP

Le transfert par protocole HTTP ne DOIT être lancé qu'après l'achèvement du dialogue initial TLS. Le dispositif PS DOIT communiquer au serveur distant HTTP/TLS au moyen du protocole HTTP normal, comme défini par [RFC 2616]. Le dispositif PS client DOIT envoyer au serveur une demande de fichier de configuration du dispositif PS ou de configuration de pare-feu selon la version HTTP 1.1. Le nom de fichier de configuration du dispositif PS utilisé dans la requête HTTP "GET Request" DOIT être le nom de fichier que le dispositif PS a reçu dans le message ACK du protocole DHCP. Le nom du fichier de configuration du pare-feu utilisé dans la requête HTTP "GET Request" DOIT être le nom de fichier que le dispositif PS a reçu dans le champ "nom de fichier" du fichier de configuration du dispositif PS, ou qu'il a reçu par requête SET (mise à jour) du protocole SNMP.

Le dispositif PS client DOIT manipuler tous les messages de description d'état conformément au [RFC 2616]. Si le dispositif PS client reçoit un message HTTP de description d'état indiquant que le téléchargement HTTP ne peut pas être achevé, le dispositif PS DOIT échouer à la session et envoyer l'événement 68003000 avec la valeur appropriée du code d'erreur conformément au [RFC 2616] puis relancer la préconfiguration selon la procédure de réessai définie au § 7.4.2.4: "Fonctionnement après déclenchement", afin de traiter les réessais.

NOTE – Une fois que le fichier de configuration a été téléchargé avec succès, le dispositif PS DOIT envoyer l'événement 68003200.

11.10 Sécurité physique

Le dispositif PS est tenu de conserver, dans sa mémoire non volatile, des clés et d'autres variables cryptographiques associées à la sécurité du réseau. Le dispositif PS DOIT interdire l'accès physique illicite à ce matériel cryptographique.

Le niveau de protection physique des matériaux de verrouillage par clés requis pour le dispositif PS est spécifié en termes des niveaux de sécurité définis dans le document FIPS PUBS 140-2, "Exigences de sécurité pour modules cryptographiques". En particulier, le dispositif PS DOIT satisfaire les exigences du niveau de sécurité 1 du document FIPS PUBS 140-2.

Le niveau de sécurité 1 du document FIPS PUBS 140-2 exige une protection physique minimale par l'utilisation d'enveloppes de classe industrielle et de procédés logiciels recommandés.

11.11 Algorithmes cryptographiques

11.11.1 SHA-1

L'implémentation par le dispositif PS du codage SHA-1 DOIT utiliser l'algorithme de hachage SHA-1 qui est défini dans [FIPS 180-1].

12 Processus de gestion

12.1 Introduction/Aperçu général

Le présent paragraphe offre des exemples de traitement associé à l'utilisation des utilitaires décrits dans le § 6 (Utilitaires de gestion) et des traitements supplémentaires qui facilitent d'autres fonctions de gestion obligatoires, définies dans la présente Recommandation. L'accès à une base de données PS et d'autres opérations du dispositif PS au portail de gestion IPCable2Home (portail CMP) sont décrites dans le § 6. Les règles typiques d'accès à une base MIB sont présentées dans le § 6.3.3.1.4.2.

Les processus relatifs à la gestion et d'autres processus descriptifs sont présentés pour les scénarios suivants:

- processus d'utilitaire de gestion:
  - fonctionnement du portail CTP:
    - utilitaire de vitesse de connexion;
    - utilitaire de sondage par écho;
- fonctionnement des services de portail:
  - accès à une base de données PS;
  - reconfiguration:
    - téléchargement de logiciel des services de portail;
    - téléchargement du fichier de configuration du dispositif PS;
- accès de base MIB:
  - configuration de modèle VACM;
  - configuration de messagerie d'événements de gestion:
    - fonctionnement de la notification d'événement de portail CMP;
    - fonctionnement du ralentissement et de la limitation des événements au portail CMP.

12.1.1 Objectifs

Le présent paragraphe est principalement composé d'un texte informatif destiné à faciliter la compréhension et qui ne contient pas d'exigences. Les exemples décrivent comment les utilitaires de gestion servent à accomplir des fonctions de gestion typiques. Des organigrammes séquentiels des processus de gestion supplémentaires (c'est-à-dire non définis dans le § 6) sont également fournis, y compris les processus de gestion ou les étapes des processus associés à l'utilisation des utilitaires de gestion obligatoires. Tous les processus représentés impliquent l'interaction de l'élément de services de portail avec les systèmes de tête de réseau.

12.2 Processus d'utilitaire de gestion

Les processus d'utilitaire de gestion sont ceux qui sont associés aux utilitaires de gestion obligatoires définis dans le § 6.

12.2.1 Fonctionnement du portail CTP

Le portail d'essais IPcable2Home (CTP) offre des capacités d'essai de vitesse de connexion et d'essai de sondage par écho, décrites dans les § 6.4.3.1 et 6.4.3.2, respectivement.

12.2.1.1 Essai à distance de vitesse de connexion

L'essai à distance de vitesse de connexion peut servir à valider les niveaux de performance, à identifier d'éventuelles erreurs de configuration et à déterminer d'autres caractéristiques visant les performances:

1) le système de gestion de réseau (NMS) commence l'essai en initialisant les paramètres d'essai et en réglant le fanion de début d'essai, par commande SET (demande de mise à jour) du protocole SNMP;
2) l'agent SNMP du portail CMP met à jour la base de données PS avec les paramètres d'essai et notifie au portail CTP qu'il y a lieu de commencer l'essai;
3) le portail CTP interroge la base de données PS concernant les paramètres d'essai;
4) le portail CTP envoie une rafale de paquets UDP vers le port 7 du dispositif IP de réseau local spécifié. Le port 7 est réservé au service d'écho;
5) le dispositif IP de réseau local cible renvoie simplement en écho, au portail CTP, la charge utile de paquet UDP;
6) une fois que tous les paquets ont été reçus ou que la période de temporisation de l'essai a expiré, le portail CTP met à jour la base de données PS avec les résultats de l'essai et règle le fanion d'essai terminé;
7) le système NMS vérifie que la commande est achevée en vérifiant que la valeur de l'objet Status est "complete" (terminé);
8) le système NMS demande les résultats des essais par la requête GET (obtenir) du protocole SNMP;
9) l'agent SNMP du portail CMP interroge la base de données PS concernant les résultats des essais et les signale dans la réponse au message GET du protocole SNMP. Si l'essai n'est pas terminé, les données d'essai indiqueront que l'essai est toujours en cours. Le système NMS doit répéter la requête GET (obtenir) du protocole SNMP jusqu'à ce que les résultats des essais indiquent que l'essai s'est achevé.

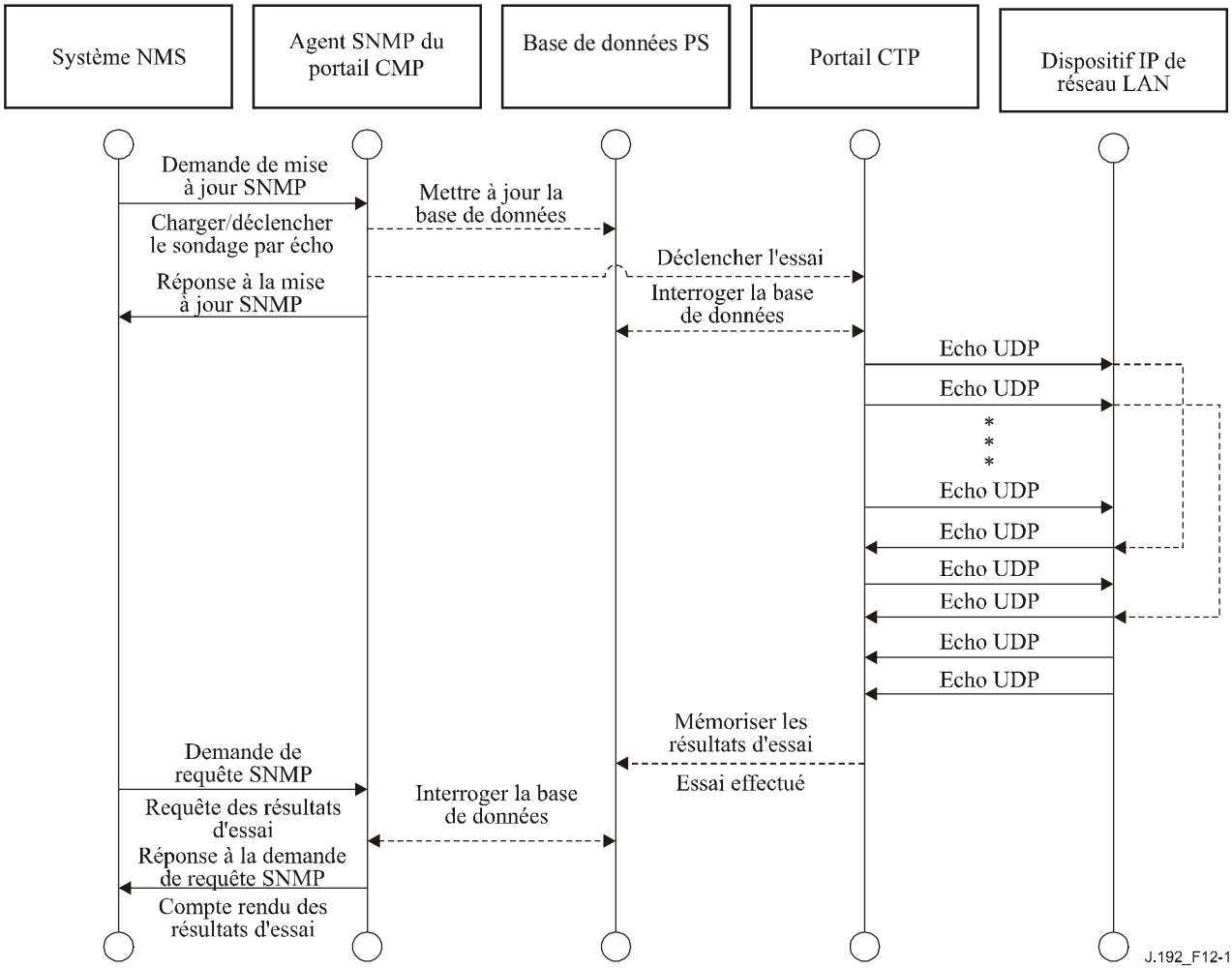


Figure 12-1/J.192 – Processus de l'utilitaire de vitesse de connexion – Diagramme séquentiel

12.2.1.2 Processus de l'utilitaire de sondage par écho

L'utilitaire de sondage par écho peut servir à la validation de l'état de connexité, à la détermination des niveaux de performance et à l'identification d'éventuelles erreurs de configuration.

1) Le système NMS commence l'essai en initialisant les paramètres d'essai et en réglant le fanion de début d'essai, par requête SET (mise à jour) du protocole SNMP;

2) l'agent SNMP du portail CMP met à jour la base de données PS avec les paramètres d'essai et signale au portail CTP qu'il y a lieu de commencer l'essai;

3) le portail CTP interroge la base de données PS pour les paramètres d'essai;

4) le portail CTP envoie un paquet de demande d'écho ICMP au dispositif IP de réseau local spécifié;

5) le dispositif IP de réseau local cible renvoie une réponse d'écho ICMP;

6) le portail CTP met à jour la base de données PS avec les résultats de l'essai et règle le fanion d'essai terminé;

7) le système NMS vérifie que la commande est exécutée en vérifiant que la valeur de l'objet Status est "complete" (terminé);

8) le système NMS demande les résultats des essais par la requête GET (obtenir) du protocole SNMP;

9) l'agent SNMP du portail CMP interroge la base de données PS au sujet des résultats des essais et les signale dans sa réponse au message GET du protocole SNMP. Si l'essai n'est pas terminé, les données d'essai indiqueront que l'essai est toujours en cours. Le système NMS doit répéter la requête GET (obtenir) du protocole SNMP jusqu'à ce que les résultats des essais indiquent que l'essai est achevé.

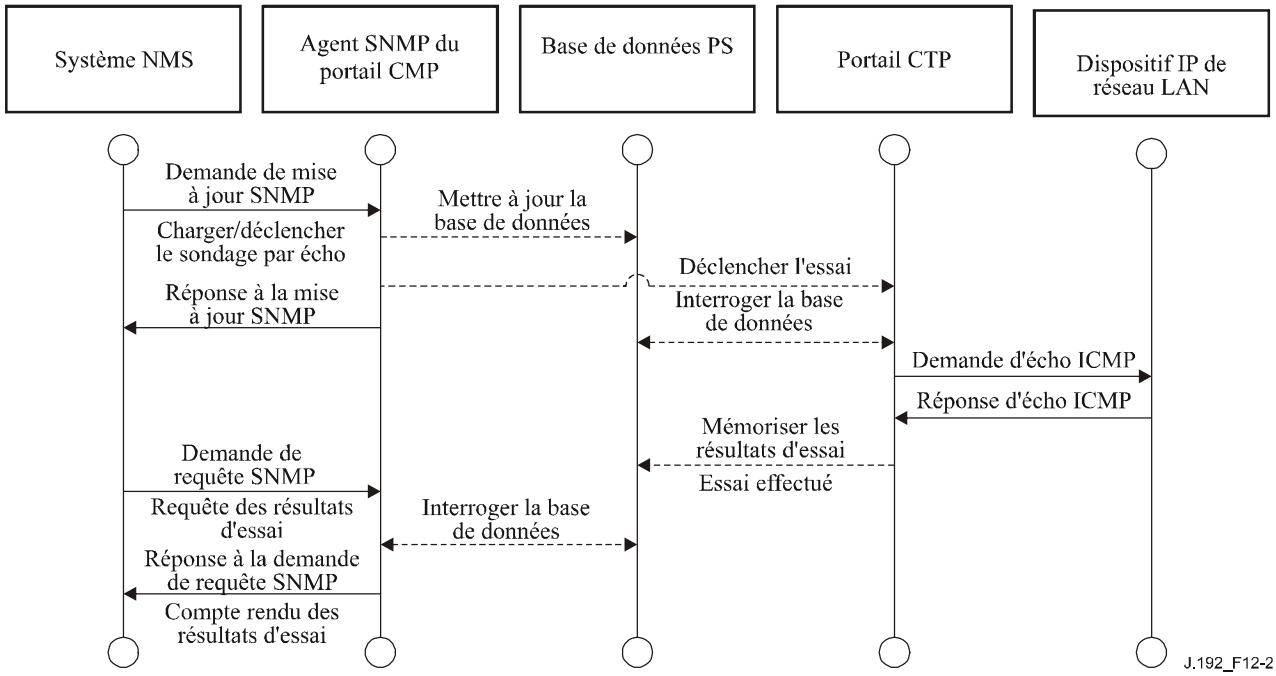


Figure 12-2/J.192 – Processus de l'utilitaire de sondage par écho – Diagramme séquentiel

12.3 Fonctionnement des services de portail

Le portail de gestion IPCable2Home (portail CMP) offre l'accès à la base de données PS par l'interface PS WAN-Man, comme décrit dans le § 6. La séquence de messages pour un fonctionnement typique d'accès à une base de données PS à partir de l'interface PS WAN-Man est décrite ci-dessous.

12.3.1 Accès à une base de données PS

Les paramètres de configuration et de gestion mémorisés dans la base de données PS font l'objet d'un accès par le système NMS via les bases MIB du protocole SNMP. Ces paramètres sont récupérés au moyen des messages GetRequest (requête), GetNext-Request (requête suivante) et Get-Bulk (requête générale) du protocole SNMP, envoyés par le système NMS avec l'adresse de l'interface PS WAN-Man en tant qu'adresse de destination. Les paramètres peuvent être modifiés et des actions (comme les utilitaires de vitesse de connexion et de sondage par écho) peuvent être exécutées par l'envoi, à partir du système NMS, du message SNMP de requête de mise à jour (Set-Request) avec les paramètres appropriés, vers l'adresse de l'interface PS WAN-Man.

La Figure 12-3 décrit les séquences de messages de gestion pour un accès typique à une base de données PS à partir de l'interface PS WAN-Man. Les séquences de messages suivantes impliquent qu'une liaison SNMPv3 sécurisée a été établie:

1) le système NMS lit les données à partir de la base de données PS au moyen de la requête "GET Request" du protocole SNMP, qui énumère les objets spécifiques que le système NMS souhaite extraire de la base de données;

2) l'agent SNMP du portail CMP interroge la base de données PS concernant les paramètres spécifiés;

3) l'agent SNMP du portail CMP signale le données au système NMS avec la réponse "GET Response" du protocole SNMP.

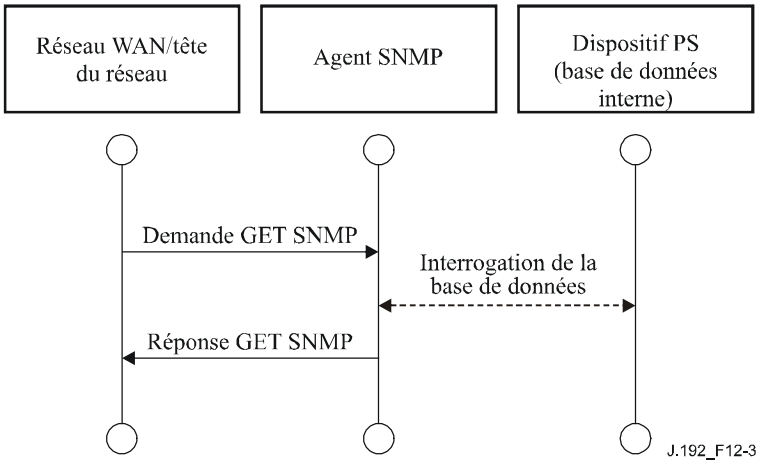


Figure 12-3/J.192 – Accès à une base de données PS à partir de l'interface PS WAN-Man – Diagramme séquentiel

12.3.2 Reconfiguration

12.3.2.1 Téléchargement de logiciel des services de portail

La Figure 12-4 décrit un processus de téléchargement de logiciel/micrologique pour un dispositif PS en mode de préconfiguration SNMP, qui est déclenché par le système NMS. Le dispositif PS est informé de l'adresse lui permettant d'obtenir le nouveau fichier de code logiciel. Une fois que le téléchargement du fichier de code est achevé, le dispositif PS contrôle l'image pour chercher toute corruption qui aurait pu se produire pendant le téléchargement. L'authentification est effectuée afin de vérifier que le fichier de code peut être considéré comme fiable. Après cette étape, un réamorçage du système est effectué.

Après le réamorçage, le dispositif PS reprend son fonctionnement avec la nouvelle image logicielle. Le dispositif PS peut avoir besoin d'être reconfiguré après la mise à jour logicielle et les interfaces avec un réseau régional peuvent avoir besoin d'être ré-préconfigurées (non représenté). Si le dispositif PS n'accepte pas la nouvelle image logicielle, il revient à la précédente version (sauvegardée) du logiciel et signale les résultats au système NMS.

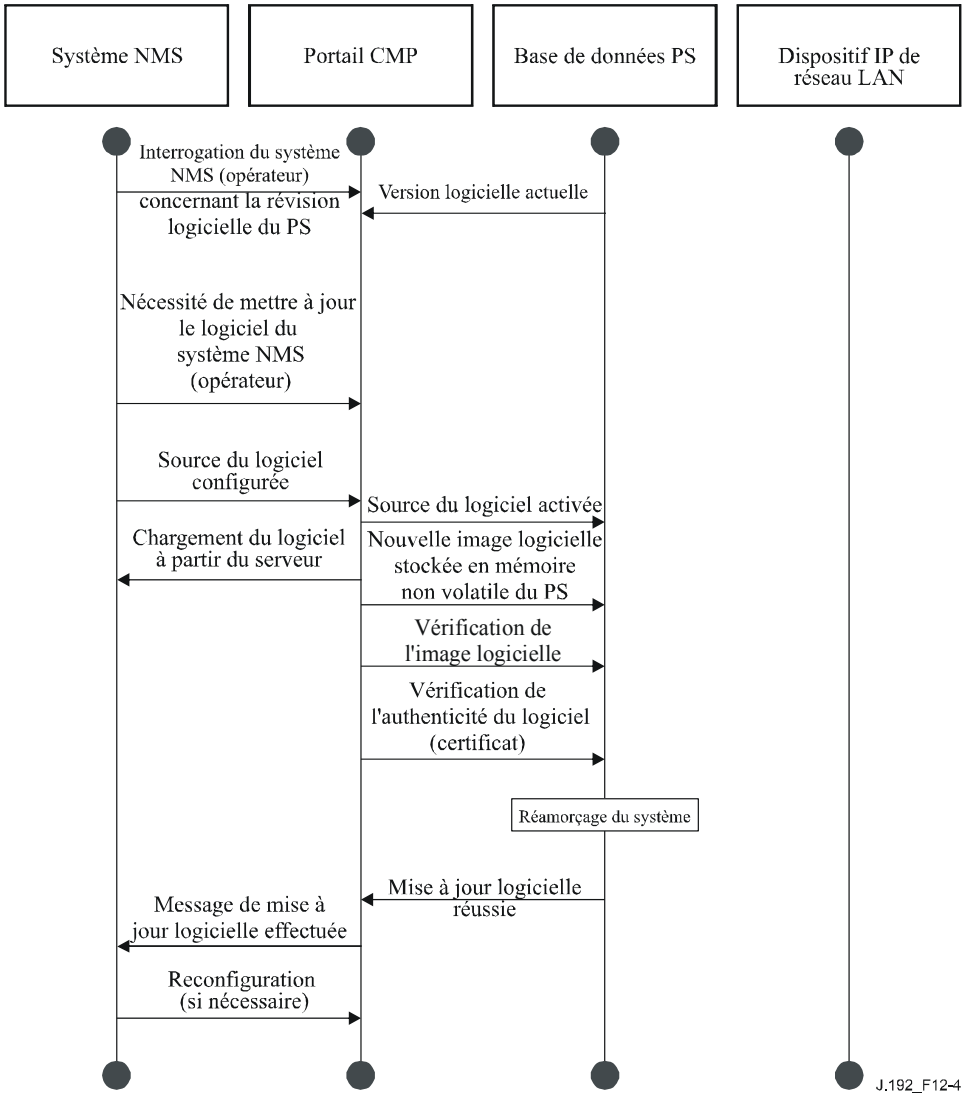


Figure 12-4/J.192 – Téléchargement de logiciel des services de portail – Diagramme séquentiel

12.3.2.2 Téléchargement du fichier de configuration du dispositif PS

La Figure 12-5 décrit la reconfiguration d'un dispositif PS en mode de préconfiguration SNMP par téléchargement du fichier de configuration. Ce processus est déclenché par le système NMS. Le fichier de configuration du dispositif PS est donné au PS par inscription du serveur de fichiers et du nom de fichier dans le dispositif PS et par déclenchement du téléchargement du fichier par le dispositif PS. Une fois que le fichier de configuration a été chargé, les commandes qu'il contient sont interprétées. Si l'une quelconque des commandes n'est pas interprétée ou n'est pas applicable, elle est sautée et un événement est produit. Quand le dispositif PS a achevé le traitement du fichier de configuration, il enregistre le nombre de nuplets TLV traités et sautés dans les objets de base MIB appropriés.

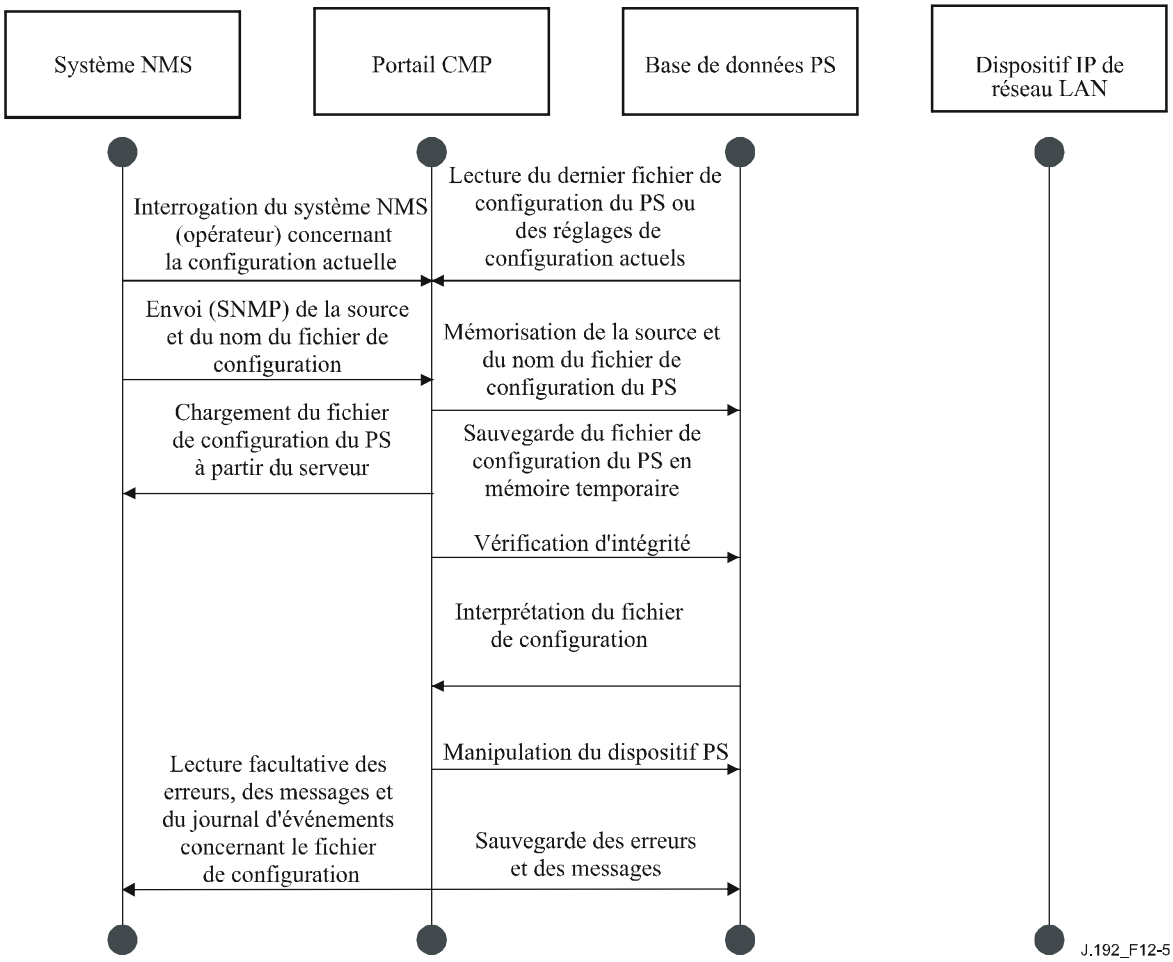


Figure 12-5/J.192 – Reconfiguration du dispositif PS (téléchargement du fichier de configuration) – Diagramme séquentiel

12.4 Accès de base MIB

12.4.1 Configuration de modèle VACM

Le modèle IPCable2Home spécifie la commande par l'opérateur du domaine de gestion IPCable2Home. Un exemple de la configuration des paramètres du modèle VACM est représenté dans la Figure 12-6.

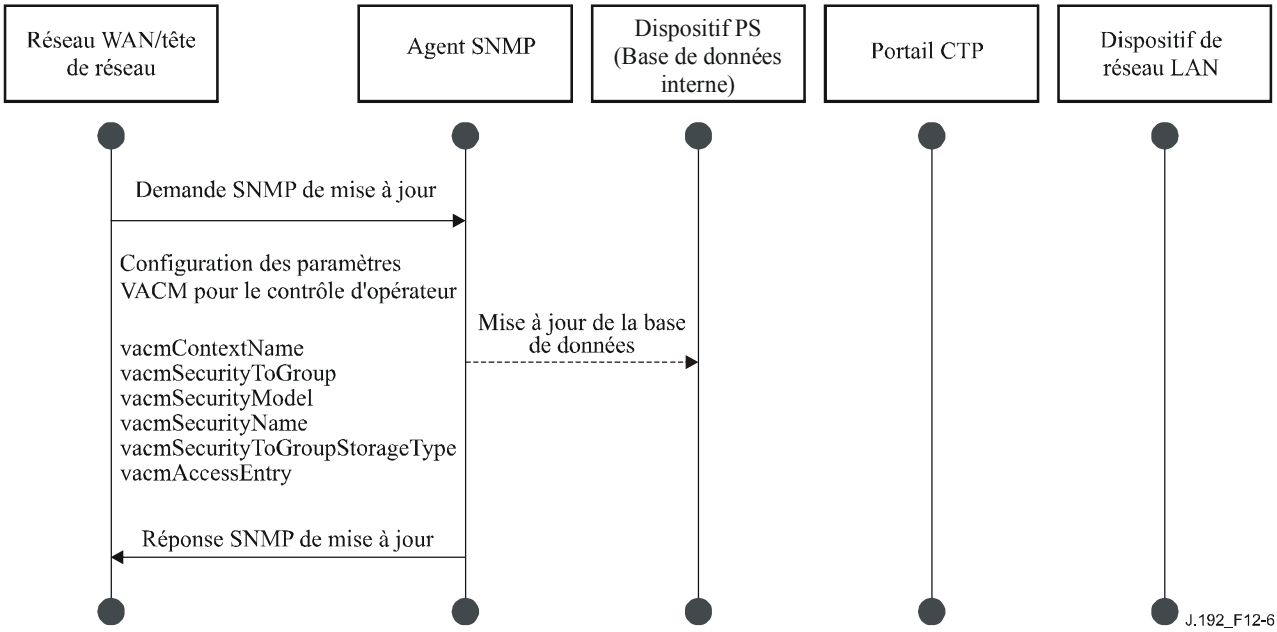


Figure 12-6/J.192 – Configuration des services de portail (paramètres du modèle VACM) – Séquence

12.4.2 Configuration de messagerie d'événement de gestion

12.4.2.1 Fonctionnement de la notification d'événement de portail CMP

Les événements IPCable2Home sont signalés par journalisation locale des événements, par messages TRAP du protocole SNMP, par messages INFORM du protocole SNMP et par messages SYSLOG. Le mécanisme de notification d'événement peut être réglé ou modifié par l'envoi d'un message SNMP de requête de mise à jour (SET) vers l'adresse de l'interface PS WAN-Man, à partir du système NMS.

La Figure 12-7 décrit la façon de configurer la base de données PS afin de mémoriser les événements dans les fichiers d'enregistrement locaux. Les événements du journal local sont de deux types: locaux-non volatils et locaux-volatils. Le système NMS lira le contenu du journal local et écrira ce contenu dans le système de journalisation d'événements de la tête de réseau. Un réamorçage du dispositif PS provoque seulement l'effacement des événements volatils de la base de données PS. Les événements non volatils persistent après un réamorçage.

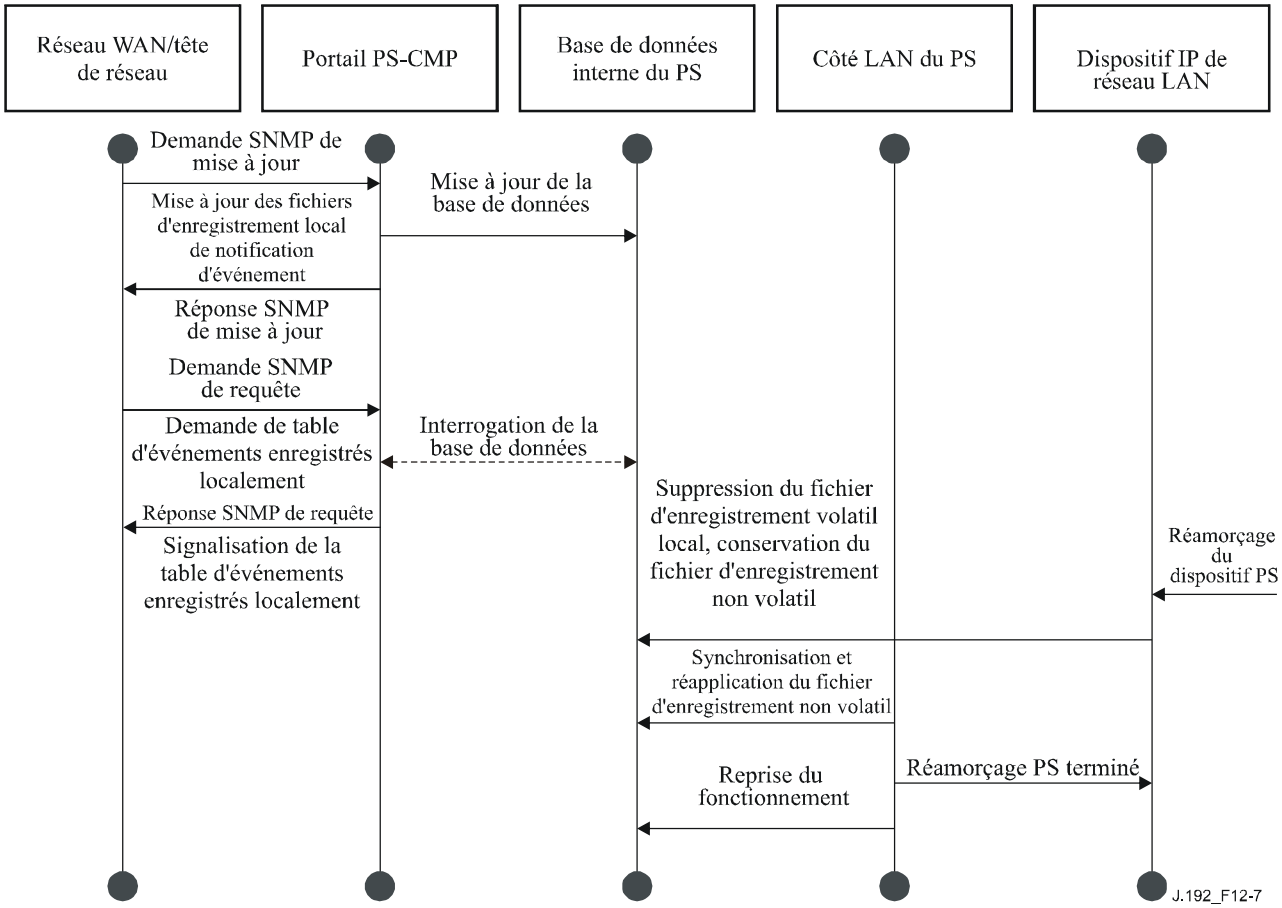


Figure 12-7/J.192 – Configuration des services de portail (contrôle d'événement) – Séquence

La Figure 12-8 décrit le téléchargement d'un fichier de configuration pour un dispositif PS en mode de préconfiguration SNMP. Ce processus est déclenché par une requête SNMP de mise à jour (SET). Le dispositif PS doit vérifier ce fichier avant de l'accepter. Dans cet exemple, une erreur de TLV existe et est rapportée. Etant donné que la notification d'événement est fixée au mode de préinterruption TRAP du protocole SNMP, l'adresse du serveur de préinterruptions TRAP est récupérée à partir de la base de données PS et l'événement est envoyé à ce serveur de préinterruptions TRAP.

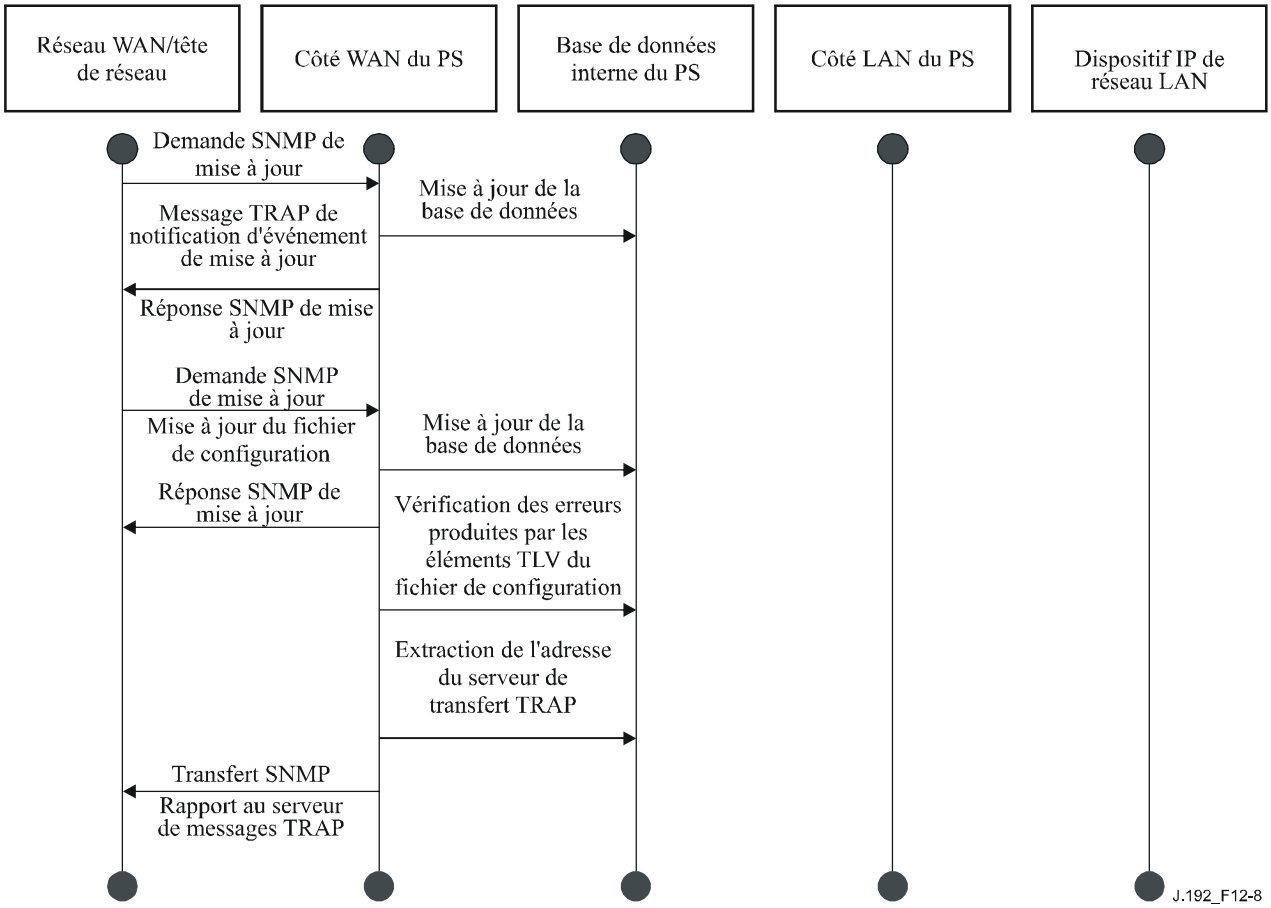


Figure 12-8/J.192 – Téléchargement du fichier de configuration du dispositif PS (avec éléments TLV non valides) – Séquence

La Figure 12-9 décrit le processus d'un dispositif IP de réseau local essayant d'obtenir une adresse IP à partir du serveur DHCP local (CDS). La fonction de serveur CDS vérifie la base de données PS afin de trouver une adresse IP disponible. Dans ce cas, le serveur CDS détecte qu'aucune adresse IP n'est disponible à partir de la réserve d'adresses et il envoie un événement au serveur SYSLOG.

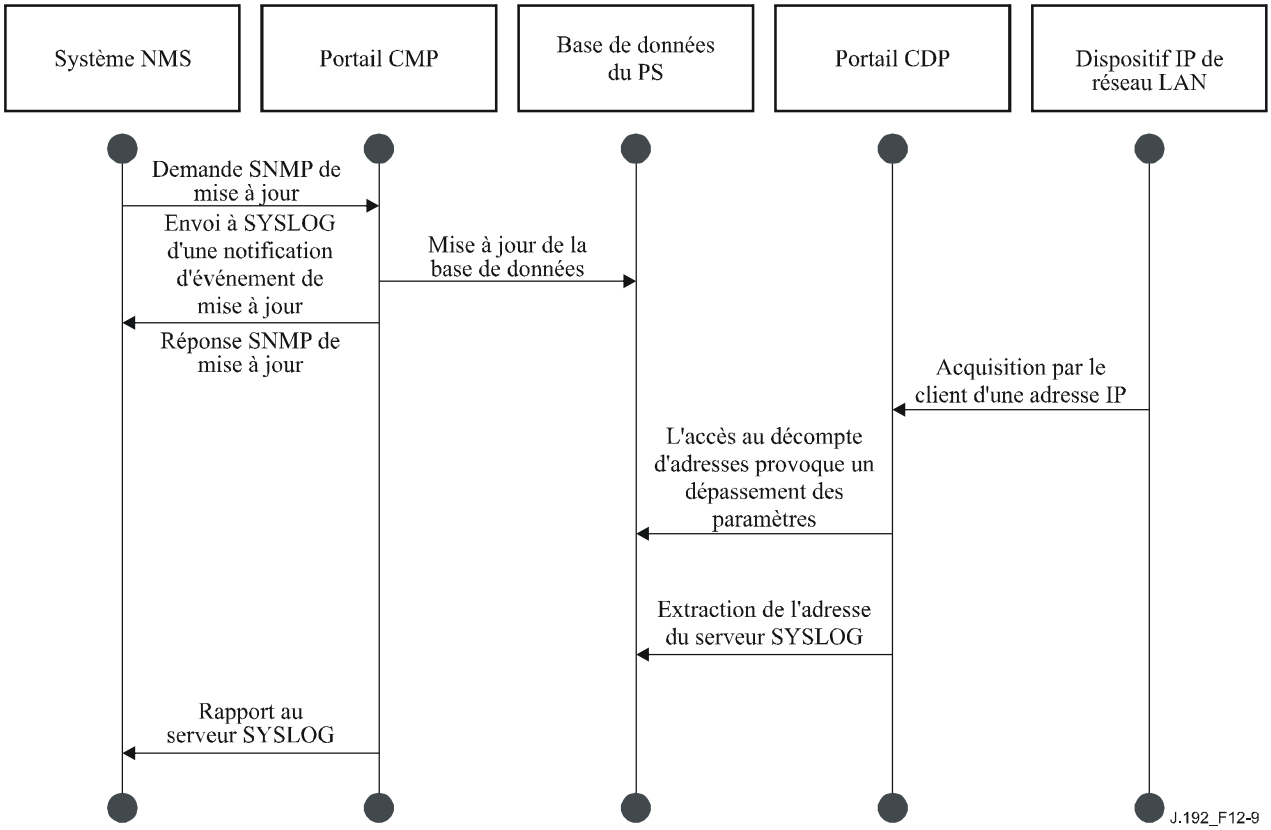


Figure 12-9/J.192 – Acquisition d'adresse (demande dépassant le compte préconfiguré) – Séquence

12.4.2.2 Exemple de fonctionnement du ralentissement et de la limitation des événements au portail CMP

La présente Recommandation offre un mécanisme de ralentissement d'événements par la fonctionnalité de portail CMP du dispositif PS. Le ralentissement et la limitation des événements constituent un mécanisme très flexible qui peut inclure des cas dans lesquels tous les événements sont signalés et des cas dans lesquels aucun événement n'est signalé au système NMS. Voir au § 6.3.3.2.4.8 une description du mécanisme de ralentissement et de limitation des événements au portail CMP.

La Figure 12-10 décrit la façon de configurer la base de données PS afin de renvoyer des événements par la méthode des messages INFORM du protocole SNMP. Au départ, plusieurs messages INFORM sont écrits dans le fichier de journal local et sont délivrés au système NMS. Le mécanisme de ralentissement d'événements règle le nombre maximal d'événements qui peuvent être envoyés au système NMS dans un laps de temps donné. Quand cette limite est atteinte, le dispositif PS arrête d'envoyer des messages INFORM au système NMS. Afin de relancer la notification d'événements, le système NMS DEVRAIT réactiver la signalisation des événements.

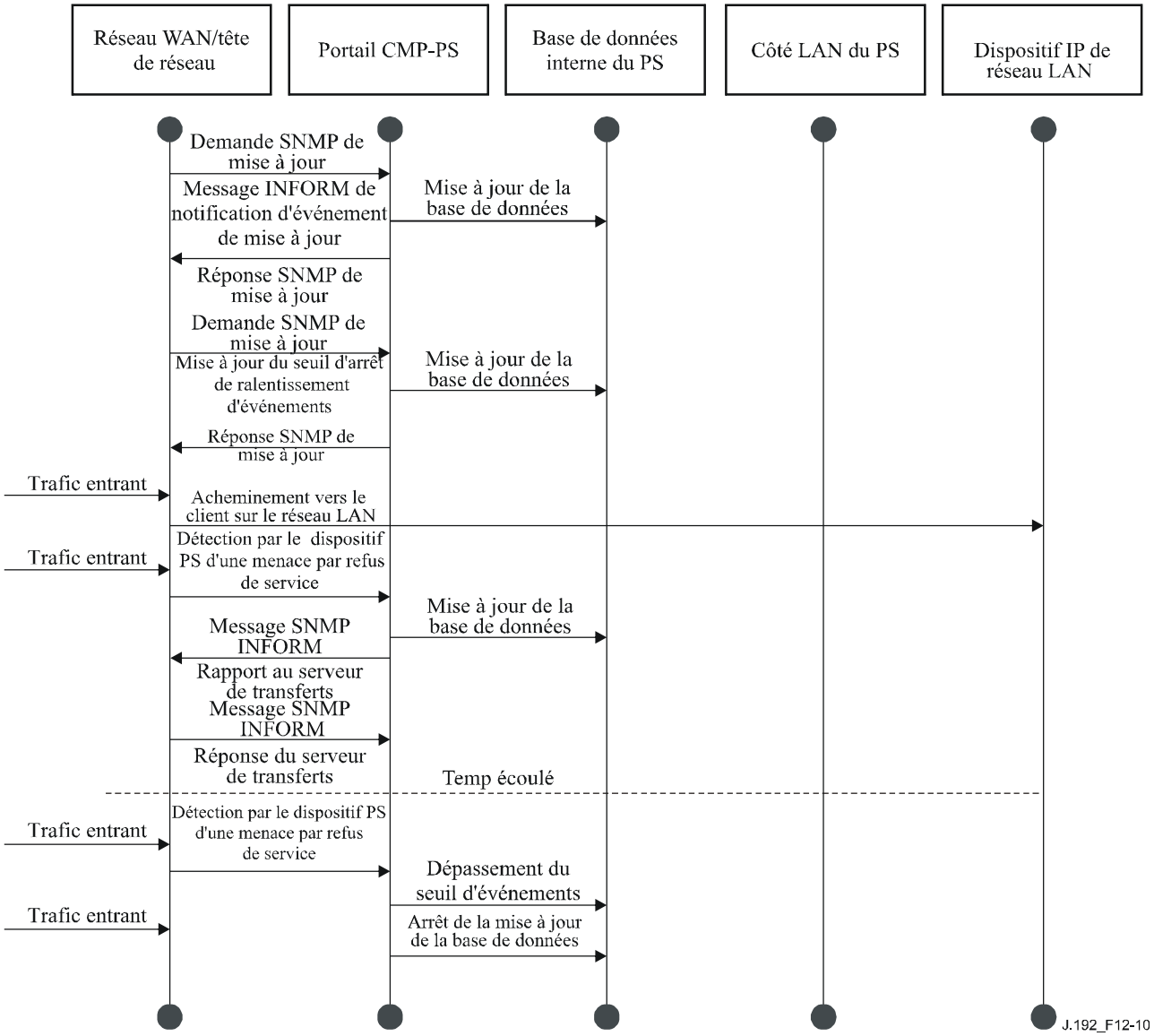


Figure 12-10/J.192 – Fonctionnement du ralentissement et de la limitation des événements au portail CMP

13 Processus de préconfiguration

Le présent paragraphe décrit les processus impliqués lors de l'utilisation des utilitaires de préconfiguration décrits dans le § 7, pour la préconfiguration initial de dispositif IP de réseau local et de l'élément de services de portail. Cette préconfiguration recouvre les trois tâches suivantes:

1) acquisition d'adresses de réseau;

2) acquisition d'informations sur le serveur;

3) téléchargement sécurisé et traitement du fichier de configuration du dispositif PS.

Les processus de préconfiguration sont décrits dans le présent paragraphe pour chacun des cas pertinents suivants:

- interface PS WAN-Man – préconfiguration de la fonctionnalité de gestion fondée sur l'interface PS WAN;
- interface PS WAN-Data – préconfiguration d'adresses IP d'interface PS WAN-Data à utiliser afin de créer des mappages de conversion CAT vers des dispositifs IP de réseau local situés dans le secteur d'adresses du réseau LAN-Trans;

- dispositif IP de réseau local situé dans le secteur LAN-Trans – préconfiguration d'un dispositif IP de réseau local avec une adresse IP convertie;
- dispositif IP de réseau local situé dans le secteur LAN-Pass – préconfiguration d'un dispositif IP de réseau local avec une adresse IP qui est transmise au réseau régional.

La préconfiguration de l'élément CM d'un dispositif PS intégré est séparé et distinct de la préconfiguration IPCable2Home et est hors du domaine d'application de la présente Recommandation. Le lecteur est prié de consulter les spécifications CableModem concernant les descriptions de la préconfiguration des câblo-modems.

Les éléments fonctionnels avec lesquels l'élément de services de portail interagit pendant les processus de préconfiguration énumérés ci-dessus sont identifiés dans la Figure 13-1. L'élément fonctionnel de centre de distribution de clés (KDC) est représenté en pointillé, car il est utilisé en mode de préconfiguration SNMP mais non en mode de préconfiguration DHCP. Les autres éléments fonctionnels sont utilisés dans les deux modes de préconfiguration.

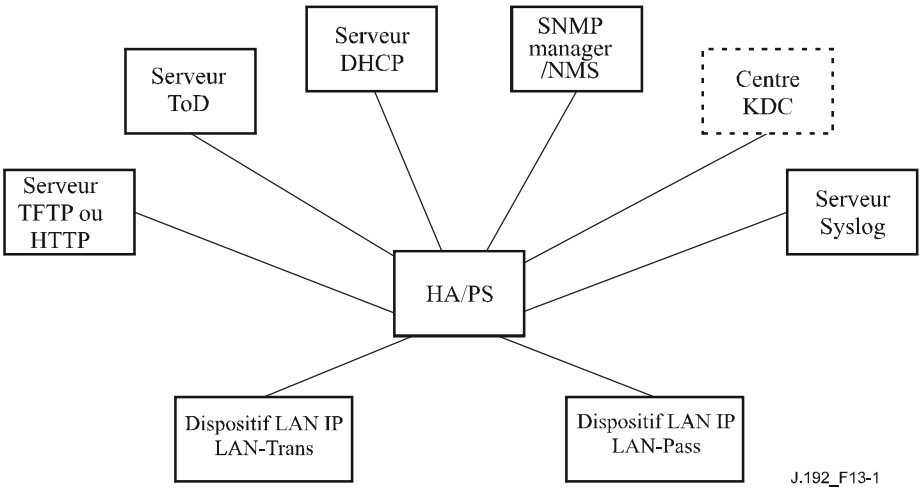


Figure 13-1/J.192 – Eléments fonctionnels de préconfiguration IPCable2Home

Le serveur distant du protocole trivial de transfert de fichiers (TFTP) ou le serveur distant du protocole de transfert d'hypertextes (HTTP) offre l'accès au fichier de configuration du dispositif PS pour le dispositif PS et suit les règles décrites dans [RFC 1350]. Le serveur temporel (ToD) offre au dispositif PS les moyens d'acquérir l'heure locale en format UTC comme décrit dans [RFC 868]. Le serveur du protocole de configuration dynamique du serveur local (DHCP) offre au dispositif PS les adresses IP privées et/ou mondiales selon [RFC 2131], et fournit d'autres informations par des options du protocole DHCP conformément au document [RFC 2132]. Le système de gestion de réseau (NMS) se conforme au protocole simple de gestion de réseau (SNMP), versions SNMPv1, SNMPv2 et SNMPv3, comme décrit dans [RFC 3584]. Le serveur de journalisation du système (SYSLOG) manipule les messages événementiels produits par le dispositif PS et par les dispositifs IP de réseau local domestique. Le dispositif PS implémente des clients pour ces serveurs fournis par le réseau de transmission de données par câble et fait appel à ces fonctions de client pendant le processus de préconfiguration décrit dans le présent paragraphe afin d'accomplir les tâches énumérées au début du présent paragraphe.

13.1 Modes de préconfiguration

Les paragraphes 5.5 et 7.2.1 présentent deux modes de préconfiguration valides qui sont pris en charge par l'élément de services de portail: le mode de préconfiguration DHCP et le mode de préconfiguration SNMP. Le dispositif PS fonctionne dans un troisième mode, le mode IPCable2Home inactif, s'il n'est pas configuré de façon à fonctionner dans un des deux modes

valides de préconfiguration. Dans le présent paragraphe, les deux modes valides de préconfiguration sont présentés plus en détail. La Figure 13-2 décrit un flux événementiel possible pour les deux modes de préconfiguration et pour le mode IPCable2Home inactif. Le point clé de la Figure 13-2 est le commutateur utilisé par le dispositif PS afin de déterminer le mode dans lequel il doit fonctionner.

Le dispositif PS fonctionne en mode de préconfiguration DHCP (mode DHCP) si le serveur DHCP dans le réseau câblé offre une adresse IP valide pour le serveur TFTP ou HTTP dans le champ 'siaddr' du message DHCP, offre un nom de fichier valide pour le fichier de configuration du dispositif PS dans le champ 'file' du message DHCP et NE fournit PAS l'option DHCP 177 avec les sous-options 3, 6 et 51 au client CDC du dispositif PS pendant la phase ACK en protocole DHCP du processus d'initialisation. Le mode de préconfiguration DHCP est destiné à activer le dispositif PS de façon à fonctionner dans une infrastructure DOCSIS 1.0 ou DOCSIS 1.1 avec peu ou pas de changements au réseau DOCSIS.

Le mode de préconfiguration SNMP est déclenché dans le dispositif PS quand le serveur DHCP situé dans le réseau câblé NE fournit PAS de valeurs pour les champs 'siaddr' et 'file' et quand le serveur DHCP du réseau câblé DOIT envoyer l'option DHCP 177 avec les sous-options 3, 6 et 51. Le mode de préconfiguration SNMP est destiné à activer le dispositif PS afin de tirer parti des caractéristiques évoluées d'une infrastructure PacketCable.

Le dispositif PS fonctionne par défaut en mode CableHome inactif s'il ne reçoit aucun des champs ou sous-options définis comme étant des déclencheurs en mode de préconfiguration DHCP et en mode de préconfiguration SNMP, ou s'il reçoit une combinaison non valide de ces champs et sous-options. Un dispositif PS intégré en tant qu'élément eSAFE avec un câblo-modem intégré conforme à eDOCSIS [eDOCSIS1] peut également être configuré au moyen de l'objet de base MIB esafePsCableHomeModeControl du câblo-modem afin de fonctionner en mode CableHome inactif. Voir le § 7.3.3.2.4.

Toutes les conditions d'erreur ne sont pas représentées dans les Figures 13-2 et 13-3. Voir au § 7.2.2 une description du comportement du dispositif PS en cas de critères incorrects de décision relative au mode de préconfiguration.

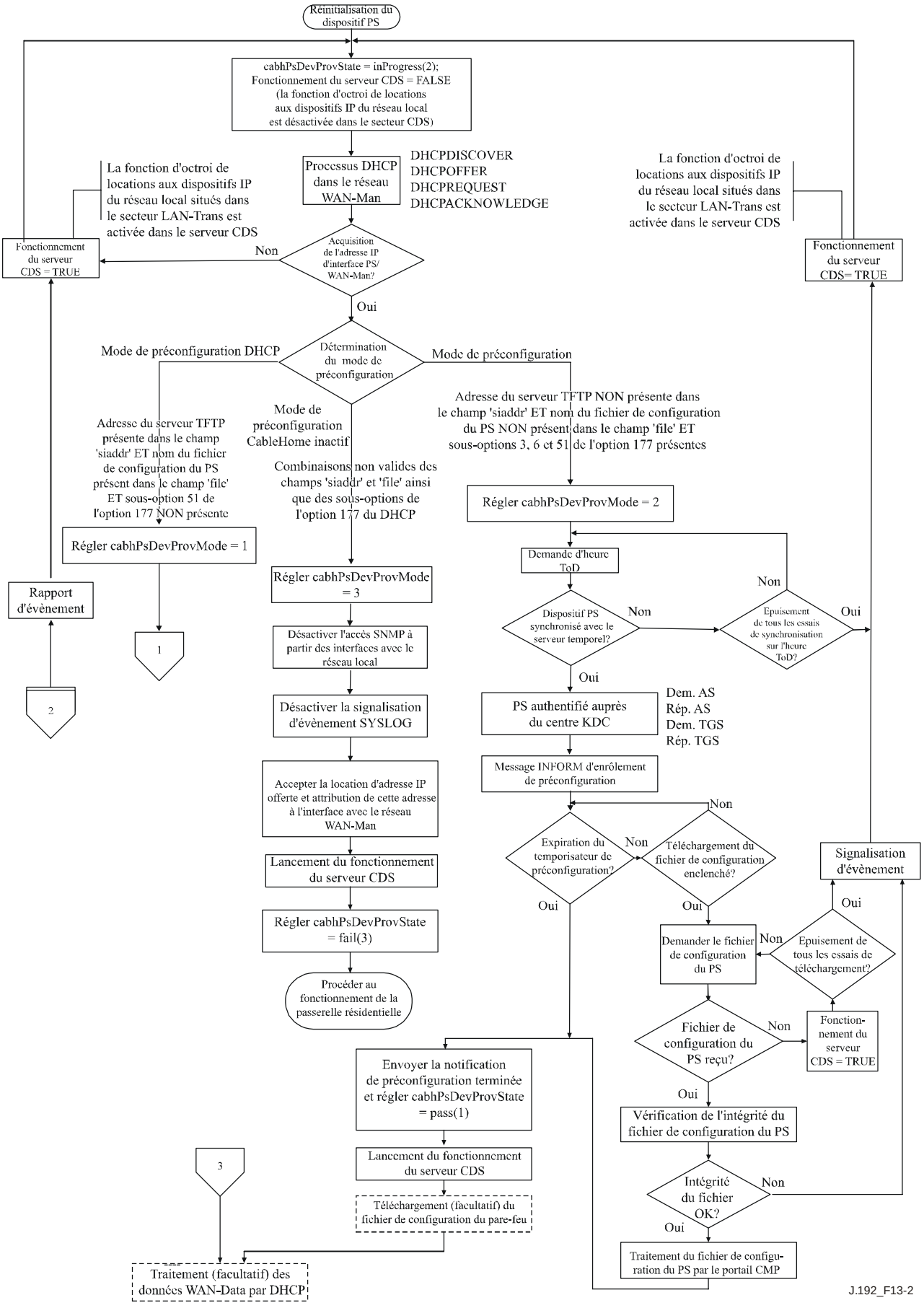


Figure 13-2/J.192 – Modes de préconfiguration IPCable2Home (partie 1)

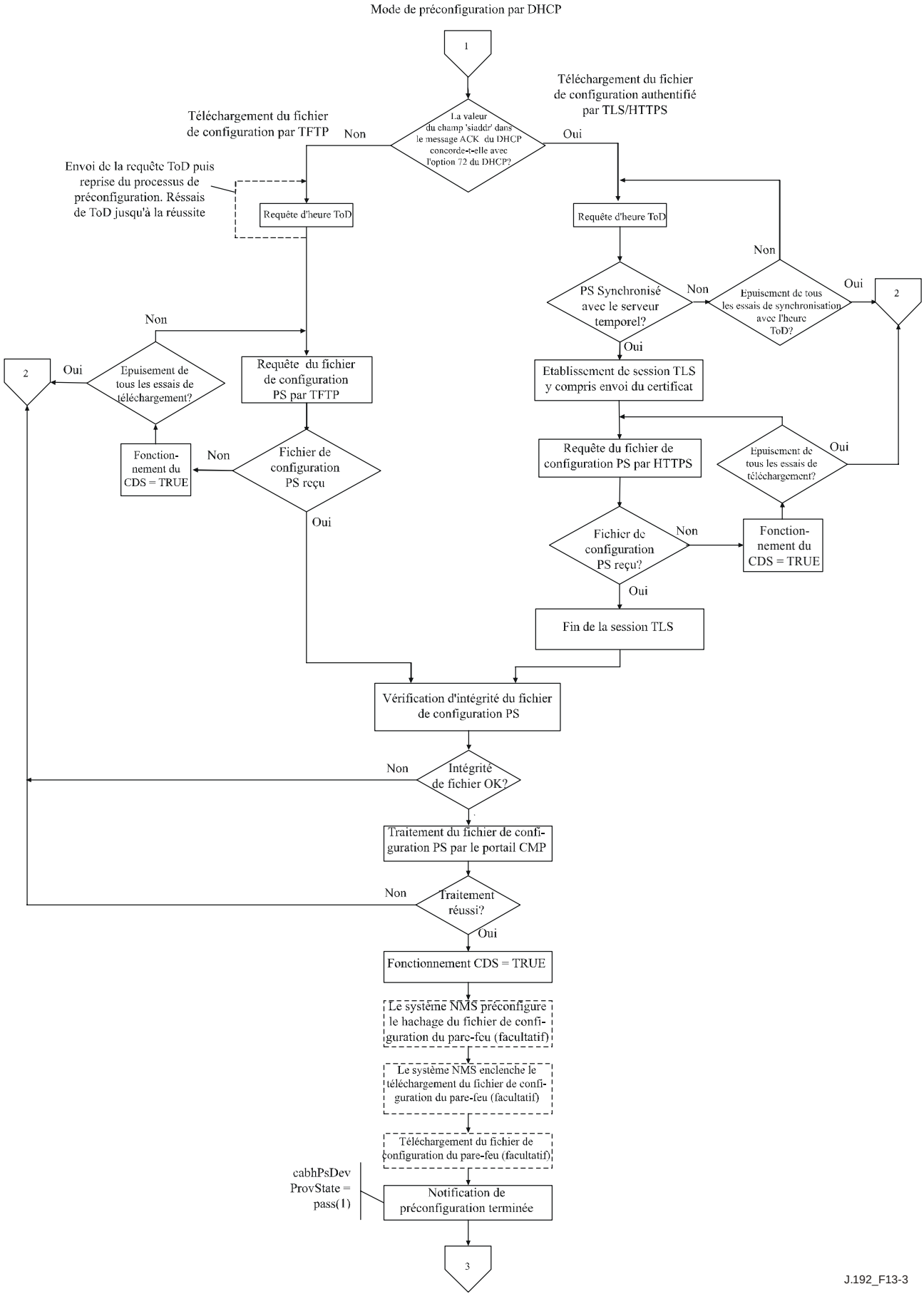


Figure 13-3/J.192 – Modes de préconfiguration IPCable2Home (partie 2)

13.2 Processus de préconfiguration des services de portail pour la gestion: mode de préconfiguration DHCP

Le dispositif PS demande au système de préconfiguration de la tête de réseau une adresse IP à utiliser pour l'échange de messages de gestion entre le système NMS et le dispositif PS. Celui-ci analyse sémantiquement le message DHCP renvoyé dans le message OFFER du protocole DHCP et prend une décision sur le mode de préconfiguration dans lequel il doit fonctionner (voir § 7.3.3.2.4). Le paragraphe 7.3.3.2.3.2 décrit trois modes d'adressage de réseau régional pris en charge pour l'acquisition des adresses IP par le dispositif PS à partir du serveur DHCP dans le réseau câblé.

Si le dispositif PS détermine qu'il doit fonctionner en mode de préconfiguration DHCP, il utilise les informations du fichier de configuration du dispositif PS transmises dans le message DHCP comme déclencheur afin de télécharger le fichier de configuration du dispositif PS comme décrit dans le § 7.3. Le téléchargement du fichier de configuration du dispositif PS est nécessaire lorsque le dispositif PS fonctionne en mode de préconfiguration DHCP, mais est facultatif lorsque le dispositif PS fonctionne en mode de préconfiguration SNMP.

En mode de préconfiguration DHCP, le dispositif PS (portail CMP) fonctionne par défaut en mode d'accès NmAccess pour l'échange de messages de gestion avec le système NMS, mais celui-ci peut (facultativement) configurer le portail CMP en mode de coexistence. Ces modes de messagerie de gestion sont décrits dans le § 6.3.3.

La Figure 13-4 et le Tableau 13-1 décrivent la séquence des messages nécessaires pour initialiser un dispositif PS fonctionnant en mode de préconfiguration DHCP. Le processus de préconfiguration pour la gestion d'un dispositif PS fonctionnant en mode de préconfiguration DHCP est le même pour le dispositif PS intégré avec un câblo-modem DOCSIS et pour le dispositif PS autonome. La préconfiguration d'un dispositif PS intégré NE DOIT PAS intervenir avant le processus de préconfiguration du câblo-modem. La préconfiguration de gestion d'un dispositif PS autonome DEVRAIT intervenir immédiatement après mise sous tension/réinitialisation.

Le processus facultatif de téléchargement d'un fichier de configuration du pare-feu est représenté en grisé dans la Figure 13-4.

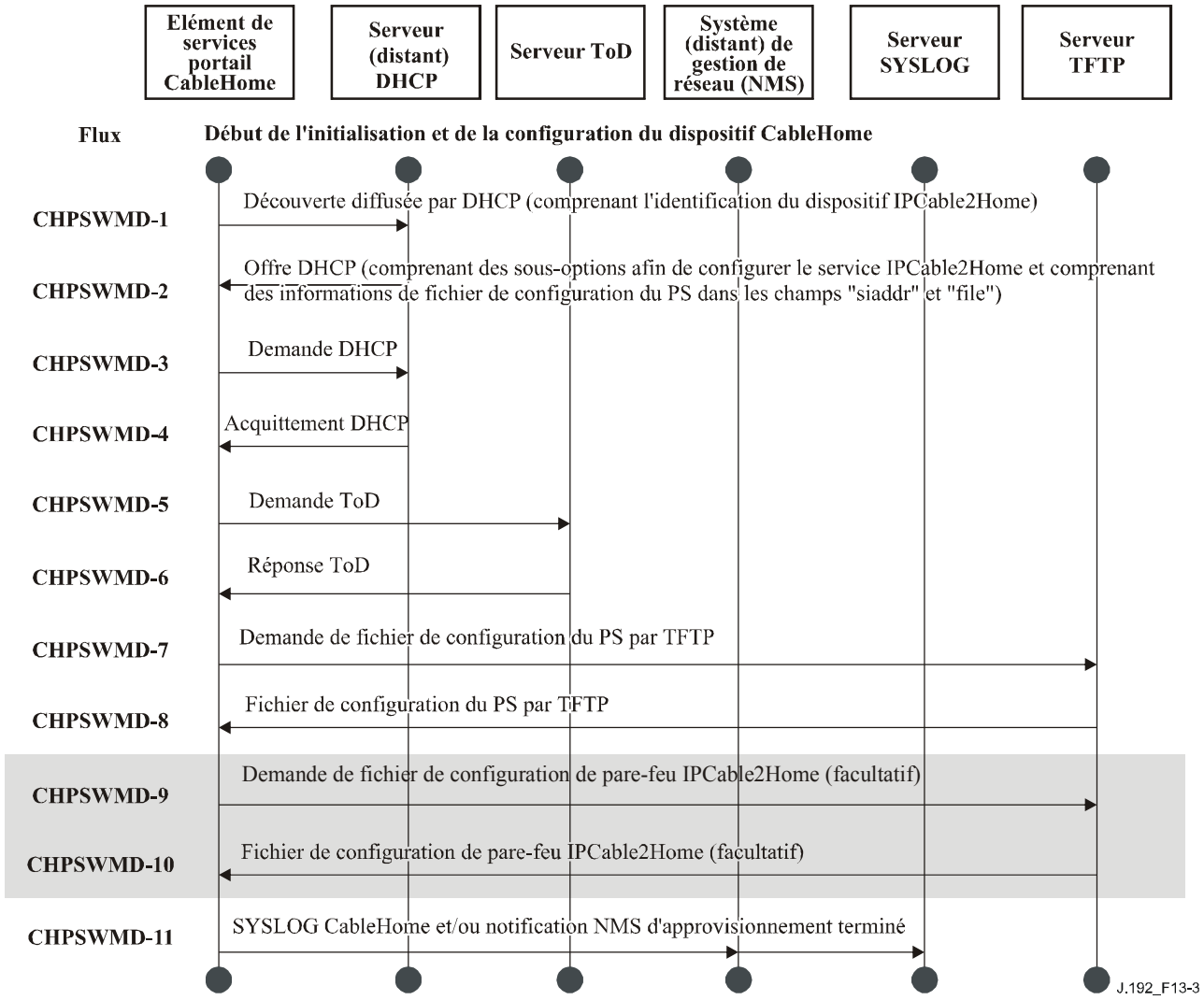


Figure 13-4/J.192 – Processus de préconfiguration pour la gestion des services portail – Mode de préconfiguration DHCP

Le Tableau 13-1 décrit les messages individuels CHPSWMD-1 – CHPSWMD-11 représentés dans la Figure 13-4.

Tableau 13-1/J.192 – Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration DHCP

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration DHCP	Séquence normale	Séquence d'échec
CHPSWMD-1	Découverte diffusée par DHCP Le portail CDP (client CDC) envoie un message diffusé DHCP DISCOVER afin d'acquérir l'adresse IP du réseau WAN-Man comme décrit dans le § 7.3.3.2.4. Le message DHCP DISCOVER diffusé par le portail CDP (client CDC) comprend les options obligatoires énumérées dans le Tableau 7-10: "Options DHCP de client CDC dans les messages DISCOVER et REQUEST". Le dispositif PS règle l'objet cabhPsDevProvState à l'état 'inProgress' (2) quand le client CDC envoie un message diffusé DHCP DISCOVER.	Commencer la séquence de préconfiguration	En cas d'échec selon le protocole DHCP, signaler une erreur et continuer à essayer le message de découverte diffusée par DHCP jusqu'à la réussite (retour à l'étape CHPSWMD-1). En cas d'échec à la première tentative d'acquérir une adresse IP de réseau WAN-Man, le dispositif PS initialise le fonctionnement du serveur CDS comme spécifié dans le § 7.3.3.2.4.
CHPSWMD-2	DHCP OFFER	CHPSWMD-2 DOIT survenir après achèvement de l'étape CHPSWMD-1	En cas d'échec selon le protocole DHCP, revenir à CHPSWMD-1 et signaler une erreur.
CHPSWMD-3	DHCP REQUEST Le portail CDP DOIT envoyer au serveur DHCP approprié un message DHCP REQUEST afin d'accepter le message OFFER du protocole DHCP.	CHPSWMD-3 DOIT survenir après achèvement de l'étape CHPSWMD-2	En cas d'échec selon le protocole DHCP, revenir à CHPSWMD-1 et signaler une erreur.
CHPSWMD-4	DHCP ACK Le serveur DHCP envoie au portail CDP un message DHCP ACK qui contient l'adresse IPv4 du dispositif PS. Celui-ci modifie l'objet cabhPsDevProvMode sur la base des informations reçues dans le message ACK du protocole DHCP (voir § 7.3.3.2.4). Le dispositif PS mémorise l'adresse du serveur temporel dans l'objet cabhPsDevTimeServerAddr. Le dispositif PS modifie l'objet cabhPsDevProvMode sur la base des informations reçues dans le message ACK du protocole DHCP (voir § 7.3.3.2.4).	CHPSWMD-4 DOIT survenir après achèvement de l'étape CHPSWMD-3	En cas d'échec selon le protocole DHCP, revenir à CHPSWMD-1 et signaler une erreur.

Tableau 13-1/J.192 – Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration DHCP

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration DHCP	Séquence normale	Séquence d'échec
CHPSWMD-5	Demande d'heure locale (ToD) selon [RFC 868] Le dispositif PS envoie une demande de ToD au serveur temporel identifié dans l'option 4 du message DHCP ACK.	CHPSWMD-5 DOIT survenir après achèvement de l'étape CHPSWMD-4	Passer à l'étape CHPSWMD-6
CHPSWMD-6	Réponse d'heure ToD Le serveur temporel ToD est censé répondre avec l'heure locale en format UTC.	CHPSWMD-6 DOIT survenir après achèvement de l'étape CHPSWMD-5	Essayer la synchronisation avec le prochain serveur d'heure actuelle (ToD) énuméré dans l'option DHCP 4 du message DHCP ACK. Si un essai infructueux de synchronisation a été fait avec chaque serveur ToD dans le cadre d'une tentative initiale de synchronisation temporelle, régler cabhPsDevTodSyncStatus = false(2), essayer d'acquérir l'heure système à partir du câblo-modem (PS intégré seulement), mettre à jour l'objet cabhPsDevDateTime, mettre à jour les heures de location du serveur CDS et passer à l'étape CHPSWMD-7. Voir de plus amples détails au § 7.5.4.
CHPSWMD-7	Demande de transfert TFTP Le dispositif PS fonctionnant en mode de préconfiguration DHCP envoie au serveur TFTP une requête Get du protocole TFTP afin de demander le fichier de données de configuration spécifié comme décrit dans le § 7.4.4.	CHPSWMD-7 DOIT survenir après achèvement de l'étape CHPSWMD-5. CHPSWMD-7 peut intervenir avant CHPSWMD-6.	Passer à l'étape CHPSWMD-8

Tableau 13-1/J.192 – Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration DHCP

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration DHCP	Séquence normale	Séquence d'échec
CHPSWMD-8	L'envoi par le serveur TFTP du fichier de configuration du dispositif PS Après que le fichier de configuration du dispositif PS est reçu, le hachage est vérifié. Voir § 7.4.4.1. Le fichier de configuration du dispositif PS est alors traité. Voir au § 7.4.4 le contenu du fichier de configuration du dispositif PS. Facultativement, l'adresse IP du serveur TFTP de fichier de configuration de pare-feu, le nom du fichier de configuration du pare-feu et le hachage du fichier de configuration du pare-feu sont inclus dans le fichier de configuration du dispositif PS s'il y a un fichier de configuration du pare-feu à charger et c'est la méthode choisie afin de le spécifier.	CHPSWMD-8 DOIT survenir après achèvement de l'étape CHPSWMD-7	Si le téléchargement TFTP échoue, prendre la mesure indiquée au § 7.4.4.4, elon la nature de l'erreur.
CHPSWMD-9	Demande de transfert TFTP – Fichier de configuration du pare-feu (facultatif) Si le dispositif PS reçoit des informations de fichier de configuration de pare-feu (nom du serveur TFTP et du fichier de configuration du pare-feu) dans le fichier de configuration du dispositif PS, celui-ci envoie au serveur TFTP de configuration de pare-feu une requête Get du protocole TFTP afin de demander un fichier de configuration de pare-feu (voir § 11.6.4.2). Si le dispositif PS ne reçoit pas d'informations de fichier de configuration de pare-feu dans le fichier de configuration du dispositif PS, le processus de préconfiguration du dispositif PS (mode de préconfiguration DHCP) DOIT sauter les étapes CHPSWMD-9 et CHPSWMD-10 et passer à l'étape CHPSWMD-11.	Si l'étape CHPSWMD-9 se produit, elle DOIT survenir après achèvement de l'étape CHPSWMD-8	Si le transfert TFTP échoue, continuer le fonctionnement des services de portail mais signaler une erreur et continuer à essayer CHPSWMD-9.

Tableau 13-1/J.192 – Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration DHCP

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration DHCP	Séquence normale	Séquence d'échec
CHPSWMD-10	Envoi par le serveur TFTP du fichier de configuration du pare-feu (facultatif) Si l'étape CHPSWMD-9 se produit, le serveur TFTP envoie au dispositif PS une réponse TFTP contenant le fichier demandé. Après que le fichier de configuration du pare-feu est reçu, le hachage du fichier de configuration est calculé et comparé à la valeur reçue dans le fichier de configuration du dispositif PS. Le fichier est alors traité. Voir le § 11.6.4.	CHPSWMD-10 DOIT survenir après achèvement de l'étape CHPSWMD-9	Si le TFTP échoue, continuer le fonctionnement des services de portail mais signaler une erreur et continuer à essayer CHPSWMD-9. Si le traitement du fichier de configuration du pare-feu produit une erreur, continuer et signaler l'erreur comme événement.
CHPSWMD-11	Préconfiguration terminée Sur demande du système de préconfiguration, le dispositif PS est tenu d'informer le système de préconfiguration de l'état de préconfiguration du dispositif PS. Le système de préconfiguration pourrait demander au dispositif PS d'envoyer un message SYSLOG ou un message TRAP du SNMP, ou les deux. Si le dispositif PS achève correctement toutes les étapes requises de l'étape CHPSWMD-1 à CHPSWMD-10 et qu'il ait reçu une adresse de serveur SYSLOG dans le message OFFER du protocole DHCP, le dispositif PS DOIT envoyer un message de préconfiguration terminé au serveur SYSLOG avec l'état de préconfiguration réglé à PASS. Si le dispositif PS achève correctement toutes les étapes de préconfiguration requises de CHPSWMD-1 à CHPSWMD-10 et qu'il ait reçu des paramètres valides pour le récepteur de notification, le dispositif PS DOIT envoyer au récepteur de notification une notification de préconfiguration terminée (objet cabhPsDevInitTrap) avec les paramètres appropriés. Le dispositif PS DOIT mettre à jour la valeur de l'objet cabhPsDevProvState avec l'état 'pass'(1) quand les étapes de flux de préconfiguration CHPSWMD-1 à CHPSWMD-11 ont été menées à bien.	CHPSWMD-11 DOIT survenir après achèvement de CHPSWMD-10	Si le transfert SNMP échoue, le serveur de préconfiguration ne peut pas savoir que le processus de préconfiguration s'est achevé à moins qu'il n'interroge l'objet cabhPsProvState.

13.3 Processus de préconfiguration des services de portail pour la gestion: mode de préconfiguration DHCP avec HTTP/TLS

Le dispositif PS demande au système de préconfiguration de la tête de réseau une adresse IP à utiliser pour l'échange de messages de gestion entre le système NMS et le dispositif PS. Celui-ci analyse le message DHCP renvoyé dans le message OFFER du protocole DHCP et prend une décision sur le mode de préconfiguration dans lequel il doit fonctionner (voir § 7.3.3.2.4). Le § 7.3.3.2.3.2 décrit trois modes d'adressage de réseau régional pris en charge pour l'acquisition des adresses IP par le dispositif PS à partir du serveur DHCP dans le réseau câblé.

Si le dispositif PS détermine qu'il doit fonctionner en mode de préconfiguration DHCP, il utilisera les informations du fichier de configuration du dispositif PS transmises dans le message DHCP, comme déclencheur afin de télécharger le fichier de configuration du dispositif PS. Si l'option DHCP de code 72 est présente dans le message ACK du message DHCP et si son contenu correspond à l'adresse IP dans le champ "siaddr", le téléchargement se produira par empilement de HTTP sur TLS, comme spécifié dans le § 11.9.

En mode de préconfiguration DHCP, le dispositif PS (portail CMP) fonctionne par défaut en mode NmAccess pour l'échange de messages de gestion avec le système NMS; mais celui-ci peut (facultativement) configurer le portail CMP en mode de coexistence. Ces modes de messagerie de gestion sont décrits dans le § 6.3.3.

La Figure 13-5 et le Tableau 13-2 décrivent la séquence de messages nécessaires pour initialiser un dispositif PS fonctionnant en mode de préconfiguration DHCP avec HTTP/TLS. Le processus de préconfiguration et la gestion du dispositif PS fonctionnant en mode de préconfiguration DHCP sont les mêmes pour le dispositif PS intégré avec un câblo-modem DOCSIS et pour le dispositif PS autonome. La préconfiguration du dispositif PS intégré NE DOIT PAS intervenir avant le processus de préconfiguration du câblo-modem. La préconfiguration de gestion d'un dispositif PS autonome DEVRAIT intervenir immédiatement après mise sous tension/réinitialisation.

Le processus facultatif de téléchargement d'un fichier de configuration du pare-feu est représenté en grisé dans la Figure 13-5.

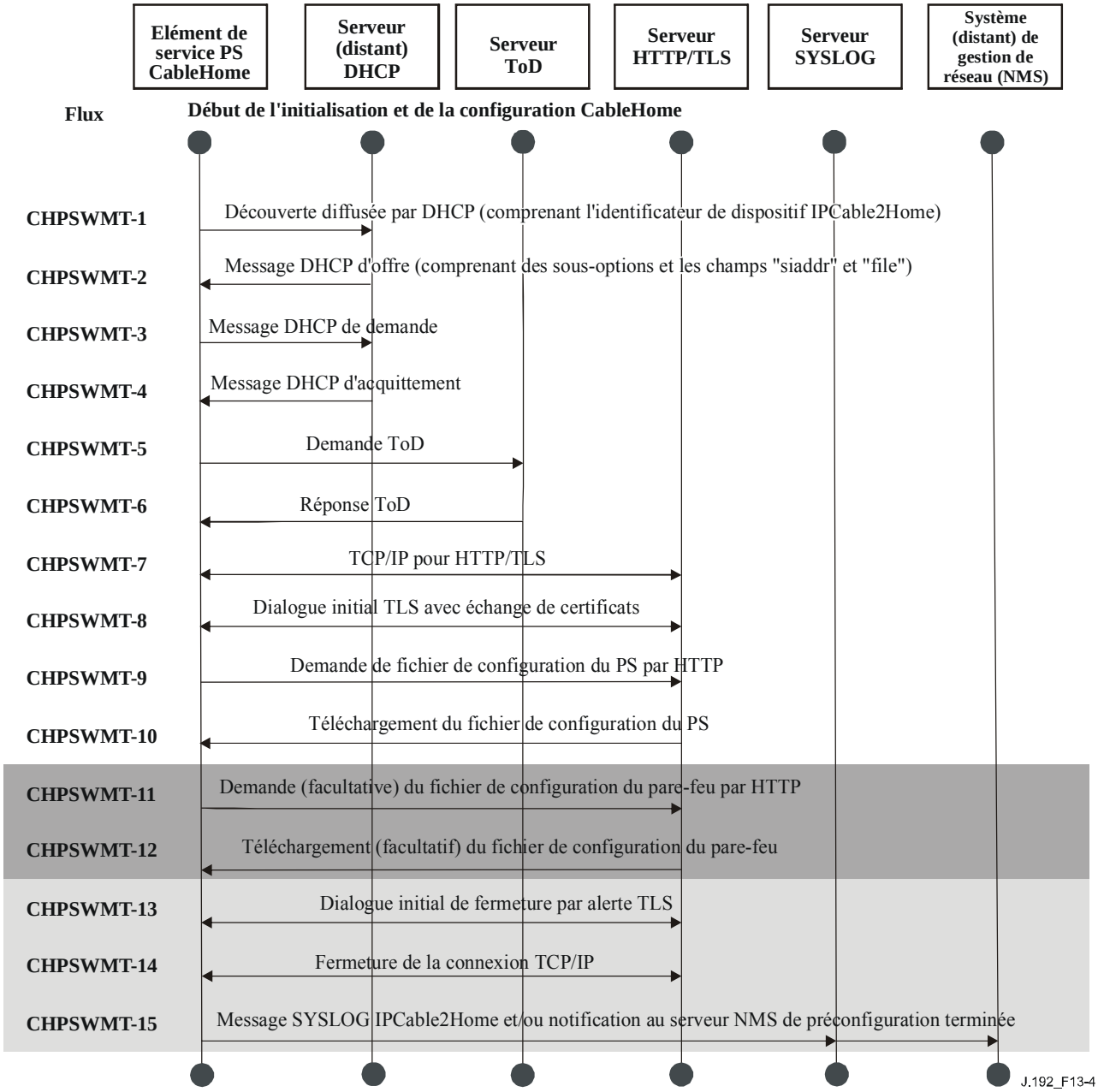


Figure 13-5/J.192 – Processus de préconfiguration – Mode de préconfiguration DHCP utilisant HTTP/TLS

Le Tableau 13-2 décrit les messages individuels CHPSWMT-1 – CHPSWMT-15 représentés dans la Figure 13-5. Pour plus d'informations, voir § 11.9, "Sécurité du fichier de configuration du dispositif PS en mode de préconfiguration DHCP".

Tableau 13-2/J.192 – Description des flux en mode de préconfiguration DHCP utilisant HTTP/TLS

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration DHCP	Séquence normale	Séquence d'échec
CHPSWMT-1	Découverte diffusée par DHCP Le portail CDP (client CDC) envoie un message diffusé DHCP DISCOVER afin d'acquérir l'adresse IP du réseau WAN-Man comme décrit dans le § 7.3.3.2.4. Le message DHCP DISCOVER diffusé par le portail CDP (client CDC) comprend les options obligatoires énumérées dans le Tableau 7-10, "Options DHCP de client CDC contenues dans les messages DISCOVER et REQUEST". Le dispositif PS règle l'objet cabhPsDevProvState à l'état 'inProgress' (2) quand le client CDC envoie un message diffusé DHCP DISCOVER.	Commencer la séquence de préconfiguration	En cas d'échec selon le protocole DHCP, signaler une erreur et continuer à essayer le message de découverte diffusée par DHCP jusqu'à la réussite (retour à l'étape CHPSWMT-1). En cas d'échec à la première tentative d'acquérir une adresse IP de réseau WAN-Man, le dispositif PS initialise le fonctionnement du serveur CDS comme spécifié dans le § 7.3.3.2.4.
CHPSWMT-2	DHCP OFFER	CHPSWMT-2 DOIT survenir après achèvement de l'étape CHPSWMT-1.	En cas d'échec selon le protocole DHCP, revenir à CHPSWMT-1 et signaler une erreur.
CHPSWMT-3	DHCP REQUEST Le portail CDP envoie au serveur DHCP approprié un message DHCP REQUEST afin d'accepter le message OFFER du protocole DHCP.	CHPSWMT-3 DOIT survenir après achèvement de l'étape CHPSWMT-2.	En cas d'échec selon le protocole DHCP, revenir à CHPSWMT-1 et signaler une erreur.

Tableau 13-2/J.192 – Description des flux en mode de préconfiguration DHCP utilisant HTTP/TLS

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration DHCP	Séquence normale	Séquence d'échec
CHPSWMT-4	DHCP ACK Le serveur DHCP envoie au portail CDP un message DHCP ACK qui contient l'adresse IPv4 du dispositif PS. Celui-ci mémorise l'adresse du serveur temporel dans l'objet cabhPsDevTimeServerAddr. Si l'adresse IP dans le champ "siaddr" du message DHCP ACK correspond à la première adresse IP dans l'option 72, le dispositif PS commence une session de sécurité TLS et télécharge le fichier de configuration à partir du serveur HTTP. Le dispositif PS modifie l'objet cabhPsDevProvMode sur la base des informations reçues dans le message ACK du protocole DHCP. Voir § 11.9, "Sécurité du fichier de configuration du dispositif PS en mode de préconfiguration DHCP".	CHPSWMT-4 DOIT survenir après achèvement de l'étape CHPSWMT-3.	En cas d'échec selon le protocole DHCP, revenir à CHPSWMT-1 et signaler une erreur.
CHPSWMT-5	Demande d'heure locale (ToD) selon [RFC 868] Le dispositif PS se synchronise avec le serveur temporel choisi à partir de l'option 4 du protocole DHCP (option de serveur temporel) dans le message ACK du protocole DHCP. Voir § 7.5.4, "Fonction de client d'heure locale: exigences".	CHPSWMT-5 DOIT survenir après achèvement de l'étape CHPSWMT-4.	Passer à l'étape CHPSWMT-6.

Tableau 13-2/J.192 – Description des flux en mode de préconfiguration DHCP utilisant HTTP/TLS

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration DHCP	Séquence normale	Séquence d'échec
CHPSWMT-6	Réponse d'heure ToD Le serveur temporel ToD est censé répondre avec l'heure locale en format UTC.	CHPSWMT-6 DOIT survenir après achèvement de l'étape CHPSWMT-5.	Essayer la synchronisation avec le prochain serveur d'heure actuelle (ToD) énuméré dans l'option DHCP 4 du message DHCP ACK. Si un essai infructueux de synchronisation a été fait avec chaque serveur ToD dans le cadre d'une tentative initiale de synchronisation temporelle, régler cabhPsDevTodSyncStatus = false(2), essayer d'acquérir l'heure système à partir du câblo-modem (PS intégré seulement), mettre à jour l'objet cabhPsDevDateTime, mettre à jour les heures de location du serveur CDS et passer à l'étape CHPSWMD-7. Voir de plus amples détails au § 7.5.4.
CHPSWMT-7	Etablissement du protocole TCP/IP Le dispositif PS fonctionnant en mode de préconfiguration DHCP établit une session TCP/IP afin d'échanger des messages HTTP avec le serveur HTTP dans le système de préconfiguration du câblo-opérateur.	CHPSWMT-7 DOIT survenir après achèvement de l'étape CHPSWMT-5. CHPSWMT-7 peut intervenir avant CHPSWMT-6.	En cas d'échec selon TCP/IP, réessayer selon la spécification. Si tous les réessais échouent, revenir à CHPSWMT-1 et signaler une erreur.
CHPSWMT-8	Dialogue initial du protocole TLS Le dispositif PS fonctionnant en mode de préconfiguration DHCP ouvre une session de sécurité TLS avec le serveur HTTPS.	CHPSWMT-8 DOIT survenir après achèvement de l'étape CHPSWMT-7.	En cas d'échec pour TLS, réessayer selon la spécification. Si tous les réessais échouent, revenir à CHPSWMT-1 et signaler une erreur.

Tableau 13-2/J.192 – Description des flux en mode de préconfiguration DHCP utilisant HTTP/TLS

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration DHCP	Séquence normale	Séquence d'échec
CHPSWMT-9	Demande de fichier de configuration par HTTP Le dispositif PS fonctionnant en mode de préconfiguration DHCP demande le fichier de configuration à partir du serveur HTTP.	CHPSWMT-9 DOIT survenir après achèvement de l'étape CHPSWMT-8.	En cas d'échec pour HTTP, réessayer selon la spécification. Si tous les réessais échouent, revenir à CHPSWMT-1 et signaler une erreur.
CHPSWMT-10	Envoi par le serveur HTTPS du fichier de configuration du dispositif PS Le fichier de configuration du dispositif PS est traité. Voir le § 7.4.4 concernant le contenu du fichier de configuration du dispositif PS. Facultativement, l'adresse IP du serveur HTTP de fichier de configuration du pare-feu et le nom du fichier de configuration du pare-feu sont inclus dans le fichier de configuration du dispositif PS.	CHPSWMT-10 DOIT survenir après achèvement de l'étape CHPSWMT-9.	Si le téléchargement HTTP échoue, signaler une erreur et revenir à CHPSWMT-9 (continuer à essayer le téléchargement du fichier de configuration du dispositif PS). Si le traitement du dispositif Fichier de configuration du dispositif PS produit une erreur, passer à l'étape CHPSWMT-13 et signaler l'erreur comme événement.
CHPSWMT-11	Demande HTTP (facultative) de fichier de configuration du pare-feu Si le dispositif PS reçoit des informations de fichier de configuration de pare-feu (nom du serveur TFTP et du fichier de configuration du pare-feu) dans le fichier de configuration du dispositif PS, le dispositif PS demande le fichier de configuration du pare-feu à partir du serveur HTTP. Si le dispositif PS ne reçoit pas d'informations de fichier de configuration de pare-feu dans le fichier de configuration du dispositif PS, le processus de préconfiguration du dispositif PS (mode de préconfiguration DHCP) DOIT sauter les étapes CHPSWMT-11 et CHPSWMT-12 et passer à l'étape CHPSWMT-13.	Si l'étape CHPSWMT-11 se produit, elle DOIT survenir après achèvement de l'étape CHPSWMT-10.	Si le protocole HTTP échoue, continuer le fonctionnement des services de portail mais signaler une erreur et continuer à essayer CHPSWMT-13.

Tableau 13-2/J.192 – Description des flux en mode de préconfiguration DHCP utilisant HTTP/TLS

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration DHCP	Séquence normale	Séquence d'échec
CHPSWMT-12	Le serveur HTTP envoie le fichier de configuration du pare-feu (facultatif) Si l'étape CHPSWMT-11 se produit, le serveur HTTP envoie au dispositif PS une réponse HTTP contenant le fichier demandé de configuration du pare-feu.	CHPSWMT-12 DOIT survenir après achèvement de l'étape CHPSWMT-11.	Si le protocole HTTP échoue, continuer le fonctionnement des services de portail mais signaler une erreur et continuer à essayer CHPSWMT-11. Si le traitement du fichier de configuration du pare-feu produit une erreur, continuer et signaler l'erreur comme événement.
CHPSWMT-13	Dialogue initial de fermeture par alerte TLS Le dispositif PS DOIT fermer la session de protocole TLS immédiatement avant d'envoyer le message de préconfiguration terminée.	CHPSWMT-13 DOIT survenir après achèvement de l'étape CHPSWMT-12.	Passer à l'étape CHPSWMT-14. En cas d'échec HTTP, réessayer selon la spécification. Si tous les réessais échouent, signaler une erreur.
CHPSWMT-14	Fermeture de session TCP/IP La session TCP/IP entre le dispositif PS et le serveur HTTP est fermée.	CHPSWMT-14 DOIT survenir après achèvement de l'étape CHPSWMT-13.	Si la fermeture de session TCP/IP échoue, signaler une erreur. Passer à l'étape 15.
CHPSWMT-15	Préconfiguration terminée Sur demande du système de préconfiguration, le dispositif PS est tenu d'informer le système de préconfiguration de l'état de préconfiguration du dispositif PS. Le système de préconfiguration pourrait demander au dispositif PS d'envoyer un message SYSLOG ou un message TRAP du SNMP, ou les deux. Si le dispositif PS achève correctement toutes les étapes requises de CHPSWMT-1 à CHPSWMT-14 et qu'il ait reçu une adresse de serveur SYSLOG dans le message OFFER du protocole DHCP, le dispositif PS DOIT envoyer un message de préconfiguration terminée au serveur SYSLOG avec l'état de préconfiguration réglé à PASS.	CHPSWMT-15 DOIT survenir après achèvement de l'étape CHPSWMT-14.	Si le préinterruption SNMP échoue, le serveur de préconfiguration ne peut pas savoir que le processus de préconfiguration s'est achevé à moins qu'il n'interroge l'objet cabhPsDevProvState.

Tableau 13-2/J.192 – Description des flux en mode de préconfiguration DHCP utilisant HTTP/TLS

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration DHCP	Séquence normale	Séquence d'échec
	Si le dispositif PS achève correctement toutes les étapes de préconfiguration requises de CHPSWMT-1 à CHPSWMT-12 et qu'il ait reçu des paramètres valides pour l'objet docsDevNmAccessGroup identifiant le récepteur de messages de préinterruption (docsDevNmAccessIP) et configurant le message de préinterruption TRAP de préconfiguration terminée (objet cabhPsDevInitTrap) avec la valeur 'lecture seulement avec préinterruption' (réglage de l'objet docsDevNmAccess à '4' voir [RFC 2669].), le dispositif PS DOIT envoyer un message TRAP de préconfiguration terminée (objet cabhPsDevInitTrap) avec les paramètres appropriés, au récepteur de préinterruptions. Si le temporisateur de préconfiguration des services de portail arrive à expiration avant que toutes les étapes requises de CHPSWMT-1 à CHPSWMT-14 soient achevées et que le dispositif PS ait reçu une adresse de serveur SYSLOG dans le message OFFER du protocole DHCP, le dispositif PS DOIT envoyer un message de préconfiguration terminée au serveur SYSLOG avec l'état de préconfiguration réglé à FAIL.		

Tableau 13-2/J.192 – Description des flux en mode de préconfiguration DHCP utilisant HTTP/TLS

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration DHCP	Séquence normale	Séquence d'échec
	Si le temporisateur de préconfiguration des services de portail arrive à expiration avant que toutes les étapes requises de CHPSWMT-1 à CHPSWMT-14 soient achevées et que le dispositif PS ait reçu des paramètres valides pour l'objet docsDevNmAccessGroup identifiant le récepteur de messages de préinterruption (docsDevNmAccessIP) et configurant le message TRAP de préconfiguration terminée (objet cabhPsDevInitTrap) avec la valeur 'lecture seulement avec préinterruptions' (mettre docsDevNmAccess à '4'. Voir [RFC 2669].), le dispositif PS DOIT envoyer un message TRAP d'échec de préconfiguration (objet cabhPsDevInitRetryTrap), au récepteur de préinterruptions. Le dispositif PS met à jour la valeur de l'objet cabhPsDevProvState avec l'état 'pass' (1) quand les étapes de flux de préconfiguration CHPSWMT-1 à CHPSWMT-14 ont été menées à bien. Voir le § 7.5.4.		

13.4 Préconfiguration des services de protail pour la gestion: mode de préconfiguration SNMP

Le dispositif PS demande une adresse de réseau WAN-Man à partir du serveur DHCP de la tête de réseau, à utiliser pour l'échange de messages de gestion entre les fonctions de gestion des services de portail et le système NMS du réseau câblé. Si le dispositif PS détermine, sur la base de la procédure décrite dans le § 7.3.3.2.4, qu'il doit fonctionner en mode de préconfiguration SNMP, ce dispositif PS va sécuriser ses messages de gestion au moyen du protocole SNMPv3, d'après la procédure d'authentification décrite dans le § 11.3.2.

Le système NMS du réseau câblé peut (facultativement) charger le dispositif PS (portail CMP), fonctionnant en mode de préconfiguration SNMP, de télécharger un fichier de configuration du dispositif PS à partir du serveur TFTP. La notification de l'achèvement du processus de préconfiguration est offerte par le processus de signalisation des événements décrit dans le § 6.3.3.2. Le dispositif PS fonctionnera sans fichier de configuration s'il n'est pas déclenché afin de télécharger ce fichier.

La Figure 13-6 décrit les flux de message qui sont à utiliser afin d'accomplir la préconfiguration du dispositif PS quand celui-ci fonctionne en mode de préconfiguration SNMP. Le processus de préconfiguration pour l'interface PS WAN-Man est le même pour le dispositif PS intégré et pour le dispositif PS autonome. La préconfiguration du dispositif PS autonome DEVRAIT intervenir immédiatement après mise sous tension/réinitialisation.

Le processus de préconfiguration pour le réseau WAN-Man d'un dispositif PS fonctionnant en mode de préconfiguration SNMP DOIT survenir par la séquence illustrée dans la Figure 13-6 et décrite en détail dans le Tableau 13-3. Les étapes facultatives sont représentées en grisé dans la Figure 13-6. Ces étapes facultatives peuvent être effectuées immédiatement après l'étape CHPSWMS-13, à un moment ultérieur, ou ne pas être effectuées du tout.

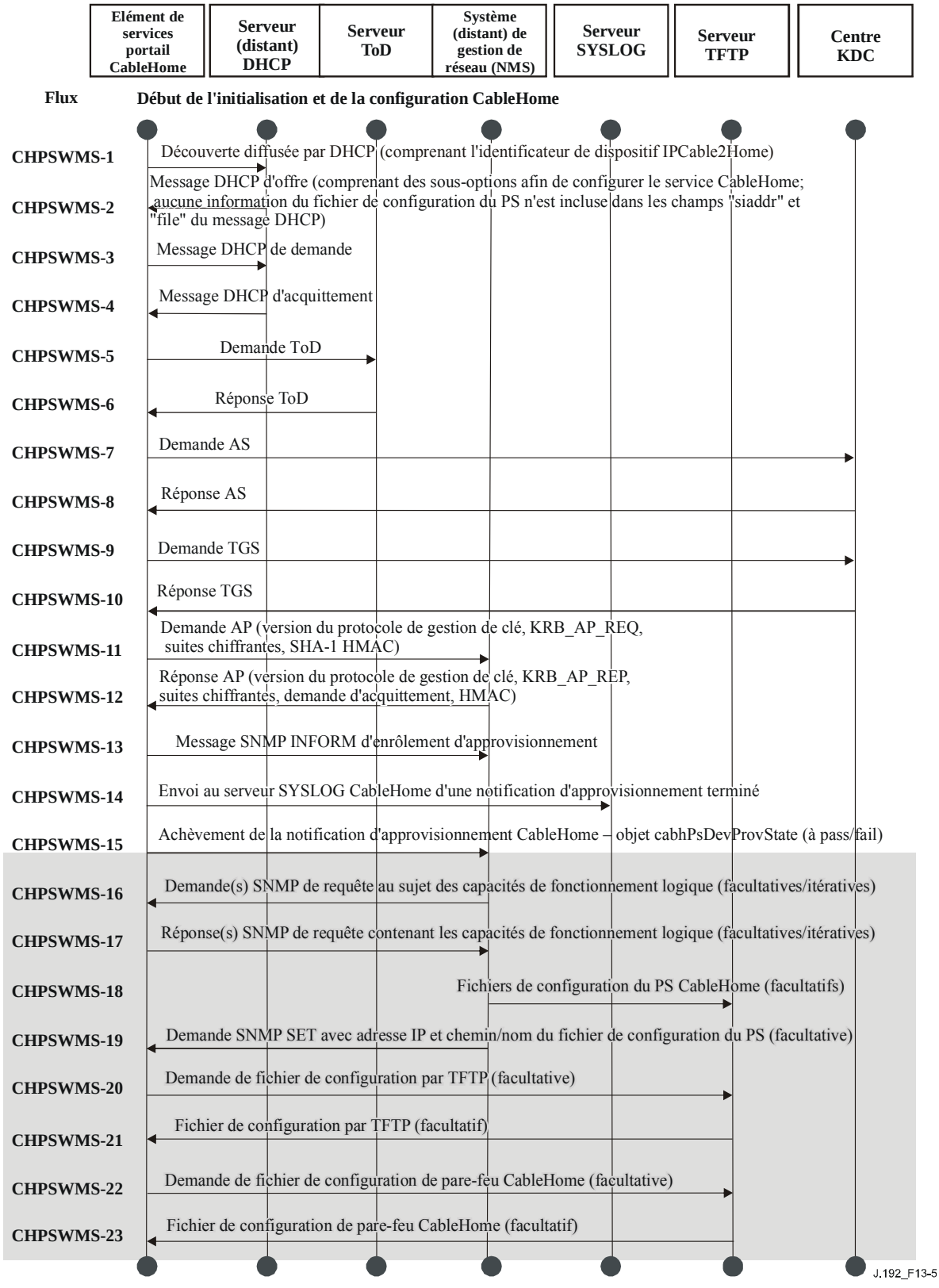


Figure 13-6/J.192 – Processus de préconfiguration pour la gestion des services de portail – Mode de préconfiguration SNMP

Le Tableau 13-3 décrit les étapes individuelles du processus de préconfiguration illustré dans la Figure 13-6.

Tableau 13-3/J.192 – Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration SNMP

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration SNMP	Séquence normale	Séquence d'échec
CHPSWMS-1	Découverte diffusée par DHCP Le portail CDP (client CDC) diffuse un message DHCP DISCOVER afin d'acquérir l'adresse IP du réseau WAN-Man comme décrit dans le § 7.3.3.2.4, "Exigences relatives au client CDC". Le message DHCP DISCOVER diffusé par le client CDC comprend les options obligatoires énumérées dans le Tableau 7-10, "Options DHCP de client CDC contenues dans les messages DISCOVER et REQUEST". Le dispositif PS commence à surveiller la durée écoulée ET règle l'objet cabhPsDevProvState à l'état 'inProgress' (2) quand le client CDC diffuse son message initial DHCP DISCOVER.	Commencer la séquence de préconfiguration	En cas d'échec selon le protocole DHCP, signaler une erreur et continuer à essayer le message de découverte diffusée par DHCP jusqu'à la réussite (retour à l'étape CHPSWMS-1). Si la première tentative d'acquérir une location d'adresse à partir du serveur DHCP du câblo-opérateur échoue, mettre en fonctionnement le serveur CDS comme spécifié dans le § 7.3.3.2.4, "Exigences relatives au client CDC".
CHPSWMS-2	DHCP OFFER	CHPSWMS-2 DOIT survenir après achèvement de l'étape CHPSWMS-1	En cas d'échec selon le protocole DHCP, revenir à CHPSWMS-1 et signaler une erreur.
CHPSWMS-3	DHCP REQUEST Le portail CDP envoie au serveur DHCP approprié un message DHCP REQUEST afin d'accepter le message OFFER du protocole DHCP.	CHPSWMS-3 DOIT survenir après achèvement de l'étape CHPSWMS-2	En cas d'échec selon le protocole DHCP, revenir à CHPSWMS-1.

Tableau 13-3/J.192 – Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration SNMP

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration SNMP	Séquence normale	Séquence d'échec
CHPSWMS-4	DHCP ACK Le serveur DHCP envoie au client CDC un message DHCP ACK qui contient l'adresse IPv4 de l'interface PS WAN-Man et qui est censé inclure le code d'option IPCable2Home 122 avec les sous-options 3, 6, et 10 ET aucune information de fichier de configuration du dispositif PS dans les champs 'siaddr' et 'file' du message DHCP. Le dispositif PS modifie l'objet cabhPsDevProvMode sur la base des informations reçues dans le message ACK du protocole DHCP (voir § 7.3.3.2.4). Le dispositif PS mémorise l'adresse du serveur temporel dans l'objet cabhPsDevTimeServerAddr.	CHPSWMS-4 DOIT survenir après achèvement de l'étape CHPSWMS-3	En cas d'échec selon le protocole DHCP, revenir à CHPSWMS-1 et signaler une erreur.
CHPSWMS-5	Demande d'heure locale (ToD) selon [RFC 868] Le dispositif PS envoie un message de demande d'heure ToD au serveur temporel identifié dans l'option 4 du protocole DHCP du message DHCP ACK.	CHPSWMS-5 DOIT survenir après achèvement de l'étape CHPSWMS-4.	Passer à l'étape CHPSWMS-6
CHPSWMS-6	Réponse d'heure ToD Le serveur temporel ToD est censé répondre avec l'heure locale en format UTC.	CHPSWMS-6 DOIT survenir après achèvement de l'étape CHPSWMS-5.	Réessayer la synchronisation avec le serveur temporel jusqu'à un total de quatre tentatives; en cas d'échec de ces quatre tentatives, essayer la synchronisation avec le prochain serveur temporel énuméré dans l'option 4 du message DHCP ACK; en cas d'échec après quatre tentatives auprès de chaque serveur temporel, signaler une erreur et revenir à CHPSWMS-1.

Tableau 13-3/J.192 – Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration SNMP

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration SNMP	Séquence normale	Séquence d'échec
CHPSWMS-7	Demande de serveur d'application (Note 1) Le dispositif PS envoie le message de demande AS au centre KDC de l'opérateur MSO IPCable2Home fourni dans l'option DHCP 122, sous-option 10, afin de demander un ticket Kerberos.	CHPSWMS-7 DOIT survenir après achèvement de l'étape CHPSWMS-6.	Retourner à CHPSWMS-1. Le dispositif PS lance le fonctionnement du serveur CDS.
CHPSWMS-8	Réponse de serveur d'application AS Le message de réponse AS est reçu du centre KDC de l'opérateur MSO IPCable2Home contenant le ticket Kerberos.	CHPSWMS-8 DOIT survenir après achèvement de l'étape CHPSWMS-7.	Retourner à CHPSWMS-1. Le dispositif PS lance le fonctionnement du serveur CDS.
CHPSWMS-9	Demande de serveur TGS (facultative) Si le dispositif PS a obtenu un ticket distributeur de tickets (TGT) pendant l'étape CHPSWMS-8, ce dispositif PS envoie le message de demande de serveur TGS au serveur de centre KDC d'opérateur MSO dont l'adresse a été transmise au dispositif PS (client CDC) dans la sous-option 10 de l'option DHCP 122.	CHPSWMS-9 DOIT survenir après achèvement de l'étape CHPSWMS-8.	Retourner à CHPSWMS-1. Le dispositif PS lance le fonctionnement du serveur CDS.
CHPSWMS-10	Réponse de serveur TGS (facultative) Le message de réponse de serveur TGS contenant le ticket est reçu du centre KDC de l'opérateur MSO IPCable2Home.	CHPSWMS-10 DOIT survenir après achèvement de l'étape CHPSWMS-9.	Retourner à CHPSWMS-1. Le dispositif PS lance le fonctionnement du serveur CDS.
CHPSWMS-11	Demande de port AP Le dispositif PS envoie le message de demande de port AP au système NMS (gestionnaire SNMP) afin de demander des informations sur la gestion des clés pour le protocole SNMPv3, comme décrit dans le § 11.3, "Infrastructure d'authentification de dispositif PS".	CHPSWMS-11 DOIT survenir après achèvement de l'étape CHPSWMS-10.	Retourner à CHPSWMS-1. Le dispositif PS lance le fonctionnement du serveur CDS.

Tableau 13-3/J.192 – Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration SNMP

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration SNMP	Séquence normale	Séquence d'échec
CHPSWMS-12	Réponse de port AP Le message de réponse AP est reçu du système NMS contenant les informations sur la gestion des clés pour le protocole SNMPv3. Noter que le dispositif PS DOIT établir les clés SNMPv3 et remplir les tables SNMPv3 associées avant d'envoyer un message INFORM selon SNMPv3. Les clés et tables sont établies au moyen des informations contenues dans la réponse de port AP. Voir § 11.3, "Infrastructure d'authentification de dispositif PS".	CHPSWMS-12 DOIT survenir après achèvement de l'étape CHPSWMS-11.	Retourner à CHPSWMS-1. Le dispositif PS lance le fonctionnement du serveur CDS.
CHPSWMS-13	Message INFORM du protocole SNMP d'enrôlement de préconfiguration Après que le dispositif PS fonctionnant en mode de préconfiguration SNMP a établi les clés SNMPv3, ce dispositif DOIT envoyer un message SNMPv3 INFORM (objet cabhPsDevProvEnrollTrap) demandant l'enrôlement dans manager SNMP dont l'adresse IP a été offerte dans l'option 122, sous-option 3, dans le message ACK du message DHCP. Après que le dispositif PS a envoyé l'objet cabhPsDevProvEnrollTrap décrit ci-dessus, le dispositif PS est appelé à commencer la surveillance de la durée écouléle, comme décrit au § 7.4.4.2.2.	CHPSWMS-13 DOIT survenir après achèvement de l'étape CHPSWMS-12.	Retourner à CHPSWMS-1

Tableau 13-3/J.192 – Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration SNMP

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration SNMP	Séquence normale	Séquence d'échec
CHPSWMS-14	Requête SNMP Get (facultative) Si l'une quelconque des capacités additionnelles du dispositif est requise par le système de préconfiguration, celui-ci les demande au dispositif PS au moyen de requêtes Get du protocole SNMPv3. Etape itérative: le système NMS envoie au dispositif PS une ou plusieurs requêtes SNMPv3 GET afin d'obtenir toutes informations requises sur les capacités du dispositif PS. L'application de préconfiguration peut utiliser une requête GetBulk afin d'obtenir plusieurs éléments informatifs dans un seul message.	L'étape CHPSWM-14 n'est pas censée intervenir avant l'achèvement de l'étape CHPSWMS-13.	Retourner à CHPSWMS-1
CHPSWMS-15	Réponse à la requête SNMP Get (facultative) Etape itérative: le dispositif PS répond aux messages de demande Get ou GetBulk du système NMS par une réponse Get à chaque demande GET. A la fin de tous les messages, le système NMS envoie les données demandées à l'application de préconfiguration.	Si l'étape CHPSWMS-14 se produit, l'étape CHPSWMS-15 DOIT survenir après achèvement de l'étape CHPSWMS-14.	N/A
CHPSWMS-16	Création du fichier de configuration Etape facultative: le système de préconfiguration fait appel aux informations des étapes CHPSWMS-16 et CHPSWMS-17 de préconfiguration du dispositif PS afin de créer un fichier de configuration du dispositif PS. Le système de préconfiguration calcule un hachage sur le contenu du fichier de configuration. Ce hachage est envoyé au dispositif PS au cours de l'étape suivante.	Si l'étape CHPSWMS-15 se produit, l'étape CHPSWMS-16 DOIT survenir après achèvement de l'étape CHPSWMS-15.	N/A

Tableau 13-3/J.192 – Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration SNMP

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration SNMP	Séquence normale	Séquence d'échec
CHPSWMS-17	Demande Set (mise à jour) du protocole SNMP (facultative) Le système de préconfiguration peut charger le système NMS d'envoyer un message de commande SNMP de mise à jour (Set) au dispositif PS, contenant l'adresse IP du serveur TFTP, le nom du fichier de configuration du dispositif PS et le hachage du fichier de configuration comme décrit dans le § 7.4.4.2.2, "Déclenchement du téléchargement du fichier de configuration du dispositif PS dans le mode de préconfiguration SNMP". Facultativement, l'adresse IP du serveur TFTP de fichier de configuration de pare-feu, le nom du fichier de configuration du pare-feu et le hachage du fichier de configuration du pare-feu sont inclus dans la requête SET (mise à jour) du protocole SNMP s'il y a un fichier de configuration du pare-feu à charger et cette méthode est choisie afin de le spécifier.	Si l'étape CHPSWMS-16 se produit, l'étape CHPSWMS-17 DOIT survenir après achèvement de l'étape CHPSWMS-16.	Retourner à CHPSWMS-1 si l'ensemble a été reçu, mais qu'il y ait eu une erreur de traitement.
CHPSWMS-18	Demande de transfert TFTP Si le système NMS incite le dispositif PS à télécharger un fichier de configuration du dispositif PS comme décrit dans le § 7.4.4.2.2, le dispositif PS envoie au serveur TFTP une requête Get du protocole TFTP afin de demander le fichier spécifié de configuration du dispositif PS.	Si l'étape CHPSWMS-17 se produit, l'étape CHPSWMS-18 DOIT survenir après achèvement de l'étape CHPSWMS-17.	Passer à l'étape CHPSWMS-17

Tableau 13-3/J.192 – Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration SNMP

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration SNMP	Séquence normale	Séquence d'échec
CHPSWMS-19	Envoi par le serveur TFTP du fichier de configuration Après que le dispositif PS a reçu le fichier de configuration du dispositif PS, celui-ci calcule le hachage du fichier de configuration du dispositif PS et le compare à la valeur reçue au cours de l'étape CHPSWMS-17. Le dispositif PS traite ensuite le fichier de configuration du dispositif PS. Facultativement, l'adresse IP du serveur TFTP de fichier de configuration de pare-feu, le nom du fichier de configuration du pare-feu et le hachage du fichier de configuration du pare-feu sont inclus dans le fichier de configuration du dispositif PS s'il y a un fichier de configuration du pare-feu à charger et c'est la méthode choisie afin de le spécifier.	Si l'étape CHPSWMS-18 se produit, l'étape CHPSWMS-19 se produit après achèvement de l'étape CHPSWMS-18.	Si le téléchargement TFTP échoue, signaler une erreur et continuer à réessayer CHPSWMS-18 (continuer à réessayer le téléchargement du fichier de configuration du dispositif PS). Si le traitement du fichier de configuration produit une erreur, continuer et signaler l'erreur comme événement.
CHPSWMS-20	Message SYSLOG Si le dispositif PS a reçu une adresse de serveur SYSLOG dans le message ACK du protocole DHCP, ce dispositif PS DOIT envoyer au serveur SYSLOG un message "préconfiguration terminée". Cette notification comportera le résultat de succès/échec de l'opération de préconfiguration. Le format général de ce message est défini dans le Tableau B.1, "Evénements définis pour IPCable2Home", ID d'événement 73001100 (voir les notes et détails sur les messages).	CHPSWMS-20 DOIT survenir après achèvement de l'étape CHPSWMS-19.	

Tableau 13-3/J.192 – Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration SNMP

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration SNMP	Séquence normale	Séquence d'échec
CHPSWMS-21	SNMP INFORM Le dispositif PS DOIT envoyer au système NMS un message SNMP INFORM (objet cabhPsDevInitTrap) contenant une notification "préconfiguration terminée" et régler la valeur de l'objet cabhPsDevProvState à pass(1) dans l'une ou l'autre des deux circonstances suivantes: – le dispositif PS n'a pas été incité par le système NMS à télécharger un fichier de configuration PS avant la fin de la durée spécifiée par la valeur de l'objet cabhPsDevProvisioningTimer, qui s'est écoulée depuis l'information d'enrôlement décrite dans l'étape CHPSWMS-13. – le dispositif PS a été incité par le système NMS à télécharger un fichier de configuration PS pendant la durée définie par la valeur de l'objet cabhPsDevProvisioningTimer après l'information d'enrôlement et le dispositif PS a correctement téléchargé et traité ce fichier de configuration PS. Le téléchargement et le traitement du fichier de configuration ne sont pas tenus de s'achever avant la fin de la durée définie par la valeur de cabhPsDevProvisioningTimer depuis l'information d'enrôlement. Le dispositif PS NE DOIT PAS envoyer de message INFORM du protocole SNMP (cabhPsDevInitTrap) contenant une notification de "préconfiguration terminée", et le dispositif PS DOIT régler à fail(3) la valeur de cabhPsDevProvState s'il a été incité par le système NMS à télécharger un fichier de configuration PS avant la fin de la durée spécifiée par la valeur de cabhPsDevProvisioningTimer depuis l'envoi de l'information d'enrôlement ET si le dispositif PS échoue lors du téléchargement et du traitement du fichier de configuration après avoir épuisé le nombre maximal de réessais défini dans le § 7.4.4.2.4: "Fonctionnement après déclenchement".	CHPSWMS-21 DOIT survenir après achèvement de l'étape CHPSWMS-20.	Si le dispositif PS ne reçoit pas de réponse au message INFORM de préconfiguration terminée, le dispositif PS DOIT réessayer d'envoyer le message INFORM (objet cabhPsDevInitTrap), pendant un total de 5 tentatives, à intervalle de 10 secondes. Si tous les 5 essais d'envoi du message cabhPsDevInitTrap échouent, le dispositif PS DOIT relancer le processus d'initialisation, revenir à CHPSWMS-1 et signaler une erreur.

Tableau 13-3/J.192 – Description des flux pour le processus de préconfiguration à l'interface PS WAN-Man en mode de préconfiguration SNMP

Etape du flux	Préconfiguration à l'interface PS WAN-Man: mode de préconfiguration SNMP	Séquence normale	Séquence d'échec
CHPSWMS-22	Demande de transfert TFTP – Fichier de configuration du pare-feu (facultatif) Le dispositif PS envoie au serveur TFTP de configuration de pare-feu une requête Get du protocole TFTP afin de demander le fichier spécifié de données de configuration du pare-feu.	Si l'étape CHPSWMS-22 se produit, elle DOIT survenir après achèvement de l'étape CHPSWMS-21.	Retourner à CHPSWMS-1
CHPSWMS-23	Envoi par le serveur TFTP du fichier de configuration du pare-feu Le serveur TFTP envoie au dispositif PS une réponse TFTP contenant le fichier demandé. Après que le dispositif PS a reçu le fichier de configuration du pare-feu, le dispositif PS calcule le hachage du fichier de configuration du pare-feu et le compare à la valeur reçue au cours de l'étape CHPSWMS-21. Le fichier est alors traité. Voir au § 7.4.4 la description du contenu du fichier de configuration du dispositif PS.	Si l'étape CHPSWMS-22 se produit, l'étape CHPSWMS-23 DOIT survenir après achèvement de l'étape CHPSWMS-22.	Si le téléchargement TFTP échoue, continuer le fonctionnement des services de portail mais signaler une erreur et continuer à réessayer CHPSWMS-22. Si le traitement du fichier de configuration du pare-feu produit une erreur, continuer et signaler l'erreur comme événement.
NOTE 1 – Les étapes CHPSWMS-5 à CHPSWMS-8 sont facultatives dans certains cas. Voir les détails au § 11. NOTE 2 – Les opérations de requête SNMP Get et de réponse à cette requête sont facultatives, selon que des informations supplémentaires sont nécessaires afin de former un fichier de configuration du dispositif PS et également selon qu'un fichier de configuration du dispositif PS est nécessaire.			

13.4.1 Téléchargement du fichier de configuration de l'interface PS WAN-Man

Le dispositif PS fonctionnant en mode de préconfiguration SNMP pourrait contenir suffisamment d'informations par défaut fixées à l'usine afin de permettre le fonctionnement du côté réseau local ou du côté réseau régional ou des deux côtés sans téléchargement de fichier de configuration du dispositif PS. Si le dispositif PS doit fonctionner en mode de préconfiguration SNMP, le système NMS pourrait déclencher le téléchargement d'un fichier de configuration du dispositif PS pour la préconfiguration initial afin de remplacer la valeur par défaut fixée à l'usine ou afin d'offrir des informations supplémentaires.

Le fichier de configuration du pare-feu contient des informations permettant d'approvisionner la fonction de pare-feu. L'indication visant à télécharger un fichier de configuration du pare-feu arrivera soit dans le fichier de configuration du dispositif PS ou par une commande SNMP de mise à jour (Set) pendant l'initialisation.

13.4.2 Temporisateur de préconfiguration des services de portail

Un temporisateur de préconfiguration est offert afin de garantir que le dispositif PS, s'il n'est pas incité à télécharger un fichier de configuration PS, continuera le processus de préconfiguration en mode SNMP. Le dispositif PS est tenu de surveiller la durée écoulée à partir du moment où il envoie le message Inform d'enrôlement de préconfiguration SNMP. S'il n'est pas incité à télécharger un fichier de configuration PS dans l'intervalle de temps défini par la valeur du temporisateur de préconfiguration, le dispositif PS signale que la préconfiguration est terminée en émettant un message SNMP Inform de préconfiguration terminée et en réglant la valeur de l'objet cabhPsDevProvState à pass(1). L'objet de temporisateur, cabhPsDevProvTimer, a une valeur d'initialisation par défaut de 5 minutes. Pour plus de détails, voir le § 7.4.4.2.2.

13.4.3 Messages INFORM d'enrôlement de préconfiguration/de préconfiguration terminée

Pour le dispositif PS fonctionnant en mode de préconfiguration SNMP seulement, le message INFORM d'enrôlement de préconfiguration (objet cabhPsDevProvEnrollTrap) permet au serveur de préconfiguration de déterminer que le dispositif PS est prêt pour le fichier de configuration du dispositif PS.

En mode de préconfiguration DHCP ou en mode de préconfiguration SNMP, le message TRAP de préconfiguration terminée (objet cabhPsDevInitTrap) indique si la séquence de préconfiguration s'est achevée correctement ou non.

13.4.4 Préconfiguration de journalisation SYSLOG

L'adresse IP du serveur Syslog DOIT être préconfigurée par le processus DHCP. L'événement Syslog ne sera pas émis si l'adresse IP du serveur Syslog n'est pas configurée.

13.4.5 Signalisation des états de préconfiguration et des erreurs

Comme indiqué dans les Tableaux 13-1 et 13-3, un échec au cours des étapes du processus de préconfiguration provoque généralement le redémarrage du processus à la première étape, CHPSWMD-1 ou CHPSWMS-1.

13.5 Processus de préconfiguration de l'interface PS WAN-Data

Le dispositif PS demande zéro, une ou plusieurs adresses de réseau WAN-Data au serveur DHCP situé dans le réseau câblé. Ces adresses serviront à l'échange de données entre éléments connectés à l'internet et dispositifs IP de réseau local.

Il n'y a aucune différence entre les modes de préconfiguration DHCP et SNMP en terme de fonctionnement de l'interface PS WAN-Data.

La Figure 13-7 illustre les flux de message qui sont à utiliser afin d'accomplir la préconfiguration des adresses IP d'interface PS WAN-Data. Le processus de préconfiguration des adresses de réseau WAN-Data d'un dispositif PS est le même pour le dispositif PS intégré avec un câblo-modem DOCSIS et pour le dispositif PS autonome.

Si le processus de préconfiguration pour l'adresse (les adresses) d'interface PS WAN-Data se produit, il DOIT suivre la séquence illustrée dans la Figure 13-7 et décrite en détail dans le Tableau 13-4.

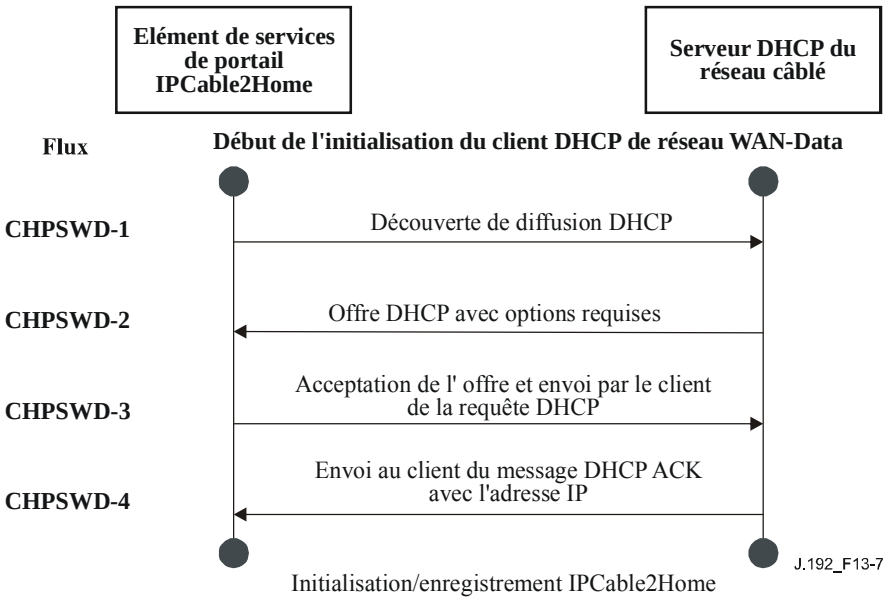


Figure 13-7/J.192 – Processus de préconfiguration de l'interface PS WAN-Data

Tableau 13-4/J.192 – Flow descriptions for PS WAN-Data provisioning process

Etape du flux	Préconfiguration d'adresse à l'interface PS/WAN-Data	Séquence normale	Séquence anormale
CHPSWD-1	Découverte de diffusion DHCP Le dispositif PS diffuse un message DHCP DISCOVER contenant les options obligatoires énumérées dans le Tableau 7-10, ainsi que les options CDC du DHCP contenues dans les messages DISCOVER et REQUEST.	Passer à l'étape CHPSWD-2.	En cas d'échec du protocole DHCP, répéter CHPSWD-1.
CHPSWD-2	Paquet DHCP OFFER Le serveur DHCP situé en tête de réseau reçoit le paquet DHCP DISCOVER, attribue une adresse IP extraite de la réserve WAN-Data, construit un paquet DHCP OFFER et le transmet à l'agent de relais DHCP [RFC 3046] contenu dans le système CMTS.	Passer à l'étape CHPSWD-3.	En cas d'échec, le client active la temporisation du protocole DHCP et l'étape CHPSWD-1 est répétée.

Tableau 13-4/J.192 – Flow descriptions for PS WAN-Data provisioning process

Etape du flux	Préconfiguration d'adresse à l'interface PS/WAN-Data	Séquence normale	Séquence anormale
CHPSWD-3	Message DHCP REQUEST Le portail CDP envoie un message DHCP REQUEST au serveur DHCP sélectionné afin d'accepter le paquet DHCP OFFER conformément aux exigences du client [voir RFC 2131].	L'étape CHPSWD-3 DOIT intervenir après l'achèvement de l'étape CHPSWD-2.	En cas d'échec du protocole DHCP, revenir à l'étape CHPSWD-1.
CHPSWD-4	DHCP ACK Le serveur DHCP envoie au portail CDP un message DHCP ACK contenant l'adresse IPv4 de l'interface PS/WAN Data.	L'étape CHPSWD-4 DOIT intervenir après l'achèvement de l'étape CHPSWD-3. La préconfigura-tion se termine par l'achèvement de l'étape CHPSWD-4.	En cas d'échec du protocole DHCP, revenir à l'étape CHPSWD-1.

13.6 Processus de préconfiguration: dispositif IP de réseau local situé dans le secteur LAN-Pass

Certaines applications de réseau local domestique ne fonctionneront pas correctement avec une adresse de couche Réseau convertie. Afin de tenir compte de ces applications, le dispositif PS est activé de façon à fonctionner en mode de transfert (dérivation transparente). Comme décrit dans le § 8.3.3.1, "Modes de traitement des paquets", la dérivation se produit quand le système NMS du réseau câblé règle le mode primaire de traitement de paquet (objet cabhCapPrimaryMode) à 'transfert', ou lorsqu'il écrit les adresses MAC de dispositifs IP de réseau local individuels dans la table de transfert (objet cabhCapPassthroughTable). Quand le dispositif PS a été configuré de façon à dériver le trafic pour un dispositif IP de réseau local, les messages DHCP DISCOVER et REQUEST envoyés par ce dispositif IP de réseau local seront servis par le serveur DHCP du réseau câblé et non par le serveur CDS.

Un dispositif IP de réseau local non conforme à l'environnement IPCable2Home est censé mettre en œuvre un client du protocole DHCP et demander une location d'adresse IP par protocole DHCP [RFC 2131]. Un dispositif IP de réseau local conforme à l'environnement IPCable2Home, c'est-à-dire qui met en œuvre la fonctionnalité de point extrême définie dans la présente Recommandation, est tenu d'implémenter un client du protocole DHCP et de demander une location d'adresse IP par protocole DHCP.

Annexe A

Objets de base MIB

La présente annexe énumère tous les objets de base MIB requis, comme indiqué dans le § 6.3.3.1.4.1, "Exigences relatives au protocole SNMP" et dans le § 6.3.3.1.4.7, "Exigences relatives aux bases MIB IPCable2Home". Elle indique les exigences de persistance de chaque objet énuméré.

Le terme "persistant", tel qu'il s'applique à la présente annexe, est défini ci-dessous:

persistant: cet adjectif exprime l'exigence que le dispositif PS conserve la valeur d'un objet de base MIB configurable (par le gestionnaire ou par le dispositif PS lui-même) après un réamorçage ou une réinitialisation du dispositif PS.

Dans le cas des objets de base MIB avec entrée 'Oui' dans la colonne "Objet persistant", la valeur de cet objet immédiatement après un réamorçage ou une réinitialisation du dispositif PS, DOIT être celle qui précédait immédiatement le réamorçage ou la réinitialisation.

Dans le cas des objets de base MIB avec entrée 'Non' dans la colonne "Objet persistant", ces objets DOIVENT être réglés à leur valeur par défaut fixée à l'usine (DEFVAL) ou, s'il n'a aucune valeur par défaut, DOIVENT être réglés à zéro ou à 'néant' selon le cas, immédiatement après un réamorçage ou une réinitialisation du dispositif PS.

Dans le cas des objets de base MIB avec entrée "-" dans la colonne "Objet persistant", une seule des conditions suivantes est applicable:

- la valeur de cet objet, immédiatement après réamorçage ou réinitialisation du dispositif PS, est dépendante de l'implémentation par le vendeur parce qu'il n'y a aucune exigence spécifique concernant cette valeur après réamorçage ou réinitialisation du dispositif PS;
- la valeur de cet objet est déterministe, sur la base de la description de base MIB. (La valeur de l'objet est fixe ou peut être déduite de valeurs connues après le réamorçage ou la réinitialisation du dispositif PS.)

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
mib-2[RFC 1213] system			
sysDescr	lecture seule	–	N/A
sysObjectID	lecture seule	–	N/A
sysUpTime	lecture seule	–	N/A
sysContact	lecture-écriture	Oui	1
sysName	lecture-écriture	Oui	1
sysLocation	lecture-écriture	Oui	1
sysServices	lecture seule	–	N/A
interfaces [RFC 2863]			
ifNumber	lecture seule	–	N/A
ifTable/ifEntry			
ifIndex	lecture seule	–	N/A
ifDescr	lecture seule	–	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
ifType	lecture seule	–	N/A
ifMtu	lecture seule	–	N/A
ifSpeed	lecture seule	–	N/A
ifPhysAddress	lecture seule	–	N/A
ifAdminStatus	lecture-écriture	Non[2]	N/A
ifOperStatus	lecture seule	–	N/A
ifLastChange	lecture seule	–	N/A
ifInOctets	lecture seule	–	N/A
ifInUcastPkts	lecture seule	–	N/A
ifInDiscards	lecture seule	–	N/A
ifInErrors	lecture seule	–	N/A
ifInUnknownProtos	lecture seule	–	N/A
ifOutOctets	lecture seule	–	N/A
ifOutUcastPkts	lecture seule	–	N/A
ifOutDiscards	lecture seule	–	N/A
ifOutErrors	lecture seule	–	N/A
[2] ifAdminStatus est persistant pour ifIndex = 254 et n'est pas persistant pour d'autres valeurs de ifIndex.			
ip [RFC 2011]			
ipForwarding	lecture-écriture	Non	N/A
ipDefaultTTL	lecture-écriture	Non	N/A
ipInReceives	lecture seule	–	N/A
ipInHdrErrors	lecture seule	–	N/A
ipInAddrErrors	lecture seule	–	N/A
ipForwDatagrams	lecture seule	–	N/A
ipInUnknownProtos	lecture seule	–	N/A
ipInDiscards	lecture seule	–	N/A
ipInDelivers	lecture seule	–	N/A
ipOutRequests	lecture seule	–	N/A
ipOutDiscards	lecture seule	–	N/A
ipOutNoRoutes	lecture seule	–	N/A
ipReasmTimeout	lecture seule	–	N/A
ipReasmReqds	lecture seule	–	N/A
ipReasmOKs	lecture seule	–	N/A
ipReasmFails	lecture seule	–	N/A
ipFragOKs	lecture seule	–	N/A
ipFragFails	lecture seule	–	N/A
ipFragCreates	lecture seule	–	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
ipNetToMediaTable/ ipNetTo MediaEntry			
ipNetToMediaIfIndex	lecture seule	Non	N/A
ipNetToMediaPhyAddress	lecture seule	Non	N/A
ipNetToMediaNetAddress	lecture seule	Non	N/A
ipNetToMediaType	lecture seule	Non	N/A
icmp			
icmpInMsgs	lecture seule	–	N/A
icmpInErrors	lecture seule	–	N/A
icmpInDestUnreachs	lecture seule	–	N/A
icmpInTimeExcds	lecture seule	–	N/A
icmpInParmProbs	lecture seule	–	N/A
icmpInSrcQuenchs	lecture seule	–	N/A
icmpInRedirects	lecture seule	–	N/A
icmpInEchos	lecture seule	–	N/A
icmpInEchosReps	lecture seule	–	N/A
icmpInTimestamps	lecture seule	–	N/A
icmpInTimestampsReps	lecture seule	–	N/A
icmpInAddrMasks	lecture seule	–	N/A
icmpInAddrMaskReps	lecture seule	–	N/A
icmpOutMsgs	lecture seule	–	N/A
icmpOutErrors	lecture seule	–	N/A
icmpOutDestUnreachs	lecture seule	–	N/A
icmpOutTimeExcds	lecture seule	–	N/A
icmpOutParmProbs	lecture seule	–	N/A
icmpOutSrcQuenchs	lecture seule	–	N/A
icmpOutRedirects	lecture seule	–	N/A
icmpOutEchos	lecture seule	–	N/A
icmpOutEchosReps	lecture seule	–	N/A
icmpOutTimestamps	lecture seule	–	N/A
icmpOutTimestampReps	lecture seule	–	N/A
icmpOutAddrMasks	lecture seule	–	N/A
icmpOutAddrMaskReps	lecture seule	–	N/A
udp [RFC 2013]			
udpInDatagrams	lecture seule	–	N/A
udpNoPorts	lecture seule	–	N/A
udpInErrors	lecture seule	–	N/A
udpOutDatagrams	lecture seule	–	N/A
udpTable/udpEntry			
udpLocalAddress	lecture seule	–	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
udpLocalPort	lecture seule	–	N/A
transmission [draft-ietf-ipcdn-bpiplus-mib-05]			
docsIfMib			
docsBpi2MIB			
docsBpi2MIBObjects			
docsBpi2CmObjects			
docsBpi2CmCertObjects			
docsBpi2CodeDownloadGroup			
docsBpi2CodeDownloadStatusCode	lecture seule	–	N/A
docsBpi2CodeDownloadStatusString	lecture seule	–	N/A
docsBpi2CodeMfgOrgName	lecture seule	Oui	1
docsBpi2CodeMfgCodeAccessStart	lecture seule	Oui	1
docsBpi2CodeMfgCvcAccessStart	lecture seule	Oui	1
docsBpi2CodeCoSignerOrg Name	lecture seule	–	N/A
docsBpi2CodeCoSignerCode AccessStart	lecture seule	–	N/A
docsBpi2CodeCoSignerCvc AccessStart	lecture seule	–	N/A
docsBpi2CodeCvcUpdate	lecture-écriture	Non	N/A
snmp [RFC 3418]			
snmpInPkts	lecture seule	–	N/A
snmpInBadVersions	lecture seule	–	N/A
snmpInBadCommunityNames	lecture seule	–	N/A
snmpInBadCommunityUses	lecture seule	–	N/A
snmpInASNParseErrs	lecture seule	–	N/A
snmpEnableAuthenTraps	lecture-écriture	Non	N/A
snmpSilentDrops	lecture seule	–	N/A
ifMIB [RFC 2863] **ifMIBOjects**			
ifXTable/ifXEntry			
ifName	lecture seule	–	N/A
ifInMulticastPkts	lecture seule	–	N/A
ifInBroadcastPkts	lecture seule	–	N/A
ifOutMulticastPkts	lecture seule	–	N/A
ifOutBroadcastPkts	lecture seule	–	N/A
ifLinkUpDownTrapEnable	lecture-écriture	Non	N/A
ifHighSpeed	lecture seule	–	N/A
ifPromiscuousMode	lecture-écriture	Non	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
ifConnectorPresent	lecture seule	–	N/A
ifAlias	lecture-écriture	Non	N/A
ifCounterDiscontinuityTime	lecture seule	–	N/A
ifStackTable/ifStackEntry			
ifStackHigherLayer	lecture seule	–	N/A
ifStackLowerLayer	lecture seule	–	N/A
ifStackStatus	lecture seule	–	N/A
docsDev [RFC 2669] **docsDevMIBObjects**			
docsDevNmAccessTable/ *docsDevNmAccessEntry*			
docsDevNmAccessIndex	non accessible	–	N/A
docsDevNmAccessIp	lecture-création	Non	N/A
docsDevNmAccessIpMask	lecture-création	Non	N/A
docsDevNmAccessCommunity	lecture-création	Non	N/A
docsDevNmAccessControl	lecture-création	Non	N/A
docsDevNmAccessInterfaces	lecture-création	Non	N/A
docsDevNmAccessStatus	lecture-création	Non	N/A
docsDevNmAccessTrapVersion	lecture-création	Non	N/A
docsDevSoftware			
docsDevSwServer	lecture-écriture	Oui	1
docsDevSwFilename	lecture-écriture	Oui	1
docsDevSwAdminStatus	lecture-écriture	Oui	1
docsDevSwOperStatus	lecture seule	Oui	1
docsDevSwCurrentVers	lecture seule	–	N/A
docsDevEvent			
docsDevEvControl	lecture-écriture	Non	N/A
docsDevEvSyslog	lecture-écriture	Non	N/A
docsDevEvThrottleAdminStatus	lecture-écriture	Non	N/A
docsDevEvThrottleInhibited	lecture seule	–	N/A
docsDevEvThrottleThreshold	lecture-écriture	Non	N/A
docsDevEvThrottleInterval	lecture-écriture	Non	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
docsDevEvControlTable/ docsDevEvControlEntry			
docsDevEvPriority	non accessible	–	N/A
docsDevEvReporting	lecture-écriture	Non	N/A
docsDevEventTable/ docsDevEventEntry			
docsDevEvIndex	non accessible	–	N/A
docsDevEvFirstTime	lecture seule	Oui	10
docsDevEvLastTime	lecture seule	Oui	10
docsDevEvCounts	lecture seule	Oui	10
docsDevEvLevel	lecture seule	Oui	10
docsDevEvId	lecture seule	Oui	10
docsDevEvText	lecture seule	Oui	10
docsDevFilter			
docsDevFilterIpTable/ docsDevFilterIpEntry			
docsDevFilterIpIndex	non accessible	–	N/A
docsDevFilterIpStatus	lecture-création	Oui	40
docsDevFilterIpControl	lecture-création	Oui	40
docsDevFilterIpIfIndex	lecture-création	Oui	40
docsDevFilterIpDirection	lecture-création	Oui	40
docsDevFilterIpBroadcast	lecture-création	Non	N/A
docsDevFilterIpSaddr	lecture-création	Oui	40
docsDevFilterIpSmask	lecture-création	Oui	40
docsDevFilterIpDaddr	lecture-création	Oui	40
docsDevFilterIpDmask	lecture-création	Oui	40
docsDevFilterIpProtocol	lecture-création	Oui	40
docsDevFilterIpSourcePortLow	lecture-création	Oui	40
docsDevFilterIpSourcePortHigh	lecture-création	Oui	40
docsDevFilterIpDestPortLow	lecture-création	Oui	40
docsDevFilterIpDestPortHigh	lecture-création	Oui	40
docsDevFilterIpMatches	lecture seule	–	N/A
docsDevFilterIpTos	lecture-création	Non	N/A
docsDevFilterIpTosMask	lecture-création	Non	N/A
docsDevFilterIpContinue	lecture seule	=	N/A
docsDevFilterIpPolicyId	lecture-création	Non	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
dot11			
dot11StationConfigTable/			
dot11StationConfigEnty[3]			
dot11PrivacyOptionImplemented	lecture seule	–	N/A
dot11DesiredSSID	lecture-écriture	Oui	1
dot11OperationalRateSet	lecture-écriture/ lecture seule	Oui/ –	1/N/A
dot11BeaconPeriod	lecture-écriture/ lecture seule	Oui/ –	1/N/A
dot11DTIMPeriod	lecture-écriture/ lecture seule	Oui/ –	1/N/A
dot11WEPDefaultKeysTable/			
dot11WEPDefaultKeysEntry[3]			
dot11WEPDefaultKeyIndex	non accessible	N/A	N/A
dot11WEPDefaultKeyValue	lecture-écriture	Oui	4
dot11PrivacyTable			
dot11PrivacyEntry[3]			
dot11PrivacyInvoked	lecture-écriture	Oui	1
dot11WEPDefaultKeyID	lecture-écriture	Oui	1
dot11OperationTable/			
dot11OperationEntry[3]			
dot11MACAddress	lecture seule	–	N/A
dot11RTSThreshold	lecture-écriture/ lecture seule	Oui/ –	1/N/A
dot11FragmentationThreshold	lecture-écriture/ lecture seule	Oui/ –	1/N/A
dot11PhyTxPowerTable/			
dot11PhyTxPowerEntry[3]			
dot11NumberSupportedPowerLevels	lecture seule	–	N/A
dot11TxPowerLevel1	lecture seule	–	N/A
dot11TxPowerLevel2	lecture seule	–	N/A
dot11TxPowerLevel3	lecture seule	–	N/A
dot11TxPowerLevel4	lecture seule	–	N/A
dot11TxPowerLevel5	lecture seule	–	N/A
dot11TxPowerLevel6	lecture seule	–	N/A
dot11TxPowerLevel7	lecture seule	–	N/A
dot11TxPowerLevel8	lecture seule	–	N/A
dot11CurrentTxPowerLevel	lecture-écriture	Oui	1

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
dot11PhyDSSSTable/			
dot11PhyDSSSEntry[3]			
dot11CurrentChannel	lecture-écriture	Oui	1
dot11PhyOFDMTable/			
dot11PhyOFDMEntry[3]			
dot11CurrentFrequency	lecture-écriture	Oui	1
dot11FrequencyBandsSupported	lecture seule	-	N/A

[3] Les objets de base MIB assortis d'exigences relatives au nombre d'entrées d'objet persistant sont indiqués pour chaque interface avec réseau sans fil prise en charge, acceptant la fonctionnalité de l'entrée dans la base MIB.

private			
enterprises			
cableLabs			
clabProject			
clabProjCableHome			
cabhPsDevMib			
cabhPsDevBase			
cabhPsDevDateTime	lecture-écriture	Non	N/A
cabhPsDevResetNow	lecture-écriture	Non	N/A
cabhPsDevSerialNumber	lecture seule	–	N/A
cabhPsDevHardwareVersion	lecture seule	–	N/A
cabhPsDevWanManMacAddress	lecture seule	–	N/A
cabhPsDevWanDataMacAddress	lecture seule	–	N/A
cabhPsDevTypeIdentifier	lecture seule	–	N/A
cabhPsDevSetToFactory	lecture-écriture	Non	N/A
cabhPsDevTodSyncStatus	lecture seule	–	N/A
cabhPsDevProvMode	lecture seule	–	N/A
cabhPsDevLastSetToFactory	lecture seule	–	N/A
cabhPsDevTrapControl	lecture-écriture	Non	N/A
cabhPsDevProv			
cabhPsDevProvisioningTimer	lecture-écriture	Non	N/A
cabhPsDevProvConfigFile	lecture-écriture	Non	N/A
cabhPsDevProvConfigHash	lecture-écriture	Non	N/A
cabhPsDevProvConfigFileSize	lecture seule	–	N/A
cabhPsDevProvConfigFileStatus	lecture seule	–	N/A
cabhPsDevProvConfigTLVProcessed	lecture seule	–	N/A
cabhPsDevProvConfigTLVRejected	lecture seule	–	N/A
cabhPsDevProvSolicitedKeyTimeout	lecture-écriture	Oui	1

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
cabhPsDevProvState	lecture seule	–	N/A
cabhPsDevProvAuthState	lecture seule	–	N/A
cabhPsDevTimeServerAddrType	lecture seule	–	N/A
cabhPsDevTimeServerAddr	lecture seule	–	N/A
cabhPsDevAttrib **cabhPsDevPsAttrib**			
cabhPsDevPsDeviceType	lecture seule	–	N/A
cabhPsDevPsManufacturerURL	lecture seule	–	N/A
cabhPsDevPsModelURL	lecture seule	–	N/A
cabhPsDevPsModelUPC	lecture seule	–	N/A
cabhPsDevPsStats			
cabhPsDevLanIpTrafficCountersReset	lecture-écriture	Non	N/A
cabhPsDevLanIpTrafficCountersLastReset	lecture seule	–	N/A
cabhPsDevLanIpTrafficEnabled	lecture-écriture	Non	N/A
cabhPsDevLanIpTrafficTable/cabhPsDev LanIpTrafficEntry			
cabhPsDevLanIpTrafficIndex	non accessible	–	N/A
cabhPsDevLanIpTrafficInetAddressType	lecture seule	–	N/A
cabhPsDevLanIpTrafficInetAddress	lecture seule	–	N/A
cabhPsDevLanIpTrafficInOctets	lecture seule	–	N/A
cabhPsDevLanIpTrafficOutOctets	lecture seule	–	N/A
cabhPsDevPsAccessControl			
cabhPsDevAccessControlEnable	lecture-écriture	Non	N/A
cabhPsDevAccessControlTable/ cabhPsDevAccessControlEntry			
cabhPsDevAccessControlIndex	non accessible	–	N/A
cabhPsDevAccessControlPhysAddr	lecture-écriture	Oui	20
cabhPsDevAccessControlRowStatus	lecture-création	Oui	20
cabhPsDevPsMisc **cabhPsDevPsUI**			
cabhPsDevUILogin	lecture-écriture	Oui	1
cabhPsDevUIPassword	lecture-écriture	Oui	1
cabhPsDevUISelection	lecture-écriture	Oui	1
cabhPsDevUIServerURL	lecture-écriture	Oui	1
cabhPsDevUISelectionDisabledBodyText	lecture-écriture	Oui	1

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
cabhPsDev802dot11BaseTable/			
cabhPsDev802dot11BaseEntry[4]			
cabhPsDev802dot11BaseSetToDefault	lecture-écriture	–	N/A
cabhPsDev802dot11BaseLastSetToDefault	lecture seule	–	N/A
cabhPsDev802dot11BaseAdvertiseSSID	lecture-écriture	Oui	1
cabhPsDev802dot11BasePhyCapabilities	lecture seule	–	N/A
cabhPsDev802dot11BasePhyOperMode	lecture-écriture	Oui	1
cabhPsDev802dot11SecTable/			
cabhPsDev802dot11SecEntry[4]			
cabhPsDev802dot11SecCapabilities	lecture seule	-	N/A
cabhPsDev802dot11SecOperMode	lecture-écriture	Oui	1
cabhPsDev802dot11SecPassPhraseToWEP Key	lecture-écriture	Oui	1
cabhPsDev802dot11SecUsePassPhraseTo WEPKeyAlg	lecture-écriture	Oui	1
cabhPsDev802dot11SecPSKPassPhrase ToKey	lecture-écriture	Oui	1
cabhPsDev802dot11SecWPAPreSharedKey	lecture-écriture	Oui	1
cabhPsDev802dot11SecWPARekeyTime	lecture-écriture	Oui	1
cabhPsDev802dot11SecControl	lecture-écriture	Non	N/A
cabhPsDev802dot11SecCommitStatus	lecture seule	Non	N/A

[4] Les objets de base MIB assortis d'exigences relatives au nombre d'entrées d'objet persistant sont indiqués pour chaque interface avec réseau sans fil prise en charge, acceptant la fonctionnalité de l'entrée dans la base MIB.

cabhPsDevUpnp **cabhPsDevUpnpBase**			
cabhPsDevUpnpEnabled	lecture-écriture	Oui	1
cabhPsDevUpnpCommands			
cabhPsDevUpnpCommandIpType	lecture-écriture	Non	N/A
cabhPsDevUpnpCommandIp	lecture-écriture	Non	N/A
cabhPsDevUpnpCommand	lecture-écriture	Non	N/A
cabhPsDevUpnpCommandUpdate	lecture-écriture	Non	N/A
cabhPsDevUpnpLastCommandUpdate	lecture seule	–	N/A
cabhPsDevUpnpCommandStatus	lecture seule	–	N/A
cabhPsDevUpnpInfoTable/ *cabhPsDevUpnpInfoEntry*			
cabhPsDevUpnpInfoXmlFragment	lecture seule	–	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
cabhSecMib *cabhSecCertObjects*			
cabhSecCertPsCert	lecture seule	–	1
cabhSec2FwObjects **cabhSec2FwBase**			
cabhSec2FwEnable	lecture-écriture	Oui	N/A
cabhSec2FwPolicyFileURL	lecture-écriture	Non	N/A
cabhSec2FwPolicyFileHash	lecture-écriture	Non	N/A
cabhSec2FwPolicyFileOperStatus	lecture seule	–	N/A
cabhSec2FwPolicyFileCurrentVersion	lecture-écriture	Oui	N/A
cabhSec2FwClearPreviousRuleset	lecture-écriture	Non	N/A
cabhSec2FwPolicySelection	lecture-écriture	Oui	N/A
cabhSec2FwEventSetToFactory	lecture-écriture	Non	N/A
cabhSec2FwEventLastSetToFactory	lecture seule	–	N/A
cabhSec2FwPolicySuccessfulFileURL	lecture seule	Oui	1
cabhSec2FwConfiguredRulesetPriority	lecture seule	Oui	1
cabhSec2FwClearLocalRuleset	lecture-écriture	Non	N/A
cabhSec2FwEvent			
cabhSec2FwEventControlTable/ *cabhSec2FwEventControlEntry/*			
cabhSec2FwEventType	non accessible	–	N/A
cabhSec2FwEventEnable	lecture-écriture	Non	N/A
cabhSec2FwEventThreshold	lecture-écriture	Non	N/A
cabhSec2FwEventInterval	lecture-écriture	Non	N/A
cabhSec2FwEventCount	lecture seule	–	N/A
cabhSec2FwEventLogReset	lecture-écriture	Non	N/A
cabhSec2FwEventLogLastReset	lecture seule	–	N/A
cabhSec2FwLogTable *cabhSec2FwLogEntry*			
cabhSec2FwLogIndex	non accessible	–	N/A
cabhSec2FwLogEventType	lecture seule	Oui	40
cabhSec2FwLogEventPriority	lecture seule	Oui	40
cabhSec2FwLogEventId	lecture seule	Oui	40
cabhSec2FwLogTime	lecture seule	Oui	40
cabhSec2FwLogIpProtocol	lecture seule	Oui	40

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
cabhSec2FwLogIpSourceAddr	lecture seule	Oui	40
cabhSec2FwLogIpDestAddr	lecture seule	Oui	40
cabhSec2FwLogIpSourcePort	lecture seule	Oui	40
cabhSec2FwLogIpDestPort	lecture seule	Oui	40
cabhSec2FwLogMessageType	lecture seule	Oui	40
cabhSec2FwLogReplayCount	lecture seule	Oui	40
cabhSec2FwLogMIBPointer	lecture seule	Oui	40
cabhSec2FwLogMatchingFilterTableName	lecture seule	Oui	40
cabhSec2FwLogMatchingFilterTableIndex	lecture seule	Oui	40
cabhSec2FwLogMatchingFilterDescr	lecture seule	Oui	40
cabhSec2FwFilter			
cabhSec2FwFilterScheduleTable/ cabhSec2FwFilterScheduleEntry			
cabhSec2FwFilterScheduleStartTime	lecture-création	Oui	40
cabhSec2FwFilterScheduleEndTime	lecture-création	Oui	40
cabhSec2FwFilterScheduleDOW	lecture-création	Oui	40
cabhSec2FwFilterScheduleDescr	lecture-création	Oui	40
cabhSec2FwLocalFilterIpTable/ cabhSec2FwLocalFilterIpEntry			
cabhSec2FwLocalFilterIpIndex	non accessible	–	N/A
cabhSec2FwLocalFilterIpStatus	lecture-création	Oui	40
cabhSec2FwLocalFilterIpControl	lecture-création	Oui	40
cabhSec2FwLocalFilterIpIfIndex	lecture-création	Oui	40
cabhSec2FwLocalFilterIpDirection	lecture-création	Oui	40
cabhSec2FwLocalFilterIpSaddr	lecture-création	Oui	40
cabhSec2FwLocalFilterIpSmask	lecture-création	Oui	40
cabhSec2FwLocalFilterIpDaddr	lecture-création	Oui	40
cabhSec2FwLocalFilterIpDmask	lecture-création	Oui	40
cabhSec2FwLocalFilterIpProtocol	lecture-création	Oui	40
cabhSec2FwLocalFilterIpSourcePortLow	lecture-création	Oui	40
cabhSec2FwLocalFilterIpSourcePortHigh	lecture-création	Oui	40
cabhSec2FwLocalFilterIpDestPortLow	lecture-création	Oui	40
cabhSec2FwLocalFilterIpDestPortHigh	lecture-création	Oui	40
cabhSec2FwLocalFilterIpMatches	lecture seule	Oui	40
cabhSec2FwLocalFilterIpContinue	lecture seule	Oui	40
cabhSec2FwLocalFilterIpStartTime	lecture-création	Oui	40

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
cabhSec2FwLocalFilterIpEndTime	lecture-création	Oui	40
cabhSec2FwLocalFilterIpDOW	lecture-création	Oui	40
cabhSec2FwLocalFilterIpDescr	lecture-création	Oui	40
cabhSec2FwFactoryDefault			
cabhSec2FwFactoryDefaultTable/ cabhSec2FwFactoryDefaultEntry			
cabhSec2FwFactoryDefaultIndex	non accessible		
cabhSec2FwFactoryDefaultControl		–	N/A
cabhSec2FwFactoryDefaultIfIndex		–	N/A
cabhSec2FwFactoryDefaultDirection		–	N/A
cabhSec2FwFactoryDefaultSaddr		–	N/A
cabhSec2FwFactoryDefaultSmask		–	N/A
cabhSec2FwFactoryDefaultDaddr		–	N/A
cabhSec2FwFactoryDefaultDmask		–	N/A
cabhSec2FwFactoryDefaultProtocol		–	N/A
cabhSec2FwFactoryDefaultSourcePortLow		–	N/A
cabhSec2FwFactoryDefaultSourcePortHigh		–	N/A
cabhSec2FwFactoryDefaultDestPortLow		–	N/A
cabhSec2FwFactoryDefaultDestPortHigh		–	N/A
cabhSec2FwFactoryDefaultIFilterContinue		–	N/A
cabhSecKerbBase			
cabhSecKerbPKINITGracePeriod	lecture-écriture	Non	N/A
cabhSecKerbTGSGracePeriod	lecture-écriture	Non	N/A
cabhSecKerbUnsolicitedKeyMaxTimeout	lecture-écriture	Non	N/A
cabhSecKerbUnsolicitedKeyMaxRetries	lecture-écriture	Non	N/A
cabhCapMib **cabhCapObjects** **cabhCapBase**			
cabhCapTcpTimeWait	lecture-écriture	Non	N/A
cabhCapUdpTimeWait	lecture-écriture	Non	N/A
cabhCapIcmpTimeWait	lecture-écriture	Non	N/A
cabhCapPrimaryMode	lecture-écriture	Non	N/A
cabhCapSetToFactory	lecture-écriture	Non	N/A
cabhCapLastSetToFactory	lecture seule	–	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
CabhCapUpnpPortForwardingEnable	lecture-écriture	Oui	1
CabhCapUpnpTimeWait	lecture-écriture	Non	N/A
cabhCapMap			
cabhCapMappingTable/ cabhCapMappingEntry			
cabhCapMappingIndex	non accessible	–	N/A
cabhCapMappingWanAddrType	lecture-création	Oui[5]	16
cabhCapMappingWanAddr	lecture-création	Oui[5]	16
cabhCapMappingWanPort	lecture-création	Oui[5]	16
cabhCapMappingLanAddrType	lecture-création	Oui[5]	16
cabhCapMappingLanAddr	lecture-création	Oui[5]	16
cabhCapMappingLanPort	lecture-création	Oui[5]	16
cabhCapMappingMethod	lecture seule	–	N/A
cabhCapMappingProtocol	lecture-création	Oui[5]	16
cabhCapMappingRowStatus	lecture-création	Oui	16
cabhCapMappingNumPorts	lecture-création	Oui	16
cabhCapMappingRowDescr	lecture-création	Oui	16
cabhCapMappingCreateTime	lecture seule	Non	N/A
cabhCapMappingLastUpdateTime	lecture seule	Non	N/A
cabhCapMappingDuration	lecture-création	Oui	16
cabhCapMappingRemoteHostAddrType	lecture seule	Non	N/A
CabhCapMappingRemoteHostAddr	lecture seule	Non	N/A
CabhCapMappingEnable	Lecture seule	Non	N/A
cabhCapPassthroughTable/ cabhCapPassthroughEntry			
cabhCapPassthroughIndex	non accessible	–	N/A
cabhCapPassthroughMacAddr	lecture-création	Oui	16
cabhCapPassthroughRowStatus	lecture-création	Oui	16

[5] Les objets CabhCapMappingEntry sont persistants si préconfigurés par le système NMS et non persistants si créés dynamiquement sur la base du trafic de local à régional. Voir le § 8.3.4.4.

cabhCdpMib **cabhCdpObjects** **cabhCdpBase**			
cabhCdpSetToFactory	lecture-écriture	Non	N/A
cabhCdpLanTransCurCount	lecture seule	–	N/A
cabhCdpLanTransThreshold	lecture-écriture	Non	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
cabhCdpLanTransAction	lecture-écriture	Non	N/A
cabhCdpWanDataIpAddrCount	lecture-écriture	Non	N/A
cabhCdpLastSetToFactory	lecture seule		N/A
cabhCdpTimeOffsetSelection	lecture-écriture	Oui	1
cabhCdpSnmpSetTimeOffset	lecture-écriture	Oui	1
cabhCdpDaylightSavingTimeEnable	lecture-écriture	Oui	1
cabhCdpAddr			
cabhCdpLanAddrTable/ cabhCdpLanAddrEntry			
cabhCdpLanAddrIpType	non accessible	-	N/A
cabhCdpLanAddrIp	non accessible	–	N/A
cabhCdpLanAddrClientID	lecture-création	Oui	16
cabhCdpLanAddrLeaseCreateTime	lecture seule	–	N/A
cabhCdpLanAddrLeaseExpireTime	lecture seule	–	N/A
cabhCdpLanAddrMethod	lecture seule	Oui	16
cabhCdpLanAddrHostName	lecture seule	Oui	16
cabhCdpLanAddrRowStatus	lecture-création	Oui	16
cabhCdpWanDataAddrTable/ cabhCdpWanData AddrEntry			
CabhCdpWanDataAddrIndex	non accessible	–	N/A
CabhCdpWanDataAddrClientId	lecture-création	Non	N/A
CabhCdpWanDataAddrIpType	lecture seule	–	N/A
CabhCdpWanDataAddrIp	lecture seule	–	N/A
CabhCdpWanDataAddrRowStatus	lecture-création	Non	N/A
CabhCdpWanDataAddrLeaseCreateTime	lecture seule	–	N/A
CabhCdpWanDataAddrLeaseExpireTime	lecture seule	–	N/A
cabhCdpWanDnsServerTable/ cabhCdpWanDns ServerEntry			
cabhCdpWanDnsServerOrder	non accessible	–	N/A
cabhCdpWanDnsServerIpType	lecture seule	–	N/A
cabhCdpWanDnsServerIp	lecture seule	–	N/A
cabhCdpServer			
cabhCdpLanPoolStartType	lecture-écriture	Oui	1
cabhCdpLanPoolStart	lecture-écriture	Oui	1
cabhCdpLanPoolEndType	lecture-écriture	Oui	1
cabhCdpLanPoolEnd	lecture-écriture	Oui	1
cabhCdpServerNetworkNumberType	lecture-écriture	Oui	1

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
cabhCdpServerNetworkNumber	lecture-écriture	Oui	1
cabhCdpServerSubnetMaskType	lecture-écriture	Oui	1
cabhCdpServerSubnetMask	lecture-écriture	Oui	1
cabhCdpServerTimeOffset	lecture-écriture	Oui	1
cabhCdpServerRouterType	lecture-écriture	Oui	1
cabhCdpServerRouter	lecture-écriture	Oui	1
cabhCdpServerDnsAddressType	lecture-écriture	Oui	1
cabhCdpServerDnsAddress	lecture-écriture	Oui	1
cabhCdpServerUseCableDataNwDnsAddr	lecture-écriture	Non	N/A
cabhCdpServerSyslogAddressType	lecture-écriture	Oui	1
cabhCdpServerSyslogAddress	lecture-écriture	Oui	1
cabhCdpServerDomainName	lecture-écriture	Oui	1
cabhCdpServerTTL	lecture-écriture	Oui	1
cabhCdpServerInterfaceMTU	lecture-écriture	Oui	1
cabhCdpServerVendorSpecific	lecture-écriture	Oui	1
cabhCdpServerLeaseTime	lecture-écriture	Oui	1
cabhCdpServerDhcpAddressType	lecture seule	–	N/A
cabhCdpServerDhcpAddress	lecture seule	–	N/A
cabhCdpServerControl	lecture-écriture	Non	N/A
cabhCdpServerCommitStatus	lecture seule	–	N/A
cabhCtpMib **cabhCtpObjects** **cabhCtpBase**			
cabhCtpSetToFactory	lecture-écriture	Non	N/A
cabhCtpLastSetToFactory	lecture seule	–	N/A
cabpCtpConnSpeed			
cabhCtpConnSrcIpType	lecture-écriture	Non	N/A
cabhCtpConnSrcIp	lecture-écriture	Non	N/A
cabhCtpConnDestIpType	lecture-écriture	Non	N/A
cabhCtpConnDestIp	lecture-écriture	Non	N/A
cabhCtpConnProto	lecture-écriture	Non	N/A
cabhCtpConnNumPkts	lecture-écriture	Non	N/A
cabhCtpConnPktSize	lecture-écriture	Non	N/A
cabhCtpConnTimeOut	lecture-écriture	Non	N/A
cabhCtpConnControl	lecture-écriture	Non	N/A
cabhCtpConnStatus	lecture seule	–	N/A
cabhCtpConnPktsSent	lecture seule	–	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
cabhCtpConnPktsRecv	lecture seule	–	N/A
cabhCtpConnRTT	lecture seule	–	N/A
cabhCtpConnThroughput	lecture seule	–	N/A
cabhCtpPing			
cabhCtpPingSrcIpType	lecture-écriture	Non	N/A
cabhCtpPingSrcIp	lecture-écriture	Non	N/A
cabhCtpPingDestIpType	lecture-écriture	Non	N/A
cabhCtpPingDestIp	lecture-écriture	Non	N/A
cabhCtpPingNumPkts	lecture-écriture	Non	N/A
cabhCtpPingPktSize	lecture-écriture	Non	N/A
cabhCtpPingTimeBetween	lecture-écriture	Non	N/A
cabhCtpPingTimeOut	lecture-écriture	Non	N/A
cabhCtpPingControl	lecture-écriture	Non	N/A
cabhCtpPingStatus	lecture seule	–	N/A
cabhCtpPingNumSent	lecture seule	–	N/A
cabhCtpPingNumRecv	lecture seule	–	N/A
cabhCtpPingAvgRTT	lecture seule	–	N/A
cabhCtpPingMaxRTT	lecture seule	–	N/A
cabhCtpPingMinRTT	lecture seule	–	N/A
cabhCtpPingNumIcmpError	lecture seule	–	N/A
cabhCtpPingIcmpError	lecture seule	–	N/A
cabhQos2Mib **cabhQos2MibObjects** **cabhQos2Base**			
cabhQos2SetToFactory	lecture-écriture	Non	N/A
cabhQos2LastSetToFactory	lecture seule	–	N/A
cabhQos2PsIfAttributes			
cabhQos2PsIfAttribTable/ *cabhQos2PsIfAttribEntry*			
cabhQos2PsIfAttribIfNumPriorities	lecture seule	–	N/A
cabhQosInterfaceAttribIfNumQueues	lecture seule	–	N/A
cabhQos2PolicyHolderObjects			
cabhQos2PolicyHolderEnabled	lecture-écriture	Oui	1
cabhQos2PolicyAdmissionControl	lecture-écriture	Oui	1
cabhQos2NumActivePolicyHolder	lecture seule	–	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
cabhQos2PolicyTable/ cabhQos2PolicyEntry			
cabhQos2PolicyOwner	non accessible	–	N/A
cabhQos2PolicyOwnerRuleId	non accessible	–	N/A
cabhQos2PolicyRuleOrder	lecture-création	Oui	32
cabhQos2PolicyAppDomain	lecture-création	Oui	32
cabhQos2PolicyAppName	lecture-création	Oui	32
cabhQos2PolicyServiceProvDomain	lecture-création	Oui	32
cabhQos2PolicyServiceName	lecture-création	Oui	32
cabhQos2PolicyPortDomain	lecture-création	Oui	32
cabhQos2PolicyPortNumber	lecture-création	Oui	32
cabhQos2PolicyIpProtocol	lecture-création	Oui	32
cabhQos2PolicyIpType	lecture-création	Oui	32
cabhQos2PolicySrcIp	lecture-création	Oui	32
cabhQos2PolicyDestIp	lecture-création	Oui	32
cabhQos2PolicySrcPort	lecture-création	Oui	32
cabhQos2PolicyDestPort	lecture-création	Oui	32
cabhQos2PolicyTraffImpNum	lecture-création	Oui	32
cabhQos2PolicyUserImportance	lecture-création	Oui	32
cabhQos2PolicyRowStatus	lecture-création	Oui	32
cabhQos2DeviceObjects			
cabhQos2TrafficClassTable/ cabhQos2TrafficClassEntry			
cabhQos2TrafficClassMethod	non accessible	–	N/A
cabhQos2TrafficClassIdx	non accessible	–	N/A
cabhQos2TrafficClassProtocol	lecture-création	–	N/A
cabhQos2TrafficClassIpType	lecture-création	–	N/A
cabhQos2TrafficClassSrcIp	lecture-création	–	N/A
cabhQos2TrafficClassDestIp	lecture-création	–	N/A
cabhQos2TrafficClassSrcPort	lecture-création	–	N/A
cabhQos2TrafficClassDestPort	lecture-création	–	N/A
cabhQos2TrafficClassImpNum	lecture-création	–	N/A
cabhQos2TrafficClassRowStatus	lecture-création	–	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
expérimental **snmpUSMDHObjectsMIB [RFC 2786]** **usmDHKeyObjects** **usmDHPublicObjects**			
usmDHParamaters	lecture-écriture	Non	N/A
usmDHUserKeyTable/ *usmDHUserKeyEntry*			
usmDHUserAuthKeyChange	lecture-création	Non	N/A
usmDHUserOwnAuthKeyChange	lecture-création	Non	N/A
usmDHUserPrivKeyChange	lecture-création	Non	N/A
usmDHUserOwnPrivKeyChange	lecture-création	Non	N/A
usmDHKickstartGroup			
usmDHKickstartTable/ *usmDHKickstartEntry*			
usmDHKickstartIndex	non accessible	–	N/A
usmDHKickstartMyPublic	lecture seule	–	N/A
usmDHKickstartMgrPublic	lecture seule	–	N/A
usmDHKickstartSecurityName	lecture seule	–	N/A
snmpV2 **snmpModules** **snmpMIB** **snmpMIBObjects** **snmpSet**			
snmpSetSerialNo	lecture-écriture	Non	N/A
snmpFrameworkMIB [RFC 3411] **snmpEngine**			
snmpEngineID	lecture seule	Oui	1
snmpEngineBoots	lecture seule	Oui	1
snmpEngineTime	lecture seule	–	N/A
snmpEngineMaxMessageSize	lecture seule	–	N/A
snmpMPDMIB [RFC 3412] **snmpMPDObjects** **snmpMPDStats**			

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
snmpUnknownSecurityModels	lecture seule	–	N/A
snmpInvalidMsgs	lecture seule	–	N/A
snmpUnknownPDUHandlers	lecture seule	–	N/A
snmpTargetMIB [RFC 3413] snmpTargetObjects			
snmpTargetSpinLock	lecture-écriture	Non	N/A
snmpTargetAddrTable/ snmpTargetAddrEntry			
snmpTargetAddrName	non accessible	–	N/A
snmpTargetAddrTDomain	lecture-création	Non	N/A
snmpTargetAddrTAddress	lecture-création	Non	N/A
snmpTargetAddrTimeout	lecture-création	Non	N/A
snmpTargetAddrRetryCount	lecture-création	Non	N/A
snmpTargetAddrTagList	lecture-création	Non	N/A
snmpTargetAddrParams	lecture-création	Non	N/A
snmpTargetAddrStorageType	lecture-création	Non	N/A
snmpTargetAddrRowStatus	lecture-création	Non	N/A
snmpTargetParamsTable/ snmpTargetParamsEntry			
snmpTargetParamsName	non accessible	–	N/A
snmpTargetParamsMPModel	lecture-création	Non	N/A
snmpTargetParamsSecurityModel	lecture-création	Non	N/A
snmpTargetParamsSecurityName	lecture-création	Non	N/A
snmpTargetParamsSecurityLevel	lecture-création	Non	N/A
snmpTargetParamsStorageType	lecture-création	Non	N/A
snmpTargetParamsRowStatus	lecture-création	Non	N/A
snmpUnavailableContexts	lecture seule	–	N/A
snmpUnknownContexts	lecture seule	–	N/A
snmpNotificationMIB [RFC 3413] snmpNotifyObjects			
snmpNotifyTable/snmpNotifyEntry			
snmpNotifyName	non accessible	–	N/A
snmpNotifyTag	lecture-création	Non	N/A
snmpNotifyType	lecture-création	Non	N/A
snmpNotifyStorageType	lecture-création	Non	N/A
snmpNotifyRowStatus	lecture-création	Non	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
snmpNotifyFilterProfileTable/ snmpNotifyFilterProfileEntry			
snmpNotifyFilterProfileName	lecture-création	Non	N/A
snmpNotifyFilterProfileStorType	lecture-création	Non	N/A
snmpNotifyFilterProfileRowStatus	lecture-création	Non	N/A
snmpNotifyFilterTable/ snmpNotifyFilterEntry			
snmpNotifyFilterSubtree	non accessible	–	N/A
snmpNotifyFilterMask	lecture-création	Non	N/A
snmpNotifyFilterType	lecture-création	Non	N/A
snmpNotifyFilterStorageType	lecture-création	Non	N/A
snmpNotifyFilterRowStatus	lecture-création	Non	N/A
snmpUsmMIB [RFC 3414] usmStats			
usmStatsUnsupportedSecLevels	lecture seule	–	N/A
usmStatsNotInTimeWindows	lecture seule	–	N/A
usmStatsUnknownUserNames	lecture seule	–	N/A
usmStatsUnknownEngineIDs	lecture seule	–	N/A
usmStatsWrongDigests	lecture seule	–	N/A
usmStatsDecryptionErrors	lecture seule	–	N/A
usmUser			
usmUserSpinLock	lecture-écriture	Non	N/A
usmUserTable/ usmUserEntry			
usmUserEngineID	non accessible	–	N/A
usmUserName	non accessible	–	N/A
usmUserSecurityName	lecture seule	–	N/A
usmUserCloneFrom	lecture-création	Non	N/A
usmUserAuthProtocol	lecture-création	Non	N/A
usmUserAuthKeyChange	lecture-création	Non	N/A
usmUserOwnAuthKeyChange	lecture-création	Non	N/A
usmUserPrivProtocol	lecture-création	Non	N/A
usmUserPrivKeyChange	lecture-création	Non	N/A
usmUserOwnPrivKeyChange	lecture-création	Non	N/A
usmUserPublic	lecture-création	Non	N/A
usmUserStorageType	lecture-création	Non	N/A
usmUserStatus	lecture-création	Non	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
Base MIB fondée sur la modèle de contrôle d'accès selon la vue (ACM) en protocole SNMP [RFC 3415] **snmpVacmMIB** **vacmMIBObjects**			
vacmContextTable/ *vacmContextEntry*			
vacmContextName	lecture seule	–	N/A
vacmSecurityToGroupTable/ *vacmSecurityToGroupEntry*			
vacmSecurityModel	non accessible	–	N/A
vacmSecurityName	non accessible	–	N/A
vacmGroupName	lecture-création	Non	N/A
vacmSecurityToGroupStorageType	lecture-création	Non	N/A
vacmSecurityToGroupStatus	lecture-création	Non	N/A
vacmAccessTable/ *vacmAccessEntry*			
vacmAccessContextPrefix	non accessible	–	N/A
vacmAccessSecurityModel	non accessible	–	N/A
vacmAccessSecurityLevel	non accessible	–	N/A
vacmAccessContextMatch	lecture-création	Non	N/A
vacmAccessReadViewName	lecture-création	Non	N/A
vacmAccessWriteViewName	lecture-création	Non	N/A
vacmAccessNotifyViewName	lecture-création	Non	N/A
vacmAccessStorageType	lecture-création	Non	N/A
vacmAccessStatus	lecture-création	Non	N/A
vacmMIBViews			
vacmViewSpinLock	lecture-écriture	Non	N/A
vacmViewTreeFamilyTable/ *vacmViewTreeFamilyEntry*			
vacmViewTreeFamilyViewName	non accessible	–	N/A
vacmViewTreeFamilySubtree	non accessible	–	N/A
vacmViewTreeFamilyMask	lecture-création	Non	N/A
vacmViewTreeFamilyType	lecture-création	Non	N/A
vacmViewTreeFamilyStorageType	lecture-création	Non	N/A
vacmViewTreeFamilyStatus	lecture-création	Non	N/A

Nom/paramètre de base MIB	Accès maximal	"Objet persistant"	Nombre d'entrées d'objet persistant
snmpCommunityMIB [RFC 3584] snmpCommunityMIBObjects			
snmpCommunityTable/ snmpCommunityEntry			
snmpCommunityIndex	non accessible	–	N/A
snmpCommunityName	lecture-création	Non	N/A
snmpCommunitySecurityName	lecture-création	Non	N/A
snmpCommunityContextEngineID	lecture-création	Non	N/A
snmpCommunityContextName	lecture-création	Non	N/A
snmpCommunityTransportTag	lecture-création	Non	N/A
snmpCommunityStorageType	lecture-création	Non	N/A
snmpCommunityStatus	lecture-création	Non	N/A
snmpTargetAddrExtTable/ snmpTargetAddrExtEntry			
snmpTargetAddrTMask	lecture-création	Non	N/A
snmpTargetAddrMMS	lecture-création	Non	N/A
clabSecCertObject			
clabSrvcPrvdrRootCACert	lecture seule	–	N/A
clabCVCRootCACert	lecture seule	–	N/A
clabCVCCACert	lecture seule	–	N/A
clabMfgCACert	lecture seule	–	N/A

Annexe B

Format et contenu des messages événementiels SYSLOG et Trap du protocole SNMP

Le Tableau B.1 résume le format et le contenu des entrées d'événement de journalisation locale, des messages SYSLOG et des préinterruptions (interruptions système) en protocole SNMP.

Chaque rangée du tableau spécifie un événement que le dispositif PS doit être capable de produire. Ces événements doivent être signalés par le dispositif PS par l'un des trois moyens suivants: journalisation locale des événements telle qu'implémentation par la table locale d'événements dans [RFC 2669], messages SYSLOG et messages TRAP du protocole SNMP. Le format SYSLOG est spécifié dans le § 6.3.3.2.4.4 et le format de préinterruption SNMP est défini dans la présente annexe, après le Tableau B.1.

Les première et deuxième colonnes du Tableau B.1 indiquent à quel stade l'événement se produit. La troisième colonne indique la priorité attribuée à l'événement. Ces priorités sont celles qui sont signalées dans les valeurs de l'objet docsDevEvLevel dans [RFC 2669] et dans le champ 'LEVEL' (niveau) d'un message SYSLOG.

La quatrième colonne spécifie le texte de l'événement, qui est signalé dans l'objet docsDevEvText du document [RFC 2669] et le champ de texte d'un message SYSLOG. La cinquième colonne offre des informations supplémentaires sur le texte de l'événement de la quatrième colonne. Par exemple, certains champs de texte d'événement sont constants et certains champs de texte d'événement comprennent des informations variables. Certaines des variables ne sont requises que dans le journal SYSLOG, comme décrit dans la cinquième colonne. La sixième colonne spécifie la mise à jour du code d'erreur.

La septième colonne indique un numéro d'identification unique pour l'événement, qui est attribué à l'objet docsDevEvId et au champ <eventId> d'un message SYSLOG. La huitième colonne spécifie le message TRAP du SNMP qui notifie cet événement à un récepteur d'événements SNMP.

Les règles permettant de produire de façon univoque un identificateur d'événement à partir du code d'erreur sont décrites dans le § 6.3.3.2.4.4. Les identificateurs d'événement figurant dans le tableau sont en format décimal.

Afin de mieux illustrer le tableau, ce qui suit est un exemple utilisant la première rangée dans la section des événements de mise à jour logicielle.

Les deux premières colonnes sont "Mise à jour logicielle" et "Initialisation de mise à jour logicielle". La priorité de l'événement est "Remarque". Le texte de l'événement est "INITIALISATION du téléchargement de logiciel – par NMS". La cinquième colonne indique "Pour SYSLOG seulement, ajouter: MAC addr: <P1> P1 = Adresse de commande MAC". Il s'agit d'une note sur le journal SYSLOG. C'est-à-dire que le corps du texte du journal SYSLOG sera quelque chose comme "Initialisation du téléchargement de logiciel – par NMS – MAC addr: x1 x2 x3 x4 x5 x6".

La dernière colonne "Nom du préinterruption" correspond à l'objet cabhPsDevSwUpgradeInitTrap, dont le format est donné à la fin de la présente annexe.

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
Erreurs DHCP avant l'achèvement de la préconfiguration							
Initialiser	CDC	Critique	DHCP échoué – flux DISCOVER envoyé, aucune offre reçue		D01.0	68000100	
Initialiser	CDC	Critique	DHCP échoué – demande envoyée, aucune réponse		D02.0	68000200	
Initialiser	CDC	Critique	DHCP échoué – info demandée non prise en charge.		D03.0	68000300	
Initialiser	CDC	Erreur	Erreur DHCP – la réponse ne contient pas TOUS les champs valides OU le dispositif PS n'est pas en mesure de déterminer le mode de préconfiguration		D03.1	68000301	
Initialiser	CDC	Avertissement	Erreur DHCP – Impossible d'obtenir toutes les adresses IP de réseau WAN-Data que le dispositif PS a été configuré de façon à obtenir		P02.0	68000302	cabhPsDevCdpWan DataIpTrap
Erreurs de temps ToD avant l'achèvement de la préconfiguration							
Initialiser	ToD	Avertissement	Demande d'heure envoyée – aucune réponse reçue – Adresse du serveur temporel + <P1>	P1 = adresse IP du serveur d'heure actuelle	D04.1	68000401	cabhPsDevInitTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
Initialiser	ToD	Avertissement	Réponse ToD reçue – format de données non valide Adresse du serveur temporel + <P1>	P1 = adresse IP du serveur d'heure actuelle	D04.2	68000402	cabhPsDevInitTrap
Erreurs TFTP avant l'achèvement de la préconfiguration							
Initialiser	TFTP	Erreur	TFTP échoué – demande envoyée – Aucune réponse		D05.0	68000500	cabhPsDevInitTrap (La préinterruption n'est applicable qu'au mode d'approv. SNMP.)
Initialiser	TFTP	Erreur	TFTP échoué – fichier de configuration NON TROUVE	Pour SYSLOG seulement, ajouter: Nom de fichier = <P1> P1 = nom de fichier demandé	D06.0	68000600	cabhPsDevInitTrap (La préinterruption n'est applicable qu'au mode d'approv. SNMP.)
Initialiser	TFTP	Erreur	TFTP échoué – Paquets dans le désordre		D07.0	68000700	cabhPsDevInitTrap (La préinterruption n'est applicable qu'au mode d'approv. SNMP.)
Initialiser	TFTP	Erreur	Fichier TFTP terminé – mais échec de la vérification du hachage SHA-1	Pour SYSLOG seulement, ajouter: Nom de fichier = <P1> P1 = nom de fichier TFTP	D08.0	68000800	cabhPsDevInitTrap (La préinterruption n'est applicable qu'au mode d'approv. SNMP.)

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
Initialiser	TFTP	Erreur	TFTP échoué – nombre maximal de réessais dépassé	Pour SYSLOG seulement, ajouter: nombre maximal autorisé de réessais = <P1> P1 = nombre maximal autorisé de tentatives de réessai	D09.0	68000900	cabhPsDevInitTrap (La préinterruption n'est applicable qu'au mode d'approv. SNMP.)
TFTP réussi							
Initialiser	TFTP	Remarque	TFTP réussi		D10.0	68001000	
TLS							
Initialiser	TCP/IP	Critique	PS incapable de se connecter à serveur distant HTTP/TLS, lors d'une tentative de téléchargement du fichier de configuration <P1>	P1 = 'PS' ou 'Pare-feu'	D20.0	68002000	
Initialiser	TLS	Critique	Connexion TLS expirée et nombre maximal de réessais dépassé, lors d'une tentative de téléchargement du fichier de configuration <P1>	P1 = 'PS' ou 'Pare-feu'	D21.0	68002100	
Initialiser	TLS	Critique	Erreur fatale TLS <code P1>, lors d'une tentative de téléchargement du fichier de configuration <P2>	P1 = code d'erreur à partir du document [RFC 2246] P2 = 'PS' ou 'Pare-feu'	D22.0	68002200	

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
HTTP							
Initialiser	HTTP	Critique	Téléchargement du fichier de configuration échoué, mais réessai prévu. Erreur HTTP. <P1>, lors d'une tentative de téléchargement du fichier de configuration <P2>	P1 = codes d'état à partir du document [RFC 2616] P2 = 'PS' ou 'Pare-feu'	D30.0	68003000	
Initialiser	HTTP	Critique	Téléchargement du fichier de configuration échoué du fait que la connexion a expiré et que le nombre maximal de réessais a été dépassé. Opération abandonnée, lors d'une tentative de téléchargement du fichier de configuration <P1>	P1 = 'PS' ou 'Pare-feu'	D31.0	68003100	
Initialiser	HTTP	Critique	Téléchargement sécurisé du fichier de configuration correctement achevé, lors d'une tentative de téléchargement du fichier de configuration <P1>	P1 = 'PS' ou 'Pare-feu'	D32.0	68003200	
Analyse sémantique de TLV							
Initialiser	Analyse sémantique de TLV	Avertissement	TLV-27 ou TLV-28 – OID non reconnu lors d'une tentative de téléchargement du fichier de configuration <P1>	P1 = 'PS' ou 'Pare-feu'	I401.0	73040100	cabhPsDevInit TLVUnknownTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
Initialiser	Analyse sémantique de TLV	Avertissement	Nuplet TLV inconnu	Pour SYSLOG seulement, ajouter le fichier de configuration <P2>. Le nuplet TLV est <P1>, P1 = le nuplet TLV complet en hexadécimal. P2 = 'PS' ou 'Pare-feu'	I401.1	73040101	cabhPsDevInitTLV UnknownTrap
Initialiser	Analyse sémantique de TLV	Erreur	Format/contenu de TLV non valide	Pour SYSLOG seulement, ajouter le fichier de configuration <P2>. Le nuplet TLV est <P1>, P1+ = le nuplet TLV complet en hexadécimal. P2 = 'PS' ou 'Pare-feu'	I401.2	73040102	
Préconfiguration							
Initialiser	Préconfiguration terminée	Remarque	Préconfiguration terminée	Pour SYSLOG seulement, ajouter MAC Addr: <P1>. P1 = adresse MAC du dispositif PS	I11.0	73001100	cabhPsDevInitTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
Initialisation de mise à jour logicielle (Note)							
Mise à jour logicielle	Initialisation de mise à jour logicielle	Remarque	Initialiser le téléchargement du logiciel – Par NMS	Pour SYSLOG seulement, ajouter: fichier de logiciel: <P1> – Serveur de logiciels: < P2>. P1 = nom de fichier du logiciel et P2 = adresse IP du serveur Tftp.	E101.0	69010100	cabhPsDevSwUpgrade InitTrap
Mise à jour logicielle	Initialisation de mise à jour logicielle	Remarque	Initialiser le téléchargement du logiciel – Par fichier de configuration <P1>	P1 = CM nom de fichier de configuration. Pour SYSLOG seulement, ajouter: fichier de logiciel: <P2> – Serveur de logiciels: < P3>. P2 = nom de fichier du logiciel et P3 = adresse IP du serveur Tftp.	E102.0	69010200	cabhPsDevSwUpgrade InitTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
Echec général de mise à jour logicielle (Note)							
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Mise à jour logicielle échouée pendant téléchargement – Maximum d'essais dépassé (3)	Pour SYSLOG seulement, ajouter: fichier de logiciel: <P1> – Serveur de logiciels: < P2>. P1 = nom de fichier du logiciel et P2 = adresse IP du serveur Tftp.	E103.0	69010300	cabhPsDevSwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Mise à jour logicielle échouée avant téléchargement – Serveur absent	Pour SYSLOG seulement, ajouter: fichier de logiciel: <P1> – Serveur de logiciels: < P2>. P1 = nom de fichier du logiciel et P2 = adresse IP du serveur Tftp.	E104.0	69010400	cabhPsDevSwUpgrade FailTrap
Mise à jour logicielle	Echec genéral de mise à jour logicielle	Erreur	Mise à jour logicielle échouée avant téléchargement – Fichier absent	Pour SYSLOG seulement, ajouter: fichier de logiciel: <P1> – Serveur de logiciels: < P2>. P1 = nom de fichier du logiciel et P2 = adresse IP du serveur Tftp.	E105.0	69010500	cabhPsDevSwUpgrade FailTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Mise à jour logicielle échouée avant téléchargement – TFTP Maximum d'essais dépassé	Pour SYSLOG seulement, ajouter: fichier de logiciel: <P1> – Serveur de logiciels: < P2>. P1 = nom de fichier du logiciel et P2 = adresse IP du serveur Tftp.	E106.0	69010600	cabhPsDevSwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Mise à jour logicielle échouée après téléchargement – Fichier de logiciel incompatible	Pour SYSLOG seulement, ajouter: Fichier de logiciel: <P1> – Serveur de logiciels: < P2>. P1 = nom de fichier du logiciel et P2 = adresse IP du serveur Tftp.	E107.0	69010700	cabhPsDevSwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Mise à jour logicielle échouée après téléchargement – Corruption du fichier de logiciel	Pour SYSLOG seulement, ajouter: fichier de logiciel: <P1> – Serveur de logiciels: < P2>. P1 = nom de fichier du logiciel et P2 = adresse IP du serveur Tftp.	E108.0	69010800	cabhPsDevSwUpgrade FailTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Interruption pendant téléchargement du logiciel – Panne d'alimentation	Pour SYSLOG seulement, ajouter: fichier de logiciel: <P1> – Serveur de logiciels: < P2>. P1 = nom de fichier du logiciel et P2 = adresse IP du serveur Tftp.	E109.0	69010900	cabhPsDevSwUpgrade FailTrap
Mise à jour logicielle réussie (Note)							
Mise à jour logicielle	Mise à jour logicielle réussie	Remarque	Téléchargement du logiciel réussi – Par NMS	Pour SYSLOG seulement, ajouter: fichier de logiciel: <P1> – Serveur de logiciels: < P2>. P1 = nom de fichier du logiciel et P2 = adresse IP du serveur Tftp.	E111.0	69011100	cabhPsDevSwUpgrade SuccessTrap
Mise à jour logicielle	Mise à jour logicielle réussie	Remarque	Téléchargement du logiciel réussi – Par fichier de configuration	Pour SYSLOG seulement, ajouter: fichier de logiciel: <P1> – Serveur de logiciels: < P2>. P1 = nom de fichier du logiciel et P2 = adresse IP du serveur Tftp.	E112.0	69011200	cabhPsDevSwUpgrade SuccessTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
Echec DHCP après achèvement de la préconfiguration							
DHCP	CDC	Erreur	DHCP RENEW émis – Aucune réponse		D101.0	68010100	cabhPsDevDHCPFail Trap
DHCP	CDC	Erreur	DHCP REBIND émis – Aucune réponse		D102.0	68010200	cabhPsDevDHCPFail Trap
DHCP	CDC	Erreur	DHCP RENEW émis – Option DHCP non valide		D103.0	68010300	cabhPsDevDHCPFail Trap
DHCP	CDC	Erreur	DHCP REBIND émis – Option DHCP non valide		D104.0	68010400	cabhPsDevDHCPFail Trap
Echec ToD après achèvement de la préconfiguration							
ToD	ToD	Avertissement	Demande d'heure envoyée – Aucune réponse reçue		D04.3	68000403	cabhPsDevTODFail Trap
ToD	ToD	Avertissement	Réponse ToD reçue – Format de données non valide		D04.4	68000404	cabhPsDevTODFail Trap
Vérification de fichier de code							
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Commandes de fichier de code inappropriées	Pour SYSLOG seulement, ajouter: fichier de code: <P1> – Serveur du fichier de code: <P2>. P1 = nom du fichier de code, P2 = adresse IP du serveur du fichier de code.	E201.0	69020100	cabhPsDevSwUpgrade FailTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Echec de validation du certificat CVC du constructeur du fichier de code	Pour SYSLOG seulement, ajouter: fichier de code: <P1> – Serveur du fichier de code: <P2>. P1 = nom du fichier de code, P2 = adresse IP du serveur du fichier de code.	E202.0	69020200	cabhPsDevSwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Echec de validation de la signature CVS du constructeur du fichier de code	Pour SYSLOG seulement, ajouter: fichier de code: <P1> – Serveur du fichier de code: <P2>. P1 = Nom du fichier de code, P2 = adresse IP du serveur du fichier de code.	E203.0	69020300	cabhPsDevSwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Echec de validation du certificat CVC du cosignataire du fichier de code	Pour SYSLOG seulement, ajouter: fichier de code: <P1> – Serveur du fichier de code: <P2>. P1 = nom du fichier de code, P2 = adresse IP du serveur du fichier de code.	E204.0	69020400	cabhPsDevSwUpgrade FailTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Echec de validation de la signature CVS du cosignataire du fichier de code	Pour SYSLOG seulement, ajouter: fichier de code: <P1> – Serveur du fichier de code: <P2>. P1 = nom du fichier de code, P2 = adresse IP du serveur du fichier de code.	E205.0	69020500	cabhPsDevSwUpgrade FailTrap
Vérification de CVC							
Mise à jour logicielle	Vérification de CVC	Erreur	Format de certificat CVC de fichier de configuration du dispositif PS inapproprié – Serveur TFTP: <P1> – Fichier de configuration: <P2>	P1 = adresse IP du serveur TFTP P2 = nom de fichier de configuration	E206.0	69020600	cabhPsDevSwUpgrade CVCFailTrap
Mise à jour logicielle	Vérification de CVC	Erreur	Echec de validation de certificat CVC dans fichier de configuration – Serveur TFTP: <P1> – fichier de configuration: <P2>	P1 = adresse IP du serveur TFTP P2 = nom de fichier de configuration	E207.0	69020700	cabhPsDevSwUpgrade CVCFailTrap
Mise à jour logicielle	Vérification de CVC	Erreur	Format inapproprié du certificat CVC par protocole Snmp – Gestionnaire Snmp: <P1>	P1 = adresse IP de gestionnaire SNMP	E208.0	69020800	cabhPsDevSwUpgrade CVCFailTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
Mise à jour logicielle	Vérification de CVC	Erreur	Echec de validation de certificat CVC par protocole SNMP – Gestionnaire Snmp: <P1>	P1 = IP Adresse du gestionnaire SNMP	E209.0	69020900	cabhPsDevSwUpgrade CVCFailTrap
Evénements de portail CDP							
CDP	CDS	Remarque	Tentative d'attribuer plus d'adresses IP de réseau LAN-Trans que permis		P01.0	80000100	cabhPsDevCDP Threshold Trap
CDP	CDS	Remarque	Incapacité à approvisionner le client DHCP de LAN – réserve d'adresses IP épuisée		P03.0	80000300	cabhPsDevCdpLanIp PoolTrap
Evénements de portail CSP							
CSP	Pare-feu	Remarque	Changement d'état de cabhSec2FwEventEnable pour le type 1. La nouvelle valeur est <P1>	P1 = valeur de l'objet cabhSec2FwEventType1Enable pour le type 1.	P101.1	80010101	cabhPsDevCSPTrap
CSP	Pare-feu	Remarque	Changement d'état de cabhSec2FwEventEnable pour le type 2. La nouvelle valeur est <P1>	P1 = valeur de l'objet cabhSec2FwEventType2Enable pour le type 2.	P101.2	80010102	cabhPsDevCSPTrap
CSP	Pare-feu	Remarque	Changement d'état de cabhSec2FwEventEnable pour le type 3. La nouvelle valeur est <P1>	P1 = valeur de l'objet cabhSec2FwEventType3Enable pour le type 3.	P101.3	80010103	cabhPsDevCSPTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
CSP	Pare-feu	Remarque	Changement d'état de cabhSec2FwEventEnable pour le type 4. La nouvelle valeur est <P1>	P1 = valeur de l'objet cabhSec2FwEventType4Enable pour le type 4.	P101.4	80010104	cabhPsDevCSPTrap
CSP	Pare-feu	Remarque	Changement d'état de cabhSec2FwEventEnable pour le type 5. La nouvelle valeur est <P1>	P1 = valeur de l'objet cabhSec2FwEventType5Enable pour le type 5.	P101.5	80010105	cabhPsDevCSPTrap
CSP	Pare-feu	Remarque	Changement d'état de cabhSec2FwEventEnable pour le type 6. La nouvelle valeur est <P1>	P1 = valeur de l'objet cabhSec2FwEventType6Enable pour le type 6.	P101.6	80010106	cabhPsDevCSPTrap
CSP	Pare-feu	Avertissement	Pare-feu de type 1 – Evénement d'atteinte de seuil		P102.1	80010201	cabhPsDevCSPTrap
CSP	Pare-feu	Avertissement	Pare-feu de type 2 – Evénement d'atteinte de seuil		P102.2	80010202	cabhPsDevCSPTrap
CSP	Pare-feu	Avertissement	Pare-feu de type 3 – Evénement d'atteinte de seuil		P102.3	80010203	cabhPsDevCSPTrap
CSP	Pare-feu	Avertissement	Pare-feu de type 4 – Evénement d'atteinte de seuil. Ensemble de <P1> échoué, <P2>	P1 = tentative de modification de l'objet de base MIB (p. ex. "cabhSec2FwPolicyFileURL") P2 = description textuelle de l'échec	P102.4	80010204	cabhPsDevCSPTrap
CSP	Pare-feu	Avertissement	Pare-feu de type 5 – Evénement d'atteinte de seuil		P102.5	80010205	cabhPsDevCSPTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
CSP	Pare-feu	Avertissement	Pare-feu de type 6 – Evénement d'atteinte de seuil		P102.6	80010206	cabhPsDevCSPTrap
CSP	TFTP du pare-feu	Critique	Téléchargement TFTP de Fichier de politique de pare-feu échoué; demande envoyée, aucune réponse. URL du fichier de configuration : <P1>	P1 = URL du fichier de politique de pare-feu demandée	P130.0	80013000	cabhPsDevCSPTrap
CSP	TFTP du pare-feu	Critique	TFTP échoué – Fichier de politique de pare-feu non trouvé; URL du fichier de configuration : <P1>	P1 = URL du fichier de politique de pare-feu demandée	P131.0	80013100	cabhPsDevCSPTrap
CSP	TFTP du pare-feu	Critique	TFTP échoué – Fichier de politique de pare-feu non valide; URL du fichier de configuration : <P1>	P1 = URL du fichier de politique de pare-feu demandée	P132.0	80013200	cabhPsDevCSPTrap
CSP	TFTP du pare-feu	Critique	Téléchargement du fichier de politique de pare-feu achevé mais échec du contrôle du hachage SHA-1 vérifié. URL du fichier de configuration : <P1> Hachage: <P2>	P1 = URL du fichier de politique de pare-feu demandée, P2 = valeur du fichier de politique de pare-feu	P133.0	80013300	cabhPsDevCSPTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
CSP	TFTP du pare-feu	Critique	Téléchargement du fichier de politique de pare-feu a dépassé le nombre maximal admissible de réessais par TFTP. URL du fichier de configuration : <P1>	P1 = URL du fichier de politique de pare-feu demandée	P134.0	80013400	cabhPsDevCSPTrap
CSP	TFTP du pare-feu	Remarque	Téléchargement par TFTP du fichier de politique du pare-feu réussi URL du fichier de configuration : <P1>	P1 = URL du fichier de politique de pare-feu demandée Pour SYSLOG seulement, ajouter: nombre maximal autorisé de réessais = <P2> P2 = nombre maximal autorisé de tentatives de réessai.	P135.0	80013500	cabhPsDevCSPTrap
Evénements de portail CAP							
CAP	C-NAT	Avertissement	CAP incapable d'effectuer le mappage C-NAT. Aucune adresse IP de réseau WAN-data disponible.		P201.0	80020100	cabhPsDevCAPTrap
CAP	C-NAPT	Avertissement	CAP incapable d'effectuer le mappage C-NAPT. Aucune Adresse IP de réseau régional disponible.		P250.0	80025000	cabhPsDevCAPTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
Evénements de portail CTP							
CTP	Utilitaire de vitesse de connexion	Remarque	Essai par utilitaire de vitesse de connexion achevé avec succès. IP d'origine: <P1>. IP de destination: <P2>. Protocole: <P3>. Valeur de temporisation: <P4> ms.	P1 = adresse IP d'origine P2 = adresse IP de destination P3 = protocole P4 = débit utile	P301.0	80030100	cabhPsDevCtpTrap
CTP	Utilitaire de vitesse de connexion	Remarque	Temporisation d'essai par utilitaire de vitesse de connexion expirée. IP d'origine: <P1>. IP de destination: <P2>. Protocole: <P3>. Valeur de temporisation: <P4> ms.	P1 = adresse IP d'origine P2 = adresse IP de destination P3 = protocole (valeur de cabhCtpConnProto) P4 = valeur de la temporisation mesurant la durée d'exécution de l'utilitaire de vitesse de connexion (millisecondes) (référence: paragraphe relatif aux exigences applicables à l'utilitaire de vitesse de connexion)	P302.0	80030200	cabhPsDevCtpTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
CTP	Utilitaire de vitesse de connexion	Remarque	Essai par utilitaire de vitesse de connexion abandonné. IP d'origine: <P1>. IP de destination: <P2>. Protocole: <P3>. Valeur de temporisation: <P4> ms.	P1 = adresse IP d'origine P2 = adresse IP de destination P3 = protocole (valeur de cabhCtpConnProto) P4 = valeur de la temporisation mesurant la durée d'exécution de l'utilitaire de vitesse de connexion (millisecondes) (référence: paragraphe relatif aux exigences applicables à l'utilitaire de vitesse de connexion)	P303.0	80030300	cabhPsDevCtpTrap
CTP	Utilitaire de sondage par écho	Remarque	Essai par utilitaire de sondage par écho achevé avec succès. IP d'origine: <P1>. IP de destination: <P2>. Protocole: <P3>. Temps moyen d'aller-retour: <P3> ms.	P1 = adresse IP d'origine P2 = adresse IP de destination P3 = temps moyen d'aller-retour (RTT, *round trip time*)	P320.0	80032000	cabhPsDevCtpTrap

Tableau B.1/J.192 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte de l'événement	Notes et détails sur les messages	Mise à jour du code d'erreur	Idenficateur d'événement	Nom du préinterruption
CTP	Utilitaire de sondage par écho	Remarque	Essai par utilitaire de sondage par écho expiré. IP d'origine: <P1>. IP de destination: <P2>. Nombre de requêtes: <P3>. Nombre de réponses: <P4>.	P1 = adresse IP d'origine P2 = adresse IP de destination P3 = nombre de requêtes envoyées P4 = nombre de réponses reçues	P321.0	80032100	cabhPsDevCtpTrap
CTP	Utilitaire de sondage par écho	Remarque	Essai par utilitaire de sondage par écho abandonné. IP d'origine: <P1>. IP de destination: <P2>. Nombre de requêtes: <P3>. Nombre de réponses: <P4>.	P1 = adresse IP d'origine P2 = adresse IP de destination P3 = nombre de requêtes envoyées P4 = nombre de réponses reçues	P322.0	80032200	cabhPsDevCtpTrap
Evénements de qualité de service							
Découverte UPnP	Recherche-M	Avertissement	Option active de détenteurs multiples de politique UPnP		Q100.0	81010000	cabhPsDevUpnpMultiplePHTrap
NOTE – Les événements de mise à jour logicielle (téléchargement sécurisé de logiciel) ne s'appliquent qu'aux services de portail autonome. La mise à jour logicielle est régie par le câblo-modem DOCSIS dans un dispositif PS intégré, de sorte que la signalisation des événements de mise à jour logicielle est gérée par le câblo-modem dans un dispositif PS intégré. Voir de plus amples informations au § 11.8, "Téléchargement de logiciel vers des éléments PS intégrés ou autonomes".							

B.1 Description des préinterruptions

Toutes les préinterruptions sont définies dans la spécification de base MIB PS DEV [voir § E.4].

Annexe C

Dangers et mesures préventives

Lors du développement d'une technique de sécurité, il est important de comprendre quelles sont les principales menaces pour une application ou un environnement donné. Ces informations peuvent alors servir à choisir les utilitaires et techniques de sécurité les plus efficaces pour la protection et la prévention contre les attaques qualifiées.

On a identifié les principaux dangers suivants pour les abonnés et les opérateurs de réseau domestique:

C.1 Vol de service: le vol de service se présente sous deux formes: un accès non autorisé aux services par câble et la duplication illicite de contenu de service.

Un accès non autorisé implique un abonné ou une tierce partie (comme un voisin) ayant accès à des services par câble pour lesquels ils n'ont pas payé. Les dispositifs pourraient être "clonés" ou modifiés de façon à apparaître comme des dispositifs qualifiés dans le réseau domestique de l'abonné. Cela pourrait également dégrader la qualité de livraison des services car ces dispositifs consomment des ressources de transport supplémentaires dans les réseaux HFC et domestiques.

La duplication illicite implique habituellement un abonné ou une tierce partie (comme un voisin) effectuant des copies illégales du contenu de service. Dans certains cas, ces copies sont distribuées à d'autres consommateurs sans l'agrément de l'opérateur ou du fournisseur de contenu;

C.2 Attaques par refus de service (DoS*, denial of service*): les attaques par refus de service peuvent survenir quand une entité tierce (attaquant, client mécontent, etc.) interrompt la communication et la livraison de services normales entre les opérateurs et leurs abonnés. Des transmissions de données fautives, venant de ce qui semble être un dispositif ou une source valide, peuvent être injectées dans le réseau domestique et dégrader sévèrement les fonctions normales. Ces transmissions de données fautives peuvent s'étendre au réseau de câble HFC de l'opérateur et y causer des problèmes de performances.

C.3 Confidentialité du service: la menace visant la confidentialité du service implique une tierce partie (voisins, attaquant, etc.) surveillant/recevant des informations sur un abonné et sur les services qu'il utilise. Cela peut provoquer le vol de mots de passe ou d'informations sur la configuration des dispositifs, ce qui permet aux attaquants d'obtenir ultérieurement accès aux ressources du réseau et à des fichiers/données confidentiels de l'abonné.

Un certain nombre de méthodes différentes peuvent être utilisées pour prévenir les dangers mentionnés ci-dessus concernant le réseau domestique. Malheureusement, une seule méthode ne peut tous les prévenir, mais une combinaison de plusieurs méthodes peut être la meilleure ligne de défense. On peut utiliser les mesures préventives suivantes:

C.4 Authentification: l'authentification implique la vérification du fait que les entités expéditrice et réceptrice sont bien ce qu'elles prétendent être. Cela inclut la source du service, le dispositif récepteur et l'abonné.

L'authentification aide à prévenir le vol de service en validant les dispositifs et les utilisateurs d'extrémité, mais n'empêche pas la copie illégale des contenus ni ne prévient l'accès non autorisé de tierces parties qui surveilleraient la liaison. Elle est efficace dans la prévention des attaques par

refus de service parce que le trafic peut être rejeté s'il ne vient pas d'une source valide. Par elle-même, l'authentification ne fournit aucun support de confidentialité de service et il faut utiliser le chiffrement;

C.5 Protection contre la copie: les méthodes de protection contre la copie limitent la capacité d'un dispositif récepteur à faire des copies non autorisées du contenu du service;

La protection contre la copie aide à prévenir le vol de service en limitant le nombre de copies qui peuvent être faites, mais ne protège pas contre l'accès non autorisé aux services. Elle ne protège pas non plus contre le refus de service et n'assure pas la protection de la confidentialité du service. En général, cette mesure préventive est implémentée à des couches d'application plus élevées;

C.6 Chiffrement des données: le chiffrement des données empêche la découverte et l'accès non autorisés aux données.

Le chiffrement des données est efficace pour la confidentialité des données et la protection contre le vol de service. Le chiffrement empêche de lire les données en l'absence de la clé de déchiffrement correcte. Cependant, il ne valide pas les entités d'émission ou de réception et ne donne pas de protection contre la copie après déchiffrement des données. Il ne protège pas non plus contre les attaques par refus de service;

C.7 Pare-feu: les applications de pare-feu empêchent le trafic du réseau de passer d'un domaine à l'autre à moins qu'il ne satisfasse à certains critères établis par l'abonné ou l'opérateur. Dans les applications domestiques, les pare-feu sont typiquement situés dans les dispositifs de passerelle résidentielle qui connectent le réseau de câble HFC au réseau domestique.

Une application de pare-feu aide à prévenir les attaques par refus de service et les attaques contre la confidentialité à partir du côté réseau régional (WAN) du pare-feu, mais elle n'empêche pas ce type d'attaques venant du côté résidentiel du pare-feu. Elle ne protège pas non plus contre le vol de service;

C.8 Sécurité des messages de gestion: cette méthode de prévention implique l'authentification et le chiffrement des seuls messages de gestion du réseau. Les messages de gestion du réseau sont utilisés pour la configuration des dispositifs, pour la commande/surveillance du réseau, pour la préconfiguration en service et pour les réservations de qualité de service (QS).

La sécurité des messages de gestion est un bon mécanisme de prévention des attaques par refus de service grâce à l'authentification et au chiffrement des messages de gestion. Les informations de configuration du réseau et les informations personnelles de l'abonné sont aussi protégées contre les attaques contre la confidentialité, mais le contenu du service ne l'est pas. Aussi la sécurité des messages de gestion n'empêche pas le vol du contenu du service par des entités non autorisées.

Annexe D

Applications par conversion CAT et pare-feu

En fonctionnement normal de la fonctionnalité de conversion d'adresse et de pare-feu, un certain nombre de protocoles et d'applications peut être empêché de fonctionner comme prévu. Le pare-feu peut filtrer délibérément certaines applications et certains protocoles aux fins de la sécurité. La politique de pare-feu peut être explicitement établie par le câblo-opérateur afin de permettre l'ouverture d'autant de ports que le client en a besoin sans ouvrir de ports qui ne sont pas requis pour la communication entre les réseaux locaux et régionaux. La limitation d'ouverture de ports et de sessions entre les réseaux locaux et régionaux peut assurer une protection du réseau local domestique à l'encontre d'attaques. Si les ports ne sont pas autorisés à être ouverts par la politique de pare-feu, un attaquant ne peut pas les utiliser afin d'attaquer le réseau local. L'objet de la présente annexe est d'offrir un niveau minimal de prise en charge des applications d'usage courant dans des scénarios spécifiques et d'aider le câblo-opérateur par une configuration commune des ports.

Le document [RFC 3235], Directives de conception d'application conviviale – Convertisseur d'adresses de réseau (NAT), décrit un certain nombre de directives afin de créer des applications de telle façon qu'elles ne soient pas compromises lorsqu'elles fonctionnent en présence de la fonctionnalité de conversion d'adresse réseau. Il est fortement recommandé que les développeurs d'applications à exploiter dans un environnement IPCable2Home observent ces directives.

Il est notoire que l'existence de la fonctionnalité de conversion NAT et de pare-feu interrompt un certain nombre de protocoles et d'applications quand les nœuds d'extrémité ou les serveurs locaux ne sont pas dans le même secteur d'adresses et doivent passer par un convertisseur d'adresses IP de couche Réseau (NAT/CAT) et/ou par un pare-feu de transit afin de relier ces secteurs. Dans de nombreux cas, la conversion CAT et le pare-feu ne peuvent pas offrir à l'application et au protocole la transparence recherchée sans l'assistance d'une passerelle de couche Application (ALG). La présente Recommandation implique qu'une passerelle ALG est implémentée dans la passerelle résidentielle, ce qui permet aux applications énumérées dans la présente annexe d'interfonctionner avec la conversion CAT.

Les applications traversant le pare-feu sont décrites en termes de protocoles, de numéros de port spécifiques, de scénarios relationnels LAN-WAN et de secteurs d'adressage. Les protocoles sont subdivisés en deux tableaux: le premier énumère les protocoles qui peuvent être gérés exclusivement par une politique et qui désignent les *Applications nécessitant exclusivement une politique de pare-feu*. Le deuxième tableau énumère les protocoles qui ne peuvent être gérés qu'avec la combinaison politique + passerelles ALG et qui désignent les *Applications nécessitant une politique de pare-feu et une passerelle ALG*.

Conformément à la politique spécifiée dans le § 11, les tableaux contiennent des commentaires à valeur informative pour que le lecteur soit capable de mapper les applications requises avec celles qui ont des exigences de politique particulières dans les environnements IPCable2Home et IPCablecom. L'environnement IPCable2Home exige que les réglages par défaut fixées à l'usine des ports soient ouverts par le pare-feu pour les opérations normales de la passerelle résidentielle. Les éléments marqués "IPCablecom" dans la colonne des commentaires seront inclus en plus des valeurs par défaut fixées à l'usine activant le passage de l'environnement IPCablecom par le pare-feu. Les réglages de pare-feu permettant d'activer IPCablecom sont énumérés dans la colonne des commentaires de chaque tableau et sont spécifiés dans le § 11 concernant le fichier de configuration.

En plus des applications spécifiées, le dispositif PS DEVRAIT prendre en charge les applications de jeu en ligne par conversion CAT et de pare-feu. Le jeu en ligne est considéré comme une application d'utilisation typique. Cependant, la présente Recommandation ne spécifie pas les jeux

car il s'agit d'une industrie dynamique et les ports des jeux en ligne dépendent de la popularité actuelle de jeux particuliers.

D.1 Scénarios relationnels

Des scénarios spécifiques peuvent définir le nombre de serveurs locaux communiquant les uns avec les autres par l'intermédiaire du dispositif PS, de même que les exigences relatives à chaque protocole et application. Chaque application/protocole et chaque scénario spécifique exige que la prise en charge de la conversion CAT et du pare-feu IPCable2Home fonctionne correctement. Les scénarios comprennent une définition "xxx à xxx" qui indique le nombre de serveurs locaux de réseau local qui communiquent avec des serveurs locaux de réseau régional (p. ex. la définition "point à multipoint" indique qu'un seul serveur de réseau local communique simultanément avec de nombreux serveurs locaux de réseau régional). Ces scénarios sont les suivants:

- relation "point à point" pour une seule instance;
- relation "point à point" pour des instances multiples (le nombre d'instances requises peut être identifié);
- relation "point à multipoint" pour une seule instance;
- relation "point à multipoint" pour des instances multiples (le nombre d'instances requises peut être identifié);
- relation "multipoint à point" pour une seule instance;
- relation "multipoint à point" pour des instances multiples (le nombre d'instances requises sera identifié si nécessaire).

NOTE – Le scénario "multipoint à multipoint" sera identique à une relation "point à point" pour instances multiples, à une relation "point à multipoint" pour instances multiples et/ou à une relation "multipoint à point" pour instances multiples.

Voir les Figures D.1 à D.3.

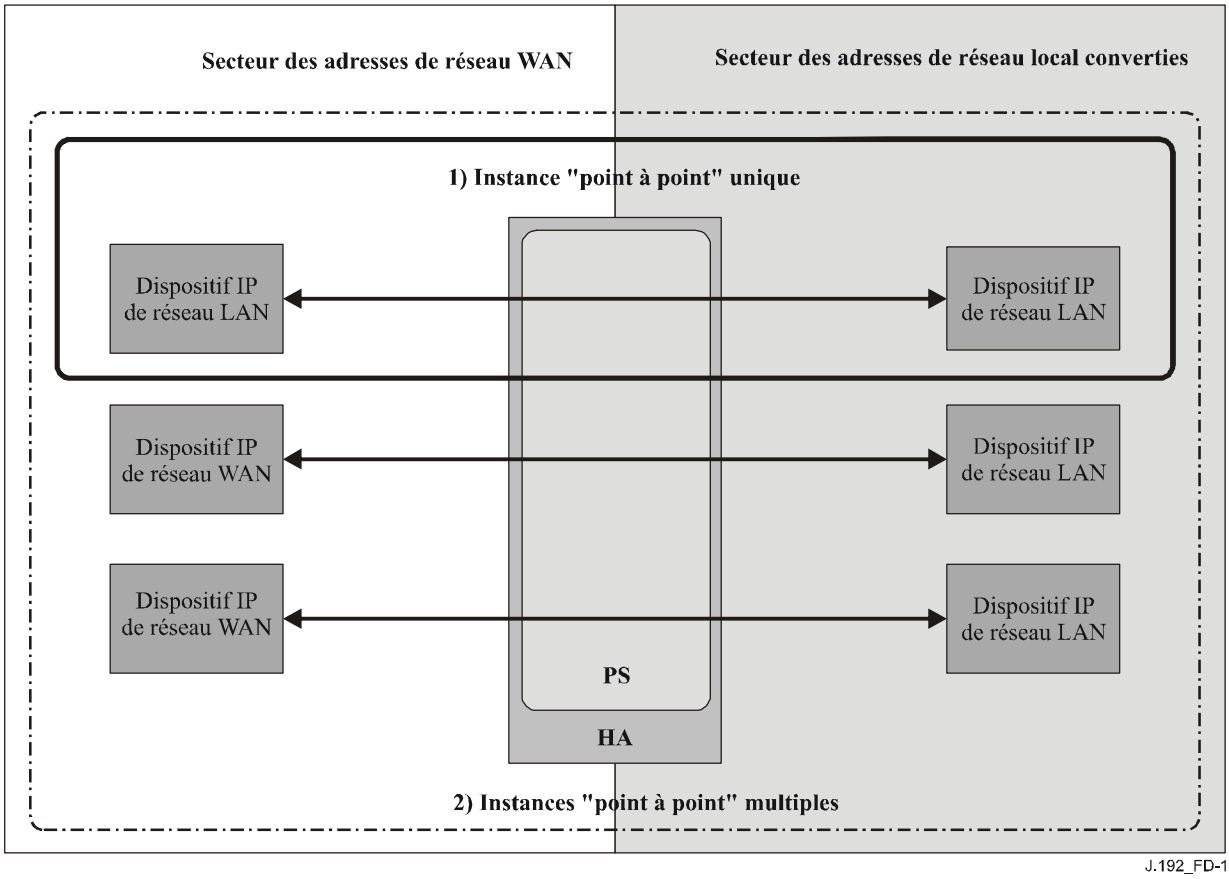


Figure D.1/J.192 – Scénarios "point à point"

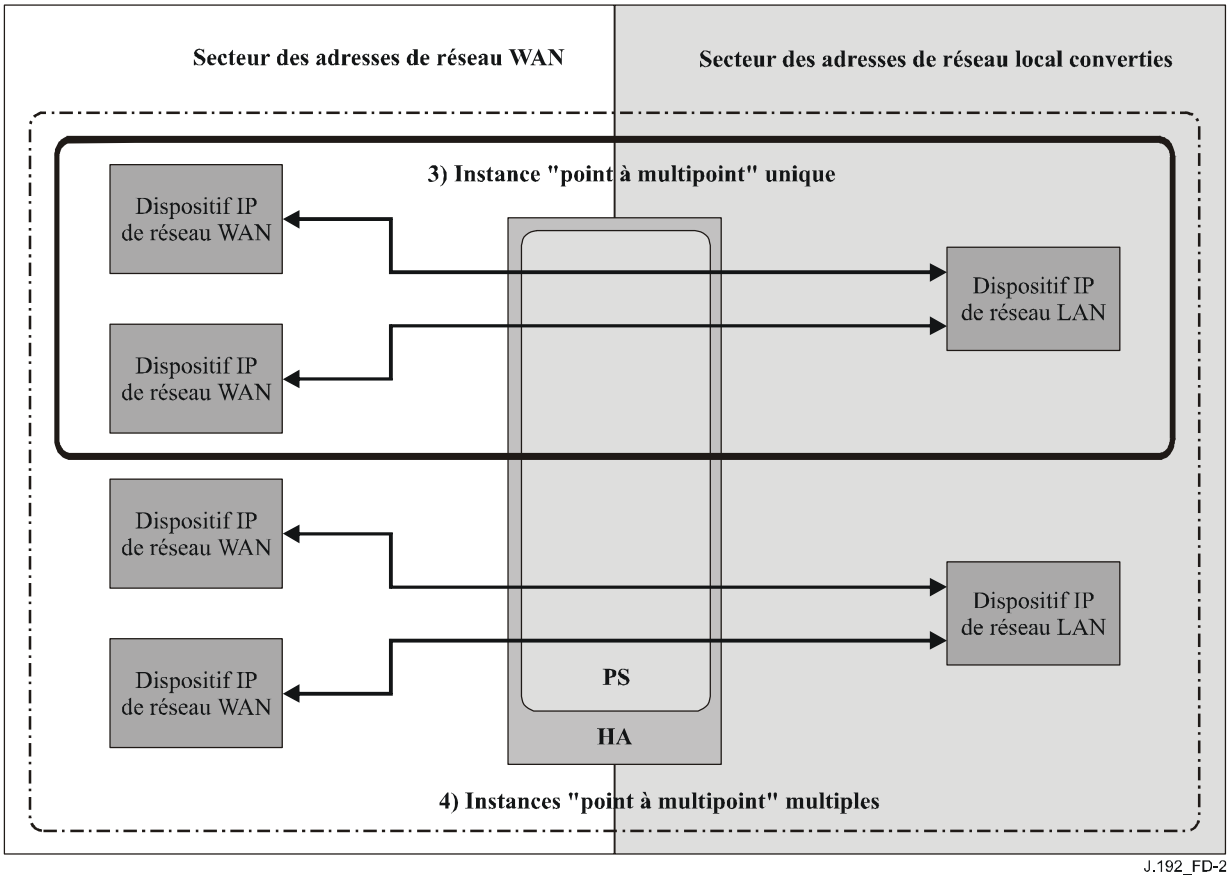


Figure D.2/J.192 – Scénarios "point à multipoint"

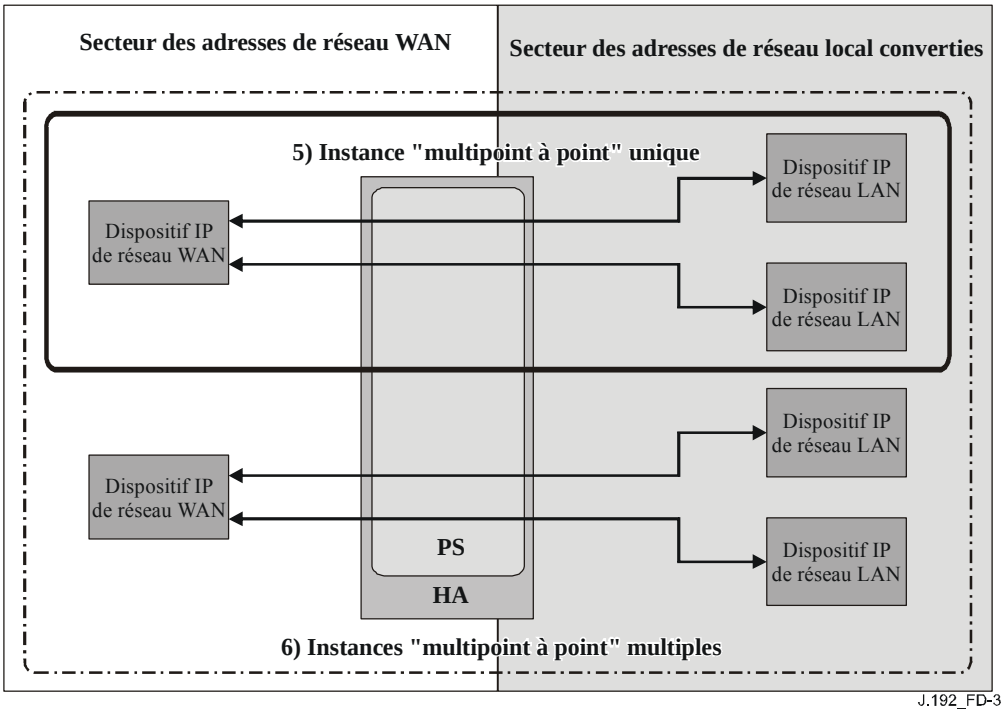


Figure D.3/J.192 – Scénarios "multipoint à point"

D.2 Applications nécessitant exclusivement une politique de pare-feu

Les Tableaux D.1 et D.2 identifient les applications et protocoles qui DOIVENT être pris en charge par conversion CAT et pare-feu. Cela n'exclut pas la prise en charge d'applications et de protocoles supplémentaires. Une fonction de conversion CAT/pare-feu qui peut prendre en charge ces applications et protocoles sera capable d'assurer la plupart des autres applications et protocoles qui ne contiennent pas d'adresse, de port ou d'autres informations affectées par la conversion d'adresse de réseau et qui ne négocient pas les sessions entrantes.

La liste de protocoles et d'applications reproduite dans le Tableau D.1 ci-dessous DOIT interfonctionner avec les implémentations par conversion CAT et pare-feu. Le pare-feu NE DOIT PAS commencer ses opérations avant que le message de préconfiguration terminée ait été émis par le dispositif PS. Les protocoles que le dispositif PS est tenu d'approvisionner ne sont pas notés dans ce tableau.

NOTE – Les applications qui nécessitent seulement une configuration par politique de pare-feu exclusive DOIVENT être prises en charge dans chacun des six scénarios relationnels sauf indication contraire dans la colonne des commentaires.

Tableau D.1/J.192 – Protocoles tenus d'opérer par conversion CAT et pare-feu CH

Application/Protocole	Ports	Commentaire
AOL IM	TCP/1090, 1091, 1092, 1093 et 13784	Valeur IP par défaut
CU-SeeMe	TCP/7648, 7649; UDP/7648, 7649, 24032	
DHCP		Valeur IP par défaut
DNS	UDP/53	IPCablecom et IPCable2Home
FTPS	989 et 990	
HTTP	TCP/80	Valeur IP par défaut
HTTPS	TCP/443	Valeur IP par défaut
IGMP et IP en multidiffusion		Exigence de l'Annexe CH 1.0
imap	143	
imap3	220	
IPSec	IKE > UDP/500 – ESP > IP/50 brut	Echange de clés IKE, mode tunnel, instance point à point unique (clé de prise en charge de CAT) Echange de clés IKE, mode de transport, instance point à point unique (mode de transfert) mode de transfert d'homologues IPCablecom et LAN
IRC	TCP/6665-6669	
Kerberos	1293	Secteur d'adresses IPCablecom et IPCable2Home du dispositif PS
L2TP	UDP/1701	
MediaPlayer (Windows)	TCP/80;1755	

Tableau D.1/J.192 – Protocoles tenus d'opérer par conversion CAT et pare-feu CH

Application/Protocole	Ports	Commentaire
Messagerie Microsoft	3330 – 3332	Valeur IP par défaut mcs-calypsoicf 3330 mcs-messaging 3331 mcs-mailsvr 3332
MGCP	2427, 2727	IPCablecom
Homologue à homologue (eDonkey)	TCP/4662 UDP/4665	eDonkey
Homologue à homologue (protocole P2P FastTrack)	TCP/1214	KaZaA, Grokster, etc.
Homologue à homologue (protocole P2P Gnutella)	TCP/6346	Gnutella, LimeWire, BearShare, Morpheus, etc.
Homologue à homologue (WinMX)	TCP/6699 UDP/6257	WinMX
Demande d'écho PING du protocole ICMP	IP/1 brut	IPCable2Home
POP3	TCP/110	Valeur IP par défaut
PPTP	Port de commande > TCP/1723 et GRE > IP/47 brut	
RealAudio/RealMedia	TCP: 80;443;554	
RSVP		IPCablecom
RTSP	TCP/554	
RTCP		IPCablecom
RTP		IPCablecom
SMTP	TCP/25	Valeur IP par défaut
SNMP	TCP/161 UDP/161	Secteur d'adresses IPCable2Home et IPCablecom
Message Trap du SNMP	TCP/162 UDP/162	Secteur d'adresses IPCable2Home et IPCablecom
SSH	TCP/22 UDP/22	Valeur IP par défaut
Syslog	UDP/514	Secteur d'adresses IPCable2Home et IPCablecom

Tableau D.1/J.192 – Protocoles tenus d'opérer par conversion CAT et pare-feu CH

Application/Protocole	Ports	Commentaire
Telnet	UDP/23	Requêtes de session sortantes. Valeur IP par défaut
TFTP	UDP/69	IPCablecom
Suivi de cheminement	IP/1 brut	Valeur IP par défaut La réponse à partir de tous les relais entre origine et destination doit être prise en charge
Messagerie Yahoo	TCP: 5050, 80 ou tout numéro disponible	Valeur IP par défaut

NOTE – Certains numéros de port énumérés dans le présent paragraphe avaient été précédemment libérés par l'autorité IANA, mais ont été récemment réattribués, de sorte qu'ils appartiennent maintenant à une autre application. Les protocoles RTP et Quicktime possèdent tous les deux les numéros 6970 à 6999 de la liste mais l'autorité IANA a maintenant attribué les numéros 6998 et 6999 aux protocoles iatp-highpri et iatp-normalpri. Le modèle IPCable2Home n'effectue aucune tentative en vue de corriger ce conflit.

D.3 Applications qui nécessitent une politique de pare-feu et une passerelle ALG

Il y a de nombreux cas où la conversion CAT et le pare-feu ne peuvent pas offrir aux applications et aux protocoles la transparence recherchée. Etant donné que la conversion CAT modifie les adresses de nœud d'extrémité (dans l'en-tête IP d'un paquet) en cours de route, certaines applications sont incapables de fonctionner par conversion CAT sans l'assistance d'une passerelle ALG. Si possible, des passerelles ALG propres aux applications DOIVENT être utilisées en conjonction avec la conversion CAT et avec la valeur appropriée de politique de pare-feu afin d'offrir le niveau de transparence recherché entre les applications. La fonction d'une passerelle ALG est propre à chaque application, de sorte qu'une liste d'applications, de protocoles et de scénarios qui DOIVENT être pris en charge est reproduite ci-dessous.

Tableau D.2/J.192 – Applications qui nécessitent une politique de pare-feu et une passerelle ALG

Application/ Protocole	Port	1) Relation point à point pour instance unique	2) Relation point à point pour instances multiples	3) Relation point à multipoint pour instance unique	4) Relation point à multipoint pour instances multiples	5) Relation multipoint à point pour instance unique	6) Relation multipoint à point pour instances multiples	Commentaires
FTP	20/tcp, 21/tcp	X	X	X	X	X	X	
Microsoft Netmeeting (H.323)	TCP/389 ILS 522 ULS 1503 T.120 1720 Etablissement d'appel 1731 Commande d'appel audio Commande dynamique d'appel TCP UDP dynamique 1024-65535 RTP sur UDP	X	X	X	X	X	X	
Messagerie MSN (H.323)	1863/tcp	X	X	X	X	X	X	Valeur IP par défaut
Net2Phone	6801/udp (également appels pour ouvrir 2 ports additionnels non spécifiés UDPPORT=6801 UDPPORT=XXXX TCPPORT=XXXX L'administrateur du réseau a besoin de s'assurer que le point UDPPORT 6801 est ouvert. Pour les autres points UDPPORT et TCPPORT, l'administrateur peut utiliser toute valeur comprise entre 1 et 30 000.)	X	X	X	X			
Quicktime 5	RTSP/TCP/554 RTP/UDP 6970-6999	X	X	X	X	X	X	La prise en charge de Quicktime sans passerelle ALG par le port 80 offre une performance inférieure à l'optimum.
Window Messenger (SIP)		X	X					Disponible sur Windows XP seulement

Annexe E

Bases MIB

E.1 IPCable2Home Address Portal (CAP) MIB requirement

Requirements

The IPCable2Home CAP MIB MUST be implemented as defined below.

```
CABH-CAP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Unsigned32,
    Integer32           FROM SNMPv2-SMI
    TimeStamp,
    TruthValue,
    RowStatus,
    DateAndTime,
    PhysAddress         FROM SNMPv2-TC
    OBJECT-GROUP,
    MODULE-COMPLIANCE   FROM SNMPv2-CONF
    InetAddressType,
    InetAddress,
    InetPortNumber      FROM INET-ADDRESS-MIB
    clabProjCableHome   FROM CLAB-DEF-MIB
    SnmpAdminString     FROM SNMP-FRAMEWORK-MIB;

cabhCapMib MODULE-IDENTITY
    LAST-UPDATED    "200502110000Z" --February 11, 2005
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
            858 Coal Creek Circle
            Louisville, Colorado 80027
            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com; mibs@cablelabs.com"
    DESCRIPTION
            "This MIB module supplies the basic management objects
            for the CableHome Address Portal (CAP) portion of
            the PS."
    ::=  { clabProjCableHome 3 }


    cabhCapObjects      OBJECT IDENTIFIER ::= { cabhCapMib 1 }
    cabhCapBase         OBJECT IDENTIFIER ::= { cabhCapObjects 1 }
    cabhCapMap          OBJECT IDENTIFIER ::= { cabhCapObjects 2 }


--========================================================================
--
--    General CAP Parameters
--
--========================================================================

cabhCapTcpTimeWait OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-write
```

```
    STATUS      current
    DESCRIPTION
            "This object is the maximum inactivity time to wait before
            assuming TCP session is terminated. It has no relation to
            the TCP session TIME_WAIT state referred to in [RFC 793]."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    DEFVAL { 300 }
    ::= { cabhCapBase 1 }

cabhCapUdpTimeWait OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The inactivity time to wait before destroying
            CAP mappings for UDP."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    DEFVAL { 300 }  -- 5 minutes
    ::={ cabhCapBase 2 }

cabhCapIcmpTimeWait OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The inactivity time to wait before destroying
            CAP mappings for ICMP."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    DEFVAL { 300 }  --  5 minutes
    ::= { cabhCapBase 3 }

cabhCapPrimaryMode OBJECT-TYPE
    SYNTAX      INTEGER {
                    napt(1),        -- NAT with Port Translation Mode
                    nat(2),         -- Traditional NAT Mode
                    passthrough(3)  -- Passthrough/Bridging Mode
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Primary Packet-handling Mode of the Portal Services
            logical element (PS) of a CableHome compliant residential
            gateway device. This object configures operation of the PS
            packet handling functions.

            When the value of this object is napt(1), the PS is
            required to support the Network Address and Port
            Translation (NAPT) process in accordance with the NAPT
            requirements defined in IETF RFC 3022. When operating in
            NAPT Primary Packet Handling Mode, the PS supports the
            translation of multiple LAN-Trans IP addresses and their
            TCP/UDP ports into a single WAN-Data IP address and its
            TCP/UDP ports.

            When the value of this object is nat(2), the PS is required
            to support the Network Address Translation (NAT) process in
```

```
            accordance with the NAT equirements defined in IETF RFC
            3022. When operating in NAT Primary Packet Handling Mode,
            the PS supports the translation of multiple LAN-Trans IP
            addresses into the same number of unique WAN-Data IP
            addresses.

            When the value of this object is passthrough(3), the PS is
            required to act as a transparent bridge in accordance with
            IEEE 802.1D. When operating in Passthrough Primary Packet
            Handling Mode, the PS does not translate network addresses,
            and bridges all traffic between its LAN and WAN interfaces.

            The PS MUST delete dynamically-created row entries from
            the cabhCapMappingTable, i.e., those with
            cabhCapMappingMethod = dynamic(2), when the value of
            cabhCapPrimaryMode changes. The PS MUST NOT delete
            statically-created row entries from the cabhCapMappingTable
            where cabhCapMappingMethod = static(1), when the value of
            cabhCapPrimaryMode changes."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    DEFVAL { napt }
    ::= { cabhCapBase 4 }

cabhCapSetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Reading this object always returns false(2). When the
            cabhCapSetToFactory object is set to true(1), the PS must
            take the following actions:

            1) Clear all entries in the cabhCapMappingTable and
               cabhCapPassthroughTable.
            2) Reset the following objects to their factory default
               values:
                 cabhCapTcpTimeWait,
                 cabhCapUdpTimeWait,
                 cabhCapIcmpTimeWait,
                 cabhCapPrimaryMode"
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    ::= { cabhCapBase 5 }

cabhCapLastSetToFactory OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when cabhCapSetToFactory was
            last set to true. Zero if never reset."
    ::= { cabhCapBase 6 }

cabhCapUpnpPortForwardingEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This MIB is effective only when the PS is performing NAPT.
            If this MIB object is set to false(2), the PS MUST disable
            the UPnP WANIpConnection service in the CableHome PS. If
```

```
            this MIB object is set to true(1), the PS MUST enable the
            WANIpConnection service in the PS. When the primary packet
            handling mode of the PS is C-NAT (2) or Passthrough(3),
            setting this MIB to true(1) MUST return InconsistentValue
            error."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    DEFVAL { 1 }
    ::= { cabhCapBase 7 }

cabhCapUpnpTimeWait OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The inactivity time to wait before destroying
            CAP mappings created by UPnP control points. The
            value of 0 indicates inactivity time wait of
            infinity, i.e., a UPnP entry does not get destroyed
            based on inactivity period."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    DEFVAL { 0 }  --  0 seconds, inactivity time wait of infinity.
    ::= { cabhCapBase 8 }


--========================================================================
--
--    cabhCapMappingTable (CAP Mapping Table)
--
--    The cabhCapMappingTable contains information pertaining to all
--    NAPT and NAT mappings in a CableHome(TM) compliant residential
--    gateway device.
--
--========================================================================


cabhCapMappingTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCapMappingEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains IP address mappings between private
            network addresses, or network addresses and port
            numbers/ICMP Identifiers, assigned to devices on the
            subscriber's home LAN, and network addresses, or network
            addresses and port numbers/ICMP Identifiers on the WAN,
            presumed to be on a separate subnetwork than the private
            IP addresses.  The CAP Mapping Table is used by the
            CableHome Address Portal (CAP) function of the PS to make
            packet forwarding decisions."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    ::= { cabhCapMap 1 }

cabhCapMappingEntry OBJECT-TYPE
    SYNTAX      CabhCapMappingEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
```

```
            "List of the private IP (LAN) address-to-cable
            operator assigned IP (WAN) address mappings stored
            in the PS and used by the PS to make packet
            forwarding decisions."
    INDEX { cabhCapMappingIndex }
    ::= { cabhCapMappingTable 1 }

CabhCapMappingEntry ::= SEQUENCE {
    cabhCapMappingIndex               INTEGER,
    cabhCapMappingWanAddrType         InetAddressType,
    cabhCapMappingWanAddr             InetAddress,
    cabhCapMappingWanPort             InetPortNumber,
    cabhCapMappingLanAddrType         InetAddressType,
    cabhCapMappingLanAddr             InetAddress,
    cabhCapMappingLanPort             InetPortNumber,
    cabhCapMappingMethod              INTEGER,
    cabhCapMappingProtocol            INTEGER,
    cabhCapMappingRowStatus           RowStatus,
    cabhCapMappingNumPorts            Unsigned32,
    cabhCapMappingRowDescr            SnmpAdminString,
    cabhCapMappingCreateTime          DateAndTime,
    cabhCapMappingLastUpdateTime      DateAndTime,
    cabhCapMappingDuration            Integer32,
    cabhCapMappingRemoteHostAddrType InetAddressType,
    cabhCapMappingRemoteHostAddr      InetAddress,
    cabhCapMappingEnable              TruthValue
    }

cabhCapMappingIndex OBJECT-TYPE
    SYNTAX      INTEGER   (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The Index into the CAP Mapping Table."
    ::= { cabhCapMappingEntry 1 }

cabhCapMappingWanAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address type assigned on the WAN side."
    DEFVAL { ipv4 }
    ::= { cabhCapMappingEntry 2 }

cabhCapMappingWanAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address assigned by the cable operator's address
            (DHCP) server, and comprising the WAN-side IP address
            of the CAP Mapping tuple. This object is populated
            either dynamically by LAN-to-WAN outbound traffic or
            statically by the cable operator."
    ::= { cabhCapMappingEntry 3 }

cabhCapMappingWanPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The TCP/UDP port number or ICMP Identifier
            on the WAN side. A port number/Identifier of
```

```
            0 indicates either a NAT or a DMZ mapping.
            A non-zero port number/Identifier indicates
            a NAPT mapping. If the value of
            cabhCapMappingNumPorts MIB object is non-zero,
            this MIB represents a starting TCP/UDP port
            number on the WAN side for which a mapping
            entry is created."
    DEFVAL { 0 }
    ::= { cabhCapMappingEntry 4 }

cabhCapMappingLanAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address type assigned on the LAN side."
    DEFVAL { ipv4 }
    ::= { cabhCapMappingEntry 5 }

cabhCapMappingLanAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address of the LAN-Trans IP Device. This object is
            populated either dynamically as a result of LAN-to-WAN
            outbound traffic or statically by the cable operator."
    ::= { cabhCapMappingEntry 6 }

cabhCapMappingLanPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The TCP/UDP port number or ICMP Identifier
            on the LAN side. A port number/Identifier
            of 0 indicates either a DMZ mapping or a NAT
            mapping. A non-zero port number/Identifier
            indicates a NAPT mapping. If the value of
            cabhCapMappingNumPorts MIB object is non-zero,
            then this MIB represents a starting TCP/UDP port
            number on the LAN side for which a mapping
            entry is created."
    DEFVAL { 0 }
    ::= { cabhCapMappingEntry 7 }

cabhCapMappingMethod OBJECT-TYPE
    SYNTAX      INTEGER {
                    static(1),
                    dynamic(2),
                    upnp(3)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Indicates how this mapping was created. Static means
            that it was provisioned, and dynamic means that it
            was handled by the PS itself. upnp (3) means that the
            CAP mapping entry was created by some UPnP compliant
            application."
    ::= { cabhCapMappingEntry 8 }

cabhCapMappingProtocol OBJECT-TYPE
    SYNTAX      INTEGER {
```

```
                    other(1),    -- any other protocol; e.g. IGMP
                    icmp(2),
                    udp(3),
                    tcp(4),
                    all(255)     -- covers all the protocols
                }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The protocol for this mapping entry. The value
            of other(1) represents a protocol other
            than ICMP, TCP, and UDP. Thus, when the value
            other(1) is specified for the cabhCapMappingProtocol
            value of a CAP Mapping Table entry,
            TCP, UDP or ICMP packets MUST NOT be forwarded even
            if the WAN and LAN IP address and port tuple
            of the packet matches with mapping entry.
            The value of all(255) represents all protocol types. Thus,
            when the cabhCapMappingProtocol value
            all(255) is specified for an entry in the CAP Mapping
            Table, traffic of all protocol types MUST be forwarded
            accordingly if the WAN and LAN IP address and port tuple
            in the packet matches the mapping entry."
    ::= { cabhCapMappingEntry 9 }

cabhCapMappingRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The RowStatus interlock for the creation and deletion
            of a cabhCapMappingTable entry. Changing the value of
            the IP address or port number columns of the CAP
            Mapping Table may have an effect on active traffic,
            so the PS will prevent modification of this table's
            columns and return an inconsistentValue error when
            cabhCapMappingRowStatus object is active(1).

            The PS must not allow RowStatus to be set to
            notInService(2) by a manager.

            A newly created row cannot be set to active(1) until
            the corresponding instances of cabhCapMappingWanAddr,
            cabhCapMappingLanAddr, and cabhCapMappingProtocol have
            been set.

            If the manager attempts to populate a row entry in
            the table with a non-unique value for the combination
            of cabhCapMappingWanAddr and range of WAN port(s)
            (identified by cabhCapMappingWanPort to
            cabhCapMappingWanPort + cabhCapMappingNumPorts –1),
            or a non-unique value for the combination of
            cabhCapMappingLanAddr and range of LAN port(s)
            (identified by cabhCapMappingLanPort to
            cabhCapMappingLanPort + cabhCapMappingNumPorts - 1),
            the PS MUST prevent the creation of this row and return
            an inconsistentValue error. This prevents creation of
            entries with overlapping port ranges in the CAP table.

            If the manager attempts to populate a row entry with
            a zero value for cabhCapMappingWanPort and a non-zero
            value for cabhCapMappingLanPort or a row entry with a
            zero value for cabhCapMappingLanPort and a non-zero value
            for cabhCapMappingWanPort, the PS MUST prevent the
```

```
            creation of this row and return an inconsistentValue
            error. This prevents creation of invalid NAT or NAPT entries.

            If the manager attempts to populate a row entry with non-zero
            values for both cabhCapMappingWanPort and
            cabhCapMappingLanPort, but a zero value for
            cabhCapMappingNumPorts, the PS MUST prevent
            the creation of this row and return an inconsistentValue
            error. This prevents creation of NAPT entries.

            When Primary Packet-handling Mode is NAPT
            (cabhCapPrimaryMode is napt(1)), provisioned rows can be
            set to active(1) regardless of whether the value to which
            cabhCapMappingWanPort, cabhCapMappingLanPort, and
            cabhCapMappingNumPorts have been set is zero or nonzero.

            When Primary Packet-handling Mode is NAT
            (cabhCapPrimaryMode is nat(2)), a newly created row can
            not be set to active(1) if a non-zero value has been set
            for cabhCapMappingWanPort, cabhCapMappingLanPort and
            cabhCapMappingNumPorts.

            In NAPT Primary Packet-handling mode, a row
            entry with zero values for cabhCapMappingWanPort,
            cabhCapMappingLanPort, and cabhCapMappingNumPorts
            objects represents a DMZ entry."
    ::={ cabhCapMappingEntry 10 }

cabhCapMappingNumPorts OBJECT-TYPE
    SYNTAX      Unsigned32(1..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "This object represents the number of ports
            available for port translation
            on both LAN and WAN side.

            When both cabhCapMappingWanPort and
            cabhCapMappingLanPort are set to zero,
            the PS MUST ignore this MIB object, and
            such a row entry represents either a DMZ entry
            (when primary packet handling mode is NAPT) or
            a NAT entry (when primary packet handling mode is
            NAT).

            When a row entry is created with non-zero
            values for cabhCapMappingWanPort,
            cabhCapMappingLanPort, and cabhCapMappingNumPorts
            the PS MUST translate range of ports on
            the WAN side (identified by cabhCapMappingWanPort
            to cabhCapMappingWanPort + cabhCapMappingNumPorts-1)
            to range of ports on the LAN side (identified by
            cabhCapMappingLanPort to cabhCapMappingLanPort +
            cabhCapMappingNumPorts-1).

            The PS MUST ignore this MIB for a CAP mapping
            entry with the value of cabhCapMappingProtocol
            equal to icmp(2)."
    DEFVAL { 1 }
    ::= { cabhCapMappingEntry 11 }

cabhCapMappingRowDescr OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-create
```

```
    STATUS      current
    DESCRIPTION
            "A string value that can be used to describe
             the purpose or attributes of the CAP Mapping
             entry."
    DEFVAL { "" }
    ::= { cabhCapMappingEntry 12 }

cabhCapMappingCreateTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "For dynamic(2) and upnp(3) CAP mapping entries, the PS MUST
             set this MIB with date and time when the entry is created.
             The PS MUST set the value of this MIB to zero valued
             11-byte string for static CAP mapping entries. This MIB
             object MUST NOT persist across the PS reboot."
    ::= { cabhCapMappingEntry 13 }

cabhCapMappingLastUpdateTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The PS MUST set the value of this MIB
             to zero valued 11-byte string for static
             CAP mapping entries. For dynamic(2) CAP
             Mapping entries, the PS MUST set the value
             of this MIB to the value of cabhCapMappingCreateTime.
             For upnp(3) CAP mapping entries, the PS MUST
             set this MIB with date and time when the entry
             is last updated. When the upnp(3)entry is first
             created, the PS MUST set this MIB with the value
             of cabhCapMappingCreateTime MIB. This MIB object
             MUST NOT persist across the PS reboot."
    ::= { cabhCapMappingEntry 14 }

cabhCapMappingDuration OBJECT-TYPE
    SYNTAX      Integer32 (-1|0..2147483647)
    UNITS       "seconds"
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "When a value greater than zero
             is assigned to this object, the PS MUST
             remove the CAP entry after the time
             duration, represented by
             this object, elapses starting from
             cabhCapMappingLastUpdateTime.

             When a value of 0 is assigned to this object,
             the PS MUST retain the CAP mapping entry
             until reboot or reset. The PS MUST retain
             a CAP mapping entry with cabhCapMappingDuration
             MIB set to 0 and cabhCapMappingMethod set
             to static(1) across the reboots. The PS MUST
             NOT retain a CAP mapping entry with
             cabhCapMappingDuration MIB set to 0 and
             cabhCapMappingMethod set to upnp(3) across
             the reboots.

             When a value of -1 is assigned for this
             MIB, the PS MUST ignore this MIB and
```

```
                MUST remove the CAP mapping entries
                based on TCP, UDP and ICMP inactivity
                time-wait depending upon their protocol
                type.

                When the cabhCapMappingMethod object is
                static(1), the default value for this object
                is 0.

                When the cabhCapMappingMethod object is
                dynamic(2), the PS MUST set the value of
                this object to -1.

                When the cabhCapMappingMethod object is
                upnp(3), the default value for this object
                is -1."

    ::= { cabhCapMappingEntry 15 }

cabhCapMappingRemoteHostAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP address type for a remote host on the WAN side."
    DEFVAL { ipv4 }
    ::= { cabhCapMappingEntry 16 }

cabhCapMappingRemoteHostAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP address of the remote host for
            a CAP mapping entry. The packet traversing
            through the PS is either originated
            from or is destined to this remote host.
            The value of all zeros for this MIB object
            indicates any IP address for a remote host."
    DEFVAL { '00000000'h }
    ::= { cabhCapMappingEntry 17 }

cabhCapMappingEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This MIB allows the PS to enable or disable
            a particular CAP mapping entry. When this MIB
            is set to true(1) for a CAP mapping entry, the
            PS MUST correctly route the traffic that
            matches this entry. When this MIB is set to
            false(2) for a CAP mapping entry, the PS MUST
            NOT route the traffic that matches this entry."
    DEFVAL { true }
    ::= { cabhCapMappingEntry 18 }

--============================================================================
--
--    cabhCapPassthroughTable (CAP Passthrough Table)
--
--    The cabhCapPassthroughTable contains the hardware addresses
--    for all LAN IP Devices for which the PS will bridge traffic at
--    OSI Layer 2 when the PS's cabhCapPrimaryMode is set to forward
```

```
--    traffic at OSI Layer 3 (NAPT/NAT) for all other hardware
--    addresses.
--
--========================================================================

cabhCapPassthroughTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCapPassthroughEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains hardware addresses of LAN IP Devices
            for which the PS will bridge traffic at OSI Layer 2."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    ::= {  cabhCapMap 2 }

cabhCapPassthroughEntry OBJECT-TYPE
    SYNTAX      CabhCapPassthroughEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "List of hardware addresses of LAN IP Devices for which
            the PS will bridge traffic at OSI Layer 2."
    INDEX { cabhCapPassthroughIndex }
::= { cabhCapPassthroughTable 1 }

CabhCapPassthroughEntry::=SEQUENCE {
    cabhCapPassthroughIndex          INTEGER,
    cabhCapPassthroughMacAddr        PhysAddress,
    cabhCapPassthroughRowStatus      RowStatus
    }

cabhCapPassthroughIndex OBJECT-TYPE
    SYNTAX      INTEGER (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index into the CAP Passthrough Table."
    ::= { cabhCapPassthroughEntry 1 }

cabhCapPassthroughMacAddr OBJECT-TYPE
    SYNTAX      PhysAddress (SIZE(0..16))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Hardware address of the LAN IP Device for which the PS
            MUST bridge traffic at OSI Layer 2."
    ::={ cabhCapPassthroughEntry 2 }

cabhCapPassthroughRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The RowStatus interlock for the creation and
            deletion of a cabhCapPassthroughTable entry.
            Any writable object in each row can be modified
            at any time while the row is active(1)."
    ::= { cabhCapPassthroughEntry 3 }
--
-- notification group is for future extension.
--
```

```
cabhCapNotification    OBJECT IDENTIFIER ::= {
    cabhCapMib 2 0 }
cabhCapConformance     OBJECT IDENTIFIER ::= {
    cabhCapMib 3 }
cabhCapCompliances     OBJECT IDENTIFIER ::= {
    cabhCapConformance 1 }
cabhCapGroups          OBJECT IDENTIFIER ::= {
    cabhCapConformance 2 }

--
--    Notification Group
--


-- compliance statements

cabhCapBasicCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for devices that implement
            the CableHome Portal Services functionality."
    MODULE   --cabhCapMib

-- unconditionally mandatory groups

MANDATORY-GROUPS {
    cabhCapGroup
    }

OBJECT cabhCapMappingProtocol
    SYNTAX      INTEGER { icmp(2) }
    WRITE-SYNTAX  INTEGER { other(1), udp(3), tcp(4), all(255) }
    DESCRIPTION
            "icmp(2) applies only to dynamic entries."

    ::= { cabhCapCompliances 1 }


cabhCapGroup OBJECT-GROUP
    OBJECTS {
    cabhCapTcpTimeWait,
    cabhCapUdpTimeWait,
    cabhCapIcmpTimeWait,
    cabhCapPrimaryMode,
    cabhCapSetToFactory,
    cabhCapLastSetToFactory,
    cabhCapMappingWanAddrType,
    cabhCapMappingWanAddr,
    cabhCapMappingWanPort,
    cabhCapMappingLanAddrType,
    cabhCapMappingLanAddr,
    cabhCapMappingLanPort,
    cabhCapMappingMethod,
    cabhCapMappingProtocol,
    cabhCapMappingRowStatus,
    cabhCapPassthroughMacAddr,
    cabhCapPassthroughRowStatus,
    cabhCapMappingNumPorts,
    cabhCapMappingRowDescr,
    cabhCapMappingCreateTime,
    cabhCapMappingLastUpdateTime,
    cabhCapMappingDuration,
    cabhCapUpnpPortForwardingEnable,
    cabhCapUpnpTimeWait,
```

```
    cabhCapMappingRemoteHostAddrType,
    cabhCapMappingRemoteHostAddr,
    cabhCapMappingEnable
    }
    STATUS      current
    DESCRIPTION
            "Group of objects for CableHome CAP MIB."
    ::= { cabhCapGroups 1 }

END
```

E.2 IPCable2Home DHCP Portal (CDP) MIB requirement

The IPCable2Home CDP MIB MUST be implemented as defined below.

```
CABH-CDP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Integer32,
    Unsigned32              FROM SNMPv2-SMI
    PhysAddress,
    TruthValue,
    DateAndTime,
    TimeStamp,
    RowStatus               FROM SNMPv2-TC --RFC2579
    OBJECT-GROUP,
    MODULE-COMPLIANCE       FROM SNMPv2-CONF
    InetAddressType,
    InetAddress             FROM INET-ADDRESS-MIB
    SnmpAdminString         FROM SNMP-FRAMEWORK-MIB
    clabProjCableHome       FROM CLAB-DEF-MIB;

cabhCdpMib MODULE-IDENTITY
    LAST-UPDATED    "200412160000Z"  -- December 16, 2004
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
            858 Coal Creek Circle
            Louisville, Colorado 80027
            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com; mibs@cablelabs.com"
    DESCRIPTION
            "This MIB module supplies the basic management objects
            for the CableHome DHCP Portal (CDP) portion of the PS
            database."
    ::=  { clabProjCableHome 4 }

cabhCdpObjects          OBJECT IDENTIFIER ::= { cabhCdpMib 1 }
cabhCdpBase             OBJECT IDENTIFIER ::= { cabhCdpObjects 1 }
cabhCdpAddr             OBJECT IDENTIFIER ::= { cabhCdpObjects 2 }
cabhCdpServer           OBJECT IDENTIFIER ::= { cabhCdpObjects 3 }

--
--    The following group describes the base objects in the CableHome
--    DHCP Portal.  The rest of this group deals with addresses defined
--    on the LAN side.
--
```

```
cabhCdpSetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Reading this object always returns false(2). When the
            cabhCdpSetToFactory object is set to true(1), the PS must
            take the following actions:
            1) Clear all cabhCdpLanAddrEntries in the CDP LAN Address
               Table.
            2) The CDS must offer the factory default DHCP options
               at the next lease renewal time.
            3) Reset the following objects to their factory default
               values:

               cabhCdpLanTransThreshold,
               cabhCdpLanTransAction,
               cabhCdpWanDataIpAddrCount,
               cabhCdpTimeOffsetSelection,
               cabhCdpSnmpSetTimeOffset,
               cabhCdpDaylightSavingTimeEnable,
               cabhCdpLanPoolStartType,
               cabhCdpLanPoolStart,
               cabhCdpLanPoolEndType,
               cabhCdpLanPoolEnd,
               cabhCdpServerNetworkNumberType,
               cabhCdpServerNetworkNumber,
               cabhCdpServerSubnetMaskType,
               cabhCdpServerSubnetMask,
               cabhCdpServerTimeOffset,
               cabhCdpServerRouterType,
               cabhCdpServerRouter,
               cabhCdpServerDnsAddressType,
               cabhCdpServerDnsAddress,
               cabhCdpServerSyslogAddressType,
               cabhCdpServerSyslogAddress,
               cabhCdpServerDomainName,
               cabhCdpServerTTL,
               cabhCdpServerInterfaceMTU,
               cabhCdpServerVendorSpecific,
               cabhCdpServerLeaseTime,
               cabhCdpServerDhcpAddressType,
               cabhCdpServerDhcpAddress,
               cabhCdpServerCommitStatus"
::= { cabhCdpBase 1 }

cabhCdpLanTransCurCount OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The current number of active leases in the
            cabhCdpLanAddrTable (the number of row entries in the
            table that have a cabhCdpLanAddrMethod value of
            reservationActive(2) or dynamicActive (4)).  This count
            does not include expired leases or reservations not
            associated with a current lease."
    ::= { cabhCdpBase 2 }

cabhCdpLanTransThreshold OBJECT-TYPE
    SYNTAX      INTEGER (0..65533)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
```

```
            "The threshold number of LAN-Trans IP addresses allocated
            or assigned above which the PS generates an alarm
            condition. Whenever an attempt is made to allocate a
            LAN-Trans IP address when cabhCdpLanTransCurCount is
            greater than or equal to cabhCdpLanTransThreshold, an
            event is generated. A value of 0 indicates that the CDP
            sets the threshold at the highest number of addresses in
            the LAN address pool."
    DEFVAL { 0 }
    ::= { cabhCdpBase 3 }

cabhCdpLanTransAction OBJECT-TYPE
    SYNTAX      INTEGER {
                    normal(1),
                    noAssignment(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The action taken when the CDS assigns a LAN-Trans
            address and the number of LAN-Trans addresses assigned
            (cabhCdpLanTransCurCount) is greater than the threshold
            (cabhCdpLanTransThreshold). The actions are as follows:
            normal - assign a LAN-Trans IP address as would
            normally occur if the threshold was not exceeded.
            noAssignment - do not assign a LAN-Trans IP address."
    DEFVAL { normal }
    ::= { cabhCdpBase 4 }

cabhCdpWanDataIpAddrCount OBJECT-TYPE
    SYNTAX      INTEGER ( 0..63 )
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This is the number of WAN-Data IP addresses the
            PS's CDC must attempt to acquire via DHCP. When
            this MIB object is incremented, the CDC MUST
            immediately attempt to acquire additional WAN-Data
            IP addresses. When this MIB object is decremented, the
            CDC MUST not renew the leases for the appropriate
            number of WAN-Data IP addresses."
    DEFVAL { 0 }
    ::= { cabhCdpBase 5 }

cabhCdpLastSetToFactory    OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when cabhCdpSetToFactory was
            last set to true. Zero if never reset."
    ::= { cabhCdpBase 6 }

cabhCdpTimeOffsetSelection OBJECT-TYPE
    SYNTAX      INTEGER {
                useDhcpOption2 (1),
                useSnmpSetOffset(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object selects the source to be used by the PS in
            determining the time offset to the time of day acquired
            from the time server. It is intended to be used in cases
```

```
            where the time zone information provisioned by the ToD
            server or DHCP Server (in DHCP Option 2) is different from
            the time zone where the provisioned device is physically
            located.

            Setting this object to useDhcpOption2(1) configures the PS
            to use the value of DHCP option 2 from the DHCP ACK message
            for time of day offset. Setting this object to
            useSnmpSetOffset(2) configures the PS to use the value of
            cabhCdpServerSnmpSetTimeOffset for time of day offset, and
            to ignore DHCP option 2. When the value of this object is
            changed, the PS MUST immediately begin using the time
            offset specified by the value of this object, regardless
            of which time offset the PS was using before the update
            occurred."
    DEFVAL { useDhcpOption2 }
 ::= { cabhCdpBase 7 }

cabhCdpSnmpSetTimeOffset OBJECT-TYPE
    SYNTAX      Integer32 (-43200..46800)  --  -12 to +13 hours (seconds)
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object is intended to be used in cases where the
            service provider's provisioning system serves devices in
            multiple time zones, or for other times when the service
            provider wants UTC time offset to be provisioned in a
            device other than from the ToD server or from the DHCP
            Server (in DHCP option 2).

            This object allows a manager to set a value for UTC time
            offset. If DHCP option 2 is not present in the DHCP ACK
            message, or if the value of DHCP option 2 is null, and time
            offset information is not provided in the response received
            from the time of day server, the PS MUST add the value of
            cabhCdpServerTimeOffset to the UTC time acquired from the
            time of day server to create the current time of day.

            If the value of cabhCdpServerTimeOffsetSelection is
            useSnmpSetOffset(2), the PS adds the value of
            cabhCdpServerSnmpSetTimeOffset to the UTC time acquired
            from the time of day server to create the current time
            of day.

            If the value of cabhCdpServerTimeOffsetSelection is
            useDhcpOption2(1), the PS ignores
            cabhCdpServerSnmpSetTimeOffset."
    DEFVAL { 0 }
    ::= { cabhCdpBase 8 }

cabhCdpDaylightSavingTimeEnable OBJECT-TYPE
    SYNTAX      INTEGER{
                enabled(1),
                disabled(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object allows a manager to configure the PS to adjust
            the current time of day based on Daylight Saving Time. If
            the value of this object is enabled(1), the PS adds 3600
            seconds and the time offset specified by
            cabhCdpServerTimeOffsetSelection to the UTC time acquired
```

```
            from the time of day server to create the current time of
            day during Daylight Saving Time, and adds only the time
            offset specified by cabhCdpServerTimeOffsetSelection to the
            UTC time acquired from the time of day server during
            standard time. The PS is responsible for knowing the date
            and time of each transition between Daylight Saving Time
            and standard time.

            If the value of this object is disabled(2), the PS adds
            only the time offset specified by
            cabhCdpServerTimeOffsetSelection to the UTC time acquired
            from the time of day server."
    DEFVAL { disabled }
    ::= { cabhCdpBase 9 }
--
--    CDP Address Management Tables
--
--=========================================================================
--
--    cabhCdpLanAddrTable (CDP LAN Address Table)
--
--    The cabhCdpLanAddrTable contains the DHCP parameters
--    for each IP address served to the LAN-Trans realm.
--
--    This table contains a list of entries for the LAN side CDP
--    parameters. These parameters can be set
--    either by the CDP or by the cable operator through the CMP.
--
--=========================================================================

cabhCdpLanAddrTable OBJECT-TYPE
       SYNTAX      SEQUENCE OF CabhCdpLanAddrEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
               "This table is a list of LAN-Trans realm parameters.
               This table has one row entry for each allocated
               LAN-Trans IP address.  Each row must have at least a
               valid cabhCdpLanAddrMethod, a cabhCdpLanAddrIpType, a
               unique cabhCdpLanAddrIp, and a unique
               cabhCdpLanAddrClientId value.

               Static/Manual address assignment: To create a new DHCP
               address reservation, the NMS creates a row with: an
               index comprised of a new cabhCdpLanAddrIp and its
               cabhCdpLanAddrIpType, a new unique
               cabhCdpLanAddrClientID, (an empty LeaseCreateTime and
               empty LeaseExpireTime,) and a
               cabhCdpLanDataAddrRowStatus of createAndGo(4).  If the
               syntax and values of the new row - indicating a
               reservation - are valid, the PS must set
               cabhCdpLanAddrMethod to reservationInactive(1) and
               cabhCdpLanDataAddrRowStatus to active(1).  When the PS
               grants a lease for a reserved IP, it must set the
               cabhCdpLanAddrMethod object for that row to
               reservationActive(2).  When a lease for a reserved IP
               expires, the PS must set the corresponding row's
               cabhCdpLanAddrMethod object to reservationInactive(1).
               For row entries that represent lease reservations - rows
               in which the cabhCdpLanAddrMethod object has a value of
               either reservationInactive(1) or reservationActive(2) -
               the cabhCdpLanAddrIpType, cabhCdpLanAddrIp,
               cabhCdpLanAddrClientID, cabhCdpLanAddrMethod, and
               cabhCdpLanAddrHostName object values must persist across
```

```
                PS reboots.

                Dynamic address assignment:  When the PS grants a lease
                for a non-reserved IP, it must set the
                cabhCdpLanAddrMethod object for that row to
                dynamicActive(4).  When a lease for a non-reserved IP
                expires, the PS must set the corresponding row's
                cabhCdpLanAddrMethod object to dynamicInactive(3).  The
                PS must create new row entries using cabhCdpLanAddrIp
                values that are unique to this table.  If all
                cabhCdpLanAddrIp values in the range defined by
                cabhCdpLanPoolStart and cabhCdpLanPoolEnd are in use in
                this table, the PS may overwrite the
                cabhCdpLanAddrClientId of a row that has a
                cabhCdpLanAddrMethod object with a value of
                dynamicInactive(3) with a new cabhCdpLanAddrClientId
                value and use that cabhCdpLanAddrIp as part of a new
                lease.  For row entries that represent active leases -
                rows in which the cabhCdpLanAddrMethod object has a
                value of dynamicActive(4) - the cabhCdpLanAddrIpType,
                cabhCdpLanAddrIp, cabhCdpLanAddrClientID,
                cabhCdpLanAddrMethod, and cabhCdpLanAddrHostName object
                values must persist across PS reboots."
    ::= { cabhCdpAddr 1 }

cabhCdpLanAddrEntry OBJECT-TYPE
    SYNTAX      CabhCdpLanAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "List of general parameters pertaining to LAN-Trans IP
            address reservations and leases."
    INDEX { cabhCdpLanAddrIpType, cabhCdpLanAddrIp }
    ::= { cabhCdpLanAddrTable 1 }

CabhCdpLanAddrEntry ::= SEQUENCE {
    cabhCdpLanAddrIpType              InetAddressType,
    cabhCdpLanAddrIp                  InetAddress,
    cabhCdpLanAddrClientID            PhysAddress,
    cabhCdpLanAddrLeaseCreateTime     DateAndTime,
    cabhCdpLanAddrLeaseExpireTime     DateAndTime,
    cabhCdpLanAddrMethod              INTEGER,
    cabhCdpLanAddrHostName            SnmpAdminString,
    cabhCdpLanAddrRowStatus           RowStatus
    }

cabhCdpLanAddrIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The type of IP address assigned to the LAN IP Device
            in the LAN-Trans Realm."
    ::= { cabhCdpLanAddrEntry 1 }

cabhCdpLanAddrIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The address assigned to the LAN IP Device. This parameter
            is entered by the CDP when the CDS grants a lease to a
            LAN IP Device in the LAN-Trans realm and creates a row
            in this table. Alternatively, this parameter can be
```

```
            entered by the NMS through the CMP, when the NMS creates
            a new DHCP address reservation.  Each cabhCdpLanAddrIp
            in the table must fall within the range of IPs defined
            inclusively by cabhCdpLanPoolStart and
            cabhCdpLanPoolEnd.  The PS must return an
            inconsistentValue error if the NMS attempts to
            create a row entry with a cabhCdpLanAddrIP value that falls
            outside of this range or is not unique from all existing
            cabhCdpLanAddrIP entries in this table. The address type of
            this object is specified by cabhCdpLanAddrIpType."
    ::= { cabhCdpLanAddrEntry 2 }

cabhCdpLanAddrClientID OBJECT-TYPE
    SYNTAX      PhysAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The client's (i.e., LAN IP Device's) hardware address as
            indicated in the chaddr field of its DHCP REQUEST message.
            There is a one-to-one relationship between the hardware
            address and the LAN IP Device. This parameter is entered
            by the PS (CDP) when the CDS grants a lease to a LAN IP
            Device in the LAN-Trans realm and creates a row in this
            table. Alternatively this parameter can be created by the
            NMS through the CMP, when the NMS creates a new DHCP
            address reservation by accessing the
            cabhCdpLanDataAddrRowStatus object with an index
            comprised of a unique cabhCdpLanAddrIp and creating
            a row with a unique cabhCdpLanAddrClientID."
    ::= { cabhCdpLanAddrEntry 3 }

cabhCdpLanAddrLeaseCreateTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This is the date and time when the LAN IP lease was
            created (if it has not yet been renewed) or last renewed.
            This MIB object contains a zero valued 11-byte string
            when a reservation is created for a LAN IP address
            and it maintains this value until the LAN IP Device
            acquires its lease and cabhCdpLanAddrMethod
            becomes reservationActive(2)."
    ::= { cabhCdpLanAddrEntry 4 }

cabhCdpLanAddrLeaseExpireTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This is the date and time when the LAN IP address lease
            expired or will expire. This MIB object contains a zero
            valued 11-byte string when a reservation is created for
            a LAN IP address and it maintains this value until the
            LAN IP Device acquires its lease and
            cabhCdpLanAddrMethod becomes reservationActive(2)."
    ::= { cabhCdpLanAddrEntry 5 }

cabhCdpLanAddrMethod OBJECT-TYPE
    SYNTAX      INTEGER {
                    mgmtReservationInactive(1),
                    mgmtReservationActive(2),
                    dynamicInactive(3),
                    dynamicActive(4),
```

```
                    psReservationInactive(5),
                    psReservationActive(6)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP allocation method indicated by this row.

            The value of mgmtReservationInactive(1)
            indicates an externally provisioned IP address
            reservation that has not yet been leased or that
            has an expired lease. This indicates an IP address
            lease reservation created either by an operator or
            a user.

            The value of mgmtReservationActive(2)
            indicates an externally provisioned IP address
            reservation that has an active lease. This indicates
            an IP address lease reservation created either
            by an operator or a user.

            The value of dynamicInactive(3) indicates an
            IP address that was once dynamically assigned to a
            LAN-Trans by the PS device but currently
            has an expired lease.

            The value of dynamicActive(4)indicates an IP
            Address that was dynamically assigned to a
            LAN-Trans device by the PS and has a current
            active lease.

            The value of psReservationInactive(5)
            indicates an IP address reservation created by some
            internal process of the PS and has not yet been
            leased or has an expired lease.

            The value of psReservationActive(6)
            indicates an IP address reservation created by some
            internal process of the PS that has an active lease."
    ::= { cabhCdpLanAddrEntry 6 }

cabhCdpLanAddrHostName OBJECT-TYPE
    SYNTAX      SnmpAdminString(SIZE(0..80))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This is the Host Name of the LAN IP address, based on DCHP
            option 12."
    ::= { cabhCdpLanAddrEntry 7 }

cabhCdpLanAddrRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The RowStatus interlock for creation and deletion of row
            entries. The PS must not allow the NMS to set RowStatus
            to notInService(2). The PS must assign a RowStatus of
            notInService(2) to any new row entry created with a
            non-unique, cabhCdpLanAddrClientID value. The PS must
            assign a RowStatus of notReady(3) to any new row entry
            created without a cabhCdpLanAddrClientID.  The PS will
            prevent modification of this table's columns and return an
            inconsistentValue error, if the NMS attempts to make such
```

```
            modifications while the RowStatus is active(1)."
    ::= { cabhCdpLanAddrEntry 8 }

--============================================================================
--
--    cabhCdpWanDataAddrTable (CDP WAN-Data Address Table)
--
--    The cabhCdpWanDataAddrTable contains the configuration or DHCP
--    parameters for each IP address mapping per WAN-Data IP Address.
--
--============================================================================

cabhCdpWanDataAddrTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCdpWanDataAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains WAN-Data address realm information."
    ::= { cabhCdpAddr 2 }

cabhCdpWanDataAddrEntry OBJECT-TYPE
    SYNTAX      CabhCdpWanDataAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "List of general parameter for CDP WAN-Data address realm."
    INDEX { cabhCdpWanDataAddrIndex }
    ::= { cabhCdpWanDataAddrTable 1 }

CabhCdpWanDataAddrEntry ::= SEQUENCE {
    cabhCdpWanDataAddrIndex        INTEGER,
    cabhCdpWanDataAddrClientId     OCTET STRING,
    cabhCdpWanDataAddrIpType       InetAddressType,
    cabhCdpWanDataAddrIp           InetAddress,
    cabhCdpWanDataAddrRenewalTime  Integer32,
    cabhCdpWanDataAddrRowStatus    RowStatus,
    cabhCdpWanDataAddrLeaseCreateTime DateAndTime,
    cabhCdpWanDataAddrLeaseExpireTime DateAndTime
    }

cabhCdpWanDataAddrIndex OBJECT-TYPE
    SYNTAX      INTEGER (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Index into table."
    ::= { cabhCdpWanDataAddrEntry 1 }

cabhCdpWanDataAddrClientId OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (1..80))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "A unique WAN-Data ClientID used when attempting
            to acquire a WAN-Data IP Address via DHCP."
    ::= { cabhCdpWanDataAddrEntry 2 }

cabhCdpWanDataAddrIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The address type assigned on the WAN-Data side."
    DEFVAL { ipv4 }
```

```
    ::= { cabhCdpWanDataAddrEntry 3 }

cabhCdpWanDataAddrIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The address assigned on the WAN-Data side."
    ::= { cabhCdpWanDataAddrEntry 4 }

cabhCdpWanDataAddrRenewalTime OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
            "This is the time remaining before the lease expires.
            This is based on DHCP Option 51."
    ::= { cabhCdpWanDataAddrEntry 5 }

cabhCdpWanDataAddrRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The RowStatus interlock for creation and deletion of row
            entries.  Any writable object in a row can be modified at
            any time while the row is active(1).  The PS must assign a
            RowStatus of notInService(2) to any new row entry created
            with a cabhCdpWanDataAddrClientId that is not unique within
            this table."
    ::= { cabhCdpWanDataAddrEntry 6 }

cabhCdpWanDataAddrLeaseCreateTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This is the date and time when the WAN-Data address lease
            was created (if it has not yet been renewed) or last
            renewed."
    ::= { cabhCdpWanDataAddrEntry 7 }

cabhCdpWanDataAddrLeaseExpireTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This is the date and time when the WAN-Data address
             lease expired or will expire."
    ::= { cabhCdpWanDataAddrEntry 8 }

--------------------------------------------------------------------
--
-- cabhCdpWanDnsServerTable (CDP WAN DNS Server Table)
--
-- The cabhCdpWanDnsServerTable is a table of 3 cable network
-- and Internet DNS Servers.
--
--------------------------------------------------------------------
cabhCdpWanDnsServerTable OBJECT-TYPE
    SYNTAX SEQUENCE OF CabhCdpWanDnsServerEntry
    MAX-ACCESS not-accessible
    STATUS current
```

```
    DESCRIPTION
            "This table contains the IP addresses of cable network and
            Internet DNS servers, in the order of preference in which
            the PS's CNP will query them, when it cannot resolve a DNS
            query using local information. Entries in this table are
            updated with the information contained in DHCP option 6,
            received during both the WAN-Man and WAN-Data IP
            acquisition processes."
    ::= { cabhCdpAddr 3 }

cabhCdpWanDnsServerEntry OBJECT-TYPE
    SYNTAX      CabhCdpWanDnsServerEntry
    MAX-ACCESS  not-accessible
    STATUS     current
    DESCRIPTION
            "List of cable network and Internet DNS servers."
    INDEX { cabhCdpWanDnsServerOrder }
    ::= { cabhCdpWanDnsServerTable 1 }

CabhCdpWanDnsServerEntry ::= SEQUENCE {
    cabhCdpWanDnsServerOrder  INTEGER,
    cabhCdpWanDnsServerIpType InetAddressType,
    cabhCdpWanDnsServerIp     InetAddress
    }

cabhCdpWanDnsServerOrder OBJECT-TYPE
    SYNTAX      INTEGER {
                    primary(1),
                    secondary(2),
                    tertiary(3)
                }
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The order of preference for cable network and Internet DNS
            servers, as listed in DHCP option 6 (Domain Server). Any
            time the CDC receives valid IP address information within
            DHCP option 6, as part of lease acquisition or renewal of
            a WAN-Man or WAN-Data IP, it must update this information
            into this table.  As entries in DHCP option 6 are listed in
            order of preference, the highest priority entry in DHCP
            option 6 must correspond to the row with a
            cabhCdpWanDnsServerOrder with a value of 1. If DHCP
            option 6 contains 1 valid IP address, the PS MUST update
            the row with a cabhCdpWanDnsServerOrder value of 1 and
            MUST NOT modify rows with
            cabhCdpWanDnsServerOrder values of 2 & 3
            (if they exist). If DHCP option 6 contains 2 valid
            IP addresses, the PS MUST update the rows with
            cabhCdpWanDnsServerOrder values of 1 and 2
            and MUST NOT modify the row with cabhCdpWanDnsServerOrder
            value of 3 (if it exists). If DHCP option 6 contains 3
            valid IP addresses, the PS MUST update rows with
            cabhCdpWanDnsServerOrder values of 1, 2, and 3.
            Any DNS server information included in DHCP option 6
            beyond primary, secondary and tertiary will not be
            represented in this table."
    ::= { cabhCdpWanDnsServerEntry 1 }

cabhCdpWanDnsServerIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS read-only
    STATUS current
```

```
    DESCRIPTION
            "This parameter indicates the IP address type of a
            WAN DNS server."
    DEFVAL { ipv4 }
    ::= { cabhCdpWanDnsServerEntry 2 }

cabhCdpWanDnsServerIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This parameter indicates the IP address of a WAN DNS
            server. The type of this address is specified by
            cabhCdpWanDnsServerIpType."
    ::= { cabhCdpWanDnsServerEntry 3 }

--
--    DHCP Server Side (CDS) Option Values for the LAN-Trans realm
--

cabhCdpLanPoolStartType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Address type of the start of range LAN Trans IP
            Addresses."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 1 }

cabhCdpLanPoolStart OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The start of range LAN Trans IP Addresses. The type of
            this address is specified by cabhCdpLanPoolStartType."
    DEFVAL { 'c0a8000a'h }    -- 192.168.0.10
    -- 192.168.0.0 is the network number
    -- 192.168.0.255 is broadcast
    -- address and 192.168.0.1
    -- is reserved for the router
    ::= { cabhCdpServer 2 }

cabhCdpLanPoolEndType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Address type of the end of range LAN Trans IP
            Addresses."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 3 }

cabhCdpLanPoolEnd OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The end of range for LAN-Trans IP Addresses. The type of
            this address is specified by cabhCdpLanPoolEndType."
    DEFVAL { 'c0a800fe'h }    -- 192.168.0.254
    ::= { cabhCdpServer 4 }
```

```
cabhCdpServerNetworkNumberType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP address type of the LAN-Trans network number."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 5 }

cabhCdpServerNetworkNumber OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The LAN-Trans network number. The type of this address is
            specified by cabhCdpServerNetworkNumberType."
    DEFVAL { 'c0a80000'h } --192.168.0.0
    ::= { cabhCdpServer 6 }

cabhCdpServerSubnetMaskType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Type of LAN-Trans Subnet Mask."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 7 }

cabhCdpServerSubnetMask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PS MUST provide the value of this MIB
            object in option 1 (Subnet Mask) of
            DHCP OFFER and ACK messages sent to a LAN IP Device."
    DEFVAL { 'ffffff00'h }    -- 255.255.255.0
    ::= { cabhCdpServer 8 }

cabhCdpServerTimeOffset OBJECT-TYPE
    SYNTAX      Integer32 (-86400..86400) -- 0 to 24 hours (in seconds)
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PS MUST provide the value of this MIB object in
            option 2 (Time Offset from Coordinated
            Universal Time-UTC) in the DHCP OFFER and ACK
            messages sent to the LAN IP Device."
    DEFVAL { 0 }    -- UTC
    ::= { cabhCdpServer 9 }

cabhCdpServerRouterType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Type of Address, Router for the LAN-Trans
            address realm."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 10 }

cabhCdpServerRouter OBJECT-TYPE
    SYNTAX      InetAddress
```

```
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The type of this address is specified by
            cabhCdpServerRouterType. The PS MUST
            provide the value of this MIB object in
            option 3 (Router IP address) of the DHCP
            OFFER and ACK messages sent to the LAN IP Device."
    DEFVAL { 'c0a80001'h }    -- 192.168.0.1
    ::= { cabhCdpServer 11 }

cabhCdpServerDnsAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Type of IP Addresses of the LAN-Trans address realm
            DNS servers."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 12 }

cabhCdpServerDnsAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The default value of this MIB object is the
            same as the value of the cabhCdpServerRouter
            object. The NMS may set the value of this
            object to a value different than the value
            of cabhCdpServerRouter (e.g., DNS server in the
            cable data network) so that a LAN IP Device can direct its
            DNS queries to a server other than the PS DNS
            server. The type of this address is specified
            by cabhCdpServerDnsAddressType. The PS MUST
            provide the value of this MIB object in option 6
            (Domain Name Server) of DHCP OFFER and ACK
            messages sent to a LAN IP Device."
    ::= { cabhCdpServer 13 }

cabhCdpServerSyslogAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Type of IP Address of the LAN-Trans SYSLOG servers."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 14 }

cabhCdpServerSyslogAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "If the value of this object is non-zero, the PS will
            include the value of this object in DHCP option 7
            (Log Servers) in DHCP OFFER and DHCP ACK messages
            sent to the LAN IP Device."
    DEFVAL { '00000000'h }    -- 0.0.0.0
    ::= { cabhCdpServer 15 }

cabhCdpServerDomainName OBJECT-TYPE
    SYNTAX      SnmpAdminString(SIZE(0..128))
    MAX-ACCESS  read-write
```

```
    STATUS      current
    DESCRIPTION
            "The PS MUST provide the value of this MIB object
            in option 15 (Domain Name Option) of the DHCP
            OFFER and ACK messages sent to the LAN IP Device."
    DEFVAL { "" }
    ::= { cabhCdpServer 16 }

cabhCdpServerTTL OBJECT-TYPE
    SYNTAX      INTEGER (1..255)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PS MUST provide the value of this MIB
             object in option 23 (Default IP TTL) of
             DHCP OFFER and ACK messages sent to a LAN IP Device."
    DEFVAL { 64 }
    ::= { cabhCdpServer 17 }

cabhCdpServerInterfaceMTU OBJECT-TYPE
    SYNTAX      Integer32 (0 | 68..4096)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PS MUST provide the value of this MIB object in
            option 26 (Interface MTU Option) of the DHCP OFFER
            and ACK messages sent to the LAN IP Device. If the value
            of this object is 0, the PS must not include this option
            in its DHCP OFFER or DHCP ACK messages to LAN IP Devices."
    DEFVAL { 0 }
    ::= { cabhCdpServer 18 }

cabhCdpServerVendorSpecific OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..255))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PS MUST provide the value of this MIB object in
            option 43 (Vendor Specific Information) of the DHCP OFFER
            and ACK messages sent to the LAN IP Device. If the value of
            this object is ' 'h,  then the PS MUST NOT include this
            option in its DHCP OFFER or DHCP ACK messages to LAN IP
            Devices."
    DEFVAL { ''h }
    ::= { cabhCdpServer 19 }

cabhCdpServerLeaseTime OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PS MUST provide the value of this MIB object in
            option 51 (IP Address lease time) of the DHCP OFFER and
            ACK messages sent to the LAN IP Device."
    DEFVAL { 3600 }
    ::= { cabhCdpServer 20 }

cabhCdpServerDhcpAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Type of LAN DHCP server IP address. The
```

```
            IP address of LAN DHCP server is provided by
            the PS in option 54 of DHCP OFFER or ACK."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 21 }

cabhCdpServerDhcpAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of this MIB object is always the
            same as the value of the cabhCdpServerRouter
            object. The type of this address is specified
            by cabhCdpServerDhcpAddressType.
            The PS MUST provide the value of this MIB
            object in option 54 (DHCP server identifier)
            field of DHCP OFFER and ACK messages
            sent to a LAN IP device."
    ::= { cabhCdpServer 22 }


cabhCdpServerControl OBJECT-TYPE
    SYNTAX      INTEGER {
                    restoreConfig(1),
                    commitConfig(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The control for the CDS (DHCP Server) configuration.
            All changes to the cabhCdpServer MIB objects are reflected
            when reading the value of the MIB objects; however, those
            changes are NOT applied to the running configuration of
            the CDS until they are successfully committed via use
            of the cabhCdpServerControl object.

            If changes are made to the cabhCdpServer MIB objects which
            are not yet successfully committed to the CDS, the
            cabhCdpServerControl object can be used to roll back all
            changes to the last valid CDS configuration and discard
            all intermediate changes.

            restoreConfig - Setting cabhCdpServerControl to this value
            will cause any changes to the cabhCdpServer objects not yet
            committed be reset to the values from the current running
            configuration of the CDS.

            commitConfig - Setting cabhCdpServerControl to this value
            will cause the CDS to validate and apply the valid
            cabhCdpServer MIB settings to its running configuration.
            The cabhCdpServerCommitStatus object will detail the
            status of this operation."
    DEFVAL { restoreConfig }
    ::= { cabhCdpServer 23 }

cabhCdpServerCommitStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                    commitSucceeded(1),
                    commitNeeded(2),
                    commitFailed(3)
                }
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "Indicates the status of committing the current
            cabhCdpServer MIB object values to the running
            configuration of the CDS (DHCP Server).

            commitSucceeded - indicates the current cabhCdpServer
            MIB object values are valid and have been successfully
            committed to the running configuration of the CDS.

            commitNeeded - indicates that the value of one or more
            objects in cabhCdpServer MIB group have been changed
            but not yet committed to the running configuration
            of the CDS.

            commitFailed - indicates the PS was unable to commit the
            cabhCdpServer MIB object values to the running
            configuration of the CDS due to conflicts in those
            values."
    DEFVAL { commitSucceeded }
    ::= { cabhCdpServer 24 }

cabhCdpServerUseCableDataNwDnsAddr OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "If the value of this object is false(2), the PS will
            provide the DNS Server IP address as specified in
            cabhCdpServerDnsAddress MIB object in option 6
            (Domain Name Server) of the DHCP OFFER and ACK messages
            sent to a LAN IP Device.

            When the object cabhCdpServerUseCableDataNwDnsAddr is set
            to true(1), the PS must take the following actions:
            The PS will provide in option 6 (Domain Name Server), of
            the DHCP OFFER and ACK messages sent to a LAN IP Device,
            the DNS server address(es) which is/are being used by the
            PS itself, i.e., the DNS server address(es) provided to the
            PS in DHCP option 6 and made available through PS MIB
            object cabhCdpWanDnsServerIp.

            The LAN IP Device can then direct its DNS queries to a
            server other than the PS DNS server. The PS MUST provide
            the value of this."
    DEFVAL { false }
    ::= { cabhCdpServer 25 }

--
-- notification group is for future extension.
--

cabhCdpNotification OBJECT IDENTIFIER ::= { cabhCdpMib 2 }
cabhCdpNotifications OBJECT IDENTIFIER ::= { cabhCdpNotification 0 }
cabhCdpConformance  OBJECT IDENTIFIER ::= { cabhCdpMib 3 }
cabhCdpCompliances  OBJECT IDENTIFIER ::= { cabhCdpConformance 1 }
cabhCdpGroups       OBJECT IDENTIFIER ::= { cabhCdpConformance 2 }

--
--    Notification Group
--


-- compliance statements
```

```
cabhCdpBasicCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for devices that implement
            the CableHome Portal Services functionality."
    MODULE   --cabhCdpMib


-- unconditionally mandatory groups

MANDATORY-GROUPS {
    cabhCdpGroup
    }

    ::= { cabhCdpCompliances 3 }

cabhCdpGroup OBJECT-GROUP
    OBJECTS {
    cabhCdpSetToFactory,
    cabhCdpLanTransCurCount,
    cabhCdpLanTransThreshold,
    cabhCdpLanTransAction,
    cabhCdpWanDataIpAddrCount,
    cabhCdpLastSetToFactory,
    cabhCdpTimeOffsetSelection,
    cabhCdpSnmpSetTimeOffset,
    cabhCdpDaylightSavingTimeEnable,

    cabhCdpLanAddrClientID,
    cabhCdpLanAddrLeaseCreateTime,
    cabhCdpLanAddrLeaseExpireTime,
    cabhCdpLanAddrMethod,
    cabhCdpLanAddrHostName,
    cabhCdpLanAddrRowStatus,

    cabhCdpWanDataAddrClientId,
    cabhCdpWanDataAddrIpType,
    cabhCdpWanDataAddrIp,
    -- cabhCdpWanDataAddrRenewalTime,
    cabhCdpWanDataAddrRowStatus,
    cabhCdpWanDataAddrLeaseCreateTime,
    cabhCdpWanDataAddrLeaseExpireTime,

    cabhCdpWanDnsServerIpType,
    cabhCdpWanDnsServerIp,

    cabhCdpLanPoolStartType,
    cabhCdpLanPoolStart,
    cabhCdpLanPoolEndType,
    cabhCdpLanPoolEnd,
    cabhCdpServerNetworkNumberType,
    cabhCdpServerNetworkNumber,
    cabhCdpServerSubnetMaskType,
    cabhCdpServerSubnetMask,
    cabhCdpServerTimeOffset,
    cabhCdpServerRouterType,
    cabhCdpServerRouter,
    cabhCdpServerDnsAddressType,
    cabhCdpServerDnsAddress,
    cabhCdpServerSyslogAddressType,
    cabhCdpServerSyslogAddress,
    cabhCdpServerDomainName,
    cabhCdpServerTTL,
    cabhCdpServerInterfaceMTU,
```

```
    cabhCdpServerVendorSpecific,
    cabhCdpServerLeaseTime,
    cabhCdpServerDhcpAddressType,
    cabhCdpServerDhcpAddress,
    cabhCdpServerControl,
    cabhCdpServerCommitStatus,
    cabhCdpServerUseCableDataNwDnsAddr
    }
    STATUS      current
    DESCRIPTION
            "Group of objects for CableHome CDP MIB."
    ::= { cabhCdpGroups 1 }

END
```

E.3 IPCable2Home Test Portal (CTP) MIB requirement

The IPCable2Home CTP MIB MUST be implemented as defined below:

```
CABH-CTP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE           FROM SNMPv2-SMI
    TimeStamp,
    TruthValue            FROM SNMPv2-TC
    OBJECT-GROUP,
    MODULE-COMPLIANCE     FROM SNMPv2-CONF
    InetAddressType,
    InetAddress           FROM INET-ADDRESS-MIB
    clabProjCableHome     FROM CLAB-DEF-MIB;

cabhCtpMib MODULE-IDENTITY
    LAST-UPDATED  "200404090000Z" -- April 9, 2004
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
            858 Coal Creek Circle
            Louisville, Colorado 80027
            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com or mibs@cablelabs.com"
    DESCRIPTION
            "This MIB module defines control and monitoring objects
            for remote diagnostic tools for a CableHome LAN
            supported by the CableHome Test Portal (CTP) as
            defined and described in CableLabs' CableHome
            specifications."
    ::=  { clabProjCableHome 5 }

-- Textual conventions


cabhCtpObjects          OBJECT IDENTIFIER ::= { cabhCtpMib 1 }
cabhCtpBase             OBJECT IDENTIFIER ::= { cabhCtpObjects 1 }
cabhCtpConnSpeed        OBJECT IDENTIFIER ::= { cabhCtpObjects 2 }
cabhCtpPing             OBJECT IDENTIFIER ::= { cabhCtpObjects 3 }

--
--    The following group describes the base objects in the CableHome
--    Management Portal.
--
```

```
cabhCtpSetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Setting this object to true(1) causes all the tables
            in the CTP MIB to be cleared, and all CTP MIB objects
            with default values set back to those default values.
            Reading this object always returns false(2)."
    ::={ cabhCtpBase 1 }

cabhCtpLastSetToFactory OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when cabhCtpSetToFactory
            was last set to true. Zero if never reset."
    ::={ cabhCtpBase 2 }

--
--    Parameter and results from Connection Speed Command
--

cabhCtpConnSrcIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP Address type used as the source address for the
            Connection Speed Test.
            The PS MUST NOT allow the value of cabhCtpConnSrcIpType
            to be changed if cabhCtpConnStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpConnSrcIpType when the
            value of cabhCtpConnStatus is running(2)."
    DEFVAL { ipv4 }
    ::= { cabhCtpConnSpeed 1 }

cabhCtpConnSrcIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP Address used as the source address for the
            Connection Speed Test. The default value is the value
            of cabhCdpServerRouter (192.168.0.1). The type of
            this address is specified by cabhCtpConnSrcIpType.
            The PS MUST NOT allow the value of cabhCtpConnSrcIp
            to be changed if cabhCtpConnStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpConnSrcIp when the
            value of cabhCtpConnStatus is running(2)."
    REFERENCE
            "CableHome Specification, Management Tools - PS
            Logical Element CableHome Test Portal (CTP) section."
    DEFVAL { 'c0a80001'h }    -- 192.168.0.1
    ::= { cabhCtpConnSpeed 2 }

cabhCtpConnDestIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
```

```
    DESCRIPTION
            "The IP Address Type for the CTP Connection Speed Tool
            destination address.
            The PS MUST NOT allow the value of cabhCtpConnDestIpType
            to be changed if cabhCtpConnStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpConnDestIpType when the
            value of cabhCtpConnStatus is running(2)."
    DEFVAL { ipv4 }
    ::={ cabhCtpConnSpeed 3 }

cabhCtpConnDestIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP Address used as the destination address for the
            Connection Speed Test. The type of this address is
            specified by cabhCtpConnDestIpType. The PS MUST NOT allow
            the value of cabhCtpConnDestIp to be changed if
            cabhCtpConnStatus = running(2). The PS MUST return
            inconsistentValue error to a manager that attempts
            to set the value of cabhCtpConnDestIp when the value of
            cabhCtpConnStatus is running(2)."
    ::= { cabhCtpConnSpeed 4 }

cabhCtpConnProto OBJECT-TYPE
    SYNTAX      INTEGER {
                    udp(1),
                    tcp(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The protocol used in the Connection Speed Test. TCP
            testing is optional.
            The PS MUST NOT allow the value of cabhCtpConnProto
            to be changed if cabhCtpConnStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpConnProto when the
            value of cabhCtpConnStatus is running(2)."
    DEFVAL { udp }
    ::= { cabhCtpConnSpeed 5 }

cabhCtpConnNumPkts OBJECT-TYPE
    SYNTAX      INTEGER (1..65535)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The number of OSI Layer 3 (IP) packets the CTP is to
            send when triggered to execute the Connection Speed Tool.
            The PS MUST NOT allow the value of cabhCtpConnNumPkts
            to be changed if cabhCtpConnStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpConnNumPkts when the
            value of cabhCtpConnStatus is running(2)."
    DEFVAL { 100 }
    ::= { cabhCtpConnSpeed 6 }

cabhCtpConnPktSize OBJECT-TYPE
    SYNTAX      INTEGER (64..1518)
    MAX-ACCESS  read-write
    STATUS      current
```

```
    DESCRIPTION
            "The size of each OSI Layer 2 frame to be
            sent by the PS CableHome Test Portal
            function when configured to execute the
            Connection Speed remote diagnostic tool.
            The PS MUST NOT allow the value of cabhCtpConnPktSize
            to be changed if cabhCtpConnStatus = running(2).
            The PS MUST return inconsistentValue error
            to a manager that attempts to set the value of
            cabhCtpConnPktSize when the value of cabhCtpConnStatus
            is running(2)."
    REFERENCE
            "CableHome Specification, Management Tools - PS
            Logical Element CableHome Test Portal (CTP) section."
    DEFVAL { 1518 }
    ::= { cabhCtpConnSpeed 7 }

cabhCtpConnTimeOut OBJECT-TYPE
    SYNTAX      INTEGER (0..600000)           -- Max 10 minutes
    UNITS       "milliseconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The timeout value for the response.  A value of zero
            indicates no time out and can be used for TCP only.
            The PS MUST NOT allow the value of cabhCtpConnTimeOut
            to be changed if cabhCtpConnStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpConnTimeOut when the
            value of cabhCtpConnStatus is running(2)."
    DEFVAL {30000}  -- 30 seconds
    ::= { cabhCtpConnSpeed 8 }

cabhCtpConnControl OBJECT-TYPE
    SYNTAX      INTEGER {
                    start(1),
                    abort(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The control for the Connection Speed Tool. Setting this
            object to start(1) causes the Connection Speed Tool to
            execute. Setting this object to abort(2) causes the
            Connection Speed Tool to stop running. This parameter
            should only be set via SNMP."
    DEFVAL  {abort }
    ::={ cabhCtpConnSpeed 9 }

cabhCtpConnStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                    notRun(1),
                    running(2),
                    complete(3),
                    aborted(4),
                    timedOut(5)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object returns the status of the Connection Speed
            Tool. The value notRun(1) indicates that the Connection
            Speed Tool has not been run since the Portal Services
            element of the CableHome residential gateway was
```

```
            initialized or reset.

            The value running(2) indicates that the Connection Speed
            Tool was initiated by a manager
            (cabhCtpConnControl = start(1)) and the test has not
            timed out and the PS has not yet completed sending
            all the packets it was configured to send or it has not
            received all responses.

            The value complete(3) indicates that the Connection Speed
            Tool was initiated by a manager, successfully sent all the
            packets it was configured to send, received all responses,
            and is no longer sending packets or waiting for responses.

            The value aborted(4) indicates that the Connection Speed
            Tool was initiated by a manager then was terminated by the
            manager by setting cabhCtpConnControl = abort(2).
            The Connection Speed Tool is no longer sending packets or
            waiting for responses.

            The value timedOut(5) indicates that the Connection Speed
            Tool was initiated by a manager and had not received all
            responses from the client but the amount of time allowed
            for the Connection Speed Tool to execute, defined by the
            value of cabhCtpConnTimeOut, has transpired. The Connection
            Speed Tool is no longer sending packets or waiting
            for responses."
    DEFVAL { notRun }
    ::={ cabhCtpConnSpeed 10 }

cabhCtpConnPktsSent OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of packets the CTP sent after it was
            triggered to execute the Connection Speed Tool."
    ::= { cabhCtpConnSpeed 11 }

cabhCtpConnPktsRecv OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of packets the CTP received after it
            executed the Connection Speed Tool."
    ::= { cabhCtpConnSpeed 12 }

cabhCtpConnRTT OBJECT-TYPE
    SYNTAX      INTEGER (0..600000)
    UNITS       "millisec"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The resulting round trip time for the set of
            packets sent to and received from the target
            LAN IP Device."
    ::= { cabhCtpConnSpeed 13 }

cabhCtpConnThroughput OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "The average round-trip throughput measured in
            kilobits per second."
    ::= { cabhCtpConnSpeed 14 }

--
--    Parameters and Results for Ping Command
--

cabhCtpPingSrcIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP Address Type for CTP Ping Tool source address.
            The PS MUST NOT allow the value of cabhCtpPingSrcIpType
            to be changed if cabhCtpPingStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpPingSrcIpType when the
            value of cabhCtpPingStatus is running(2)."
    DEFVAL { ipv4 }
    ::={ cabhCtpPing 1 }

cabhCtpPingSrcIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP Address used as the source address for the Ping
            Test. The default value is the value of
            CabhCdpServerRouter (192.168.0.1). The type of this
            address is specified by cabhCtpPingSrcIpType.
            The PS MUST NOT allow the value of cabhCtpPingSrcIp
            to be changed if cabhCtpPingTimeOut = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpPingSrcIp when the
            value of cabhCtpPingTimeOut is running(2)."
    REFERENCE
            "CableHome Specification, Management Tools - PS
            Logical Element CableHome Test Portal (CTP) section."
    DEFVAL { 'c0a80001'h } --192.168.0.1
    ::= { cabhCtpPing 2 }

cabhCtpPingDestIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP Address Type for the CTP Ping Tool destination
            address.
            The PS MUST NOT allow the value of cabhCtpPingDestIpType
            to be changed if cabhCtpPingStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpPingDestIpType when the
            value of cabhCtpPingStatus is running(2)."
    DEFVAL { ipv4 }
    ::={ cabhCtpPing 3 }

cabhCtpPingDestIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
```

```
    DESCRIPTION
            "The Destination IP Address used as the destination
            address for the Ping Test. The type of this address
            is specified by cabhCtpPingDestIpType. The PS MUST NOT
            allow the value of cabhCtpPingDestIp to be changed if
            cabhCtpPingStatus = running(2). The PS MUST return
            inconsistentValue error to a manager that attempts
            to set the value of cabhCtpPingDestIp when the value of
            cabhCtpPingStatus is running(2)."
    ::= { cabhCtpPing 4 }

cabhCtpPingNumPkts OBJECT-TYPE
    SYNTAX      INTEGER (1..4)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The number of ICMP Echo Request messages to send to
            the destination defined by cabhCtpPingDestIp. The PS
            MUST NOT allow the value of cabhCtpPingNumPkts to be
            changed if cabhCtpPingStatus = running(2).  The PS MUST
            return inconsistentValue error to a manager that attempts
            to set the value of cabhCtpPingNumPkts when the value of
            cabhCtpPingStatus is running(2)."
    DEFVAL { 1 }
    ::= { cabhCtpPing 5 }

cabhCtpPingPktSize OBJECT-TYPE
    SYNTAX      INTEGER (64..1518)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The size of the ICMP Echo Request packets to send to
            the destination defined by cabhCtpPingDestIp. The PS
            MUST NOT allow the value of cabhCtpPingPktSize to be
            changed if cabhCtpPingStatus = running(2).  The PS MUST
            return inconsistentValue error to a manager that attempts
            to set the value of cabhCtpPingPktSize when the value of
            cabhCtpPingStatus is running(2)."
    DEFVAL { 64 }
    ::= { cabhCtpPing 6 }

cabhCtpPingTimeBetween OBJECT-TYPE
    SYNTAX      INTEGER (0..600000)
    UNITS       "milliseconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The time between sending one ping and the next.
            The PS MUST NOT allow the value of cabhCtpPingTimeBetween
            to be changed if the value of cabhCtpPingStatus is
            running(2).  The PS MUST return inconsistentValue error
            to a manager that attempts to set the value of
            cabhCtpPingTimeBetween when the value of
            cabhCtpPingStatus is running(2)."
    DEFVAL { 1000 }
    ::= { cabhCtpPing 7 }

cabhCtpPingTimeOut OBJECT-TYPE
    SYNTAX      INTEGER (1..600000)
    UNITS       "milliseconds"
    MAX-ACCESS  read-write
    STATUS      current
```

```
    DESCRIPTION
            "The time out for ping response (ICMP reply) for a
            single transmitted ping message (ICMP request).
            The PS MUST NOT allow the value of cabhCtpPingTimeOut
            to be changed if cabhCtpPingStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpPingTimeOut when the
            value of cabhCtpPingStatus is running(2)."
    DEFVAL { 1000 } -- 1 second
    ::={ cabhCtpPing 8 }

cabhCtpPingControl OBJECT-TYPE
    SYNTAX      INTEGER {
                    start(1),
                    abort(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The control for the Ping Tool. Setting this object
            to start(1) causes the Ping Tool to execute. Setting
            this object to abort(2) causes the Ping Tool to stop
            running. This parameter should only be set via SNMP."
    DEFVAL {abort }
    ::={ cabhCtpPing 9 }

cabhCtpPingStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                    notRun(1),
                    running(2),
                    complete(3),
                    aborted(4),
                    timedOut(5)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object returns the status of the Ping Tool.

            The value notRun(1) indicates that the Ping Tool
            has not been run since the Portal Services element of the
            CableHome residential gateway was initialized or reset.

            The value running(2) indicates that the Ping Tool
            was initiated by a manager (cabhCtpPingControl = start(1))
            and the test has not timed out and the PS has not yet
            completed sending all the packets it was configured to
            send or it has not received all responses.

            The value complete(3) indicates that the Ping Tool
            was initiated by a manager, successfully sent all the
            packets it was configured to send, received all responses,
            and is no longer sending packets or waiting for responses.

            The value aborted(4) indicates that the Ping Tool was
            initiated by a manager then was terminated by the manager
            by setting cabhCtpPingControl = abort(2). The Ping Tool
            is no longer sending packets or waiting for responses.

            The value timedOut(5) indicates that the Ping Tool was
            initiated by a manager and had not received all responses
            from the client but the amount of time allowed for the
            Ping Tool to execute, defined by the value of
            cabhCtpPingTimeOut, has transpired. The Ping Tool is no
```

```
            longer sending packets or waiting for responses."
    DEFVAL { notRun }
    ::={ cabhCtpPing 10 }

cabhCtpPingNumSent OBJECT-TYPE
    SYNTAX      INTEGER (0..4)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of Pings sent."
    ::={ cabhCtpPing 11 }

cabhCtpPingNumRecv OBJECT-TYPE
    SYNTAX      INTEGER (0..255)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of pings received."
    ::= { cabhCtpPing 12 }

cabhCtpPingAvgRTT OBJECT-TYPE
    SYNTAX      INTEGER (0..600000)
    UNITS       "millisec"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The resulting average of round trip times for
            acknowledged packets."
    ::= { cabhCtpPing 13 }

cabhCtpPingMaxRTT OBJECT-TYPE
    SYNTAX      INTEGER (0..600000)
    UNITS       "millisec"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The resulting maximum of round trip times for
            acknowledged packets."
    ::= { cabhCtpPing 14 }

cabhCtpPingMinRTT OBJECT-TYPE
    SYNTAX      INTEGER (0..600000)
    UNITS       "millisec"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The resulting minimum of round trip times for
            acknowledged packets."
    ::= { cabhCtpPing 15 }

cabhCtpPingNumIcmpError OBJECT-TYPE
    SYNTAX      INTEGER (0..255)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Number of ICMP errors."
    ::= { cabhCtpPing 16 }

cabhCtpPingIcmpError OBJECT-TYPE
    SYNTAX      INTEGER (0..255)
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "The last ICMP error."
    ::= { cabhCtpPing 17 }

--=================================================================

--
-- notification group is for future extension.
--

cabhCtpNotification  OBJECT IDENTIFIER ::= { cabhCtpMib 2 }
cabhCtpNotifications OBJECT IDENTIFIER ::= { cabhCtpNotification 0 }
cabhCtpConformance   OBJECT IDENTIFIER ::= { cabhCtpMib 3 }
cabhCtpCompliances   OBJECT IDENTIFIER ::= { cabhCtpConformance 1 }
cabhCtpGroups        OBJECT IDENTIFIER ::= { cabhCtpConformance 2 }

--
--    Notification Group
--

-- compliance statements

cabhCtpBasicCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for devices that implement
            Portal Service feature."
    MODULE   --cabhCtpMib


-- unconditionally mandatory groups

    MANDATORY-GROUPS {
          cabhCtpGroup
    }

    ::= { cabhCtpCompliances 3 }


cabhCtpGroup OBJECT-GROUP
    OBJECTS {

        cabhCtpSetToFactory,
        cabhCtpLastSetToFactory,
        cabhCtpConnSrcIpType,
        cabhCtpConnSrcIp,
        cabhCtpConnDestIpType,
        cabhCtpConnDestIp,
        cabhCtpConnProto,
        cabhCtpConnNumPkts,
        cabhCtpConnPktSize,
        cabhCtpConnTimeOut,
        cabhCtpConnControl,
        cabhCtpConnStatus,
        cabhCtpConnPktsSent,
        cabhCtpConnPktsRecv,
        cabhCtpConnRTT,
        cabhCtpConnThroughput,

        cabhCtpPingSrcIpType,
        cabhCtpPingSrcIp,
        cabhCtpPingDestIpType,
        cabhCtpPingDestIp,
        cabhCtpPingNumPkts,
```

```
        cabhCtpPingPktSize,
        cabhCtpPingTimeBetween,
        cabhCtpPingTimeOut,
        cabhCtpPingControl,
        cabhCtpPingStatus,
        cabhCtpPingNumSent,
        cabhCtpPingNumRecv,
        cabhCtpPingAvgRTT,
        cabhCtpPingMinRTT,
        cabhCtpPingMaxRTT,
        cabhCtpPingNumIcmpError,
        cabhCtpPingIcmpError
        }
    STATUS      current
    DESCRIPTION
            "Group of objects for CableHome CTP MIB."
    ::= { cabhCtpGroups 1 }

END
```

E.4 IPCable2Home Portal Services Device (PSDev) MIB requirement

The IPCable2Home PSDev MIB MUST be implemented as defined below.

```
CABH-PS-DEV-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Integer32,
    Unsigned32,
    TimeTicks,
    NOTIFICATION-TYPE            FROM SNMPv2-SMI

    TruthValue,
    PhysAddress,
    DateAndTime,
    TimeStamp,
    RowStatus                    FROM SNMPv2-TC

    SnmpAdminString              FROM SNMP-FRAMEWORK-MIB

    OBJECT-GROUP,
    MODULE-COMPLIANCE,
    NOTIFICATION-GROUP           FROM SNMPv2-CONF

    ifIndex                      FROM IF-MIB

    InetAddressType,
    InetAddress                  FROM INET-ADDRESS-MIB

    IANAifType                   FROM IANAifType-MIB

    docsDevSwCurrentVers,
    docsDevEvLevel,
    docsDevEvId,
    docsDevEvText,
    docsDevSwFilename,
    docsDevSwServer              FROM DOCS-CABLE-DEVICE-MIB -- RFC 2669

    cabhCdpServerDhcpAddress,
    cabhCdpWanDataAddrClientId,
    cabhCdpLanTransThreshold,
```

```
    cabhCdpLanTransCurCount      FROM CABH-CDP-MIB

    ZeroBasedCounter32           FROM RMON2-MIB

    cabhQos2NumActivePolicyHolder,
    cabhQos2PolicyHolderEnabled,
    cabhQos2PolicyAdmissionControl FROM CABH-QOS2-MIB

    clabProjCableHome            FROM CLAB-DEF-MIB;

cabhPsDevMib MODULE-IDENTITY
    LAST-UPDATED    "200504080000Z" -- April 8, 2005
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
            858 Coal Creek Circle
            Louisville, Colorado 80027
            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com; mibs@cablelabs.com"
    DESCRIPTION
            "This MIB module supplies the basic management objects for
            the Portal Services logical element of a CableHome
            compliant Residential Gateway device. The PS device
            parameters describe general PS Device attributes and
            behaviour characteristics.
            Most the PS Device MIB is needed for configuration
            download."
    ::= { clabProjCableHome 1 }

-- Textual Conventions

cabhPsDevMibObjects     OBJECT IDENTIFIER ::= { cabhPsDevMib 1 }
cabhPsDevBase           OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 1 }
cabhPsDevProv           OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 2 }
cabhPsDevAttrib         OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 3 }
cabhPsDevPsAttrib       OBJECT IDENTIFIER ::= { cabhPsDevAttrib 1 }
cabhPsDevBpAttrib       OBJECT IDENTIFIER ::= { cabhPsDevAttrib 2 }
cabhPsDevStats          OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 4 }
cabhPsDevAccessControl  OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 5 }
cabhPsDevMisc           OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 6 }
cabhPsDevUI             OBJECT IDENTIFIER ::= { cabhPsDevMisc 1 }
cabhPsDev802dot11       OBJECT IDENTIFIER ::= { cabhPsDevMisc 2 }
cabhPsDevUpnp           OBJECT IDENTIFIER ::= { cabhPsDevMisc 3 }
cabhPsDevUpnpBase       OBJECT IDENTIFIER ::= { cabhPsDevUpnp 1 }
cabhPsDevUpnpCommands   OBJECT IDENTIFIER ::= { cabhPsDevUpnp 2 }

--
-- The following group describes the base objects in the PS.
-- These are device-based parameters.
--

cabhPsDevDateTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The date and time, with optional timezone information."
    ::= { cabhPsDevBase 1 }

cabhPsDevResetNow OBJECT-TYPE
    SYNTAX      TruthValue
```

```
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Setting this object to true(1) causes the standalone or
            embedded PS device to reboot. Device code initializes as if
            starting from a power-on reset. The CMP ensures that MIB
            object values persist as specified in Annex A. Reading this
            object always returns false(2)."
    ::= { cabhPsDevBase 2 }

cabhPsDevSerialNumber OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..128))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The manufacturer's serial number for this PS. This
            parameter is manufacturer provided and is stored in
            non-volatile memory."
    ::= { cabhPsDevBase 3 }

cabhPsDevHardwareVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..48))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The manufacturer's hardware version for this PS. This
            parameter is manufacturer provided and is stored in
            non-volatile memory."
    ::= { cabhPsDevBase 4 }

cabhPsDevWanManMacAddress OBJECT-TYPE
    SYNTAX      PhysAddress (SIZE (0..16))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The PS WAN-Man MAC address. This is the PS hardware
            address to be used by the CDC to uniquely identify
            the PS to the cable data network DHCP server for
            the acquisition of an IP address to be used for
            management messaging between the cable network
            NMS and the CMP."
    ::= { cabhPsDevBase 5 }

cabhPsDevWanDataMacAddress OBJECT-TYPE
    SYNTAX      PhysAddress (SIZE (0..16))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The PS WAN-Data MAC address. The PS could have multiple
            WAN-Data Interfaces, which share the same hardware address.
            The client identifiers will be unique so that each may be
            assigned a different, unique IP address."
    ::= { cabhPsDevBase 6 }

cabhPsDevTypeIdentifier OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This is a copy of the device type identifier used in the
            DHCP option 60 exchanged between the PS and the DHCP
            server."
```

```
    REFERENCE
            "CableHome Specification, CDC Function System
            Description section."
    ::= { cabhPsDevBase 7 }

cabhPsDevSetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Setting this object to true(1) sets all PsDev MIB objects
            to the factory default values. Reading this object always
            returns false(2)."
    ::= { cabhPsDevBase 8 }

cabhPsDevWanManClientId OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (1..80))
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "This is the client ID used for WAN-MAN DHCP requests.
            The default value is the 6 byte MAC address."
    ::= { cabhPsDevBase 9 }

cabhPsDevTodSyncStatus OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object indicates whether the PS was able to
            successfully synchronize with the Time of Day (ToD) Server
            in the cable network. The PS sets this object to true(1) if
            the PS successfully synchronizes its time with the ToD
            server. The PS sets this object to false(2) if the PS does
            not successfully synchronize with the ToD server."
    DEFVAL { false }
    ::= { cabhPsDevBase 10 }

cabhPsDevProvMode OBJECT-TYPE
    SYNTAX      INTEGER
    {
        dhcpmode(1),
        snmpmode(2),
        dormantCHmode(3)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object indicates the provisioning mode in which the
            PS is operating. If the PS is operating in DHCP
            Provisioning Mode as described in the CableHome
            specification, the PS sets this object to dhcpmode(1).
            If the PS is operating in SNMP Provisioning Mode, the PS
            sets this object to snmpmode(2). If the PS is not
            configured to operate in either dhcpmode or snmpmode,
            it will fall back to Dormant CableHome Mode and set
            the value of cabhPsDevProvMode to dormantCHmode(3)."
    ::= { cabhPsDevBase 11 }

cabhPsDevLastSetToFactory OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "The value of sysUpTime when cabhPsDevSetToFactory was
            last set to true. Zero if never reset."
    ::= { cabhPsDevBase 12 }

cabhPsDevTrapControl OBJECT-TYPE
    SYNTAX BITS {
        cabhPsDevInitTLVUnknownTrap(0),
        cabhPsDevInitTrap(1),
        cabhPsDevInitRetryTrap(2),
        cabhPsDevDHCPFailTrap(3),
        cabhPsDevSwUpgradeInitTrap(4),
        cabhPsDevSwUpgradeFailTrap(5),
        cabhPsDevSwUpgradeSuccessTrap(6),
        cabhPsDevSwUpgradeCVCFailTrap(7),
        cabhPsDevTODFailTrap(8),
        cabhPsDevCdpWanDataIpTrap(9),
        cabhPsDevCdpThresholdTrap(10),
        cabhPsDevCspTrap(11),
        cabhPsDevCapTrap(12),
        cabhPsDevCtpTrap(13),
        cabhPsDevProvEnrollTrap(14),
        cabhPsDevCdpLanIpPoolTrap(15),
        cabhPsDevUpnpMultiplePHTrap(16)
    }
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
            "The object is used to enable PS notifications.
            From left to right, the set bit indicates
            the corresponding PS notification is enabled.
            For example, if the first bit is set, then
            cabhPsDevInitTLVUnknownTrap is enabled.
            If the bit is zero, the trap is disabled."
    DEFVAL { '0000'h }
    ::= { cabhPsDevBase 13 }

--
--    The following group defines Provisioning Specific parameters
--

cabhPsDevProvisioningTimer OBJECT-TYPE
    SYNTAX      INTEGER (0..16383)
    UNITS       "minutes"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object enables the user to set the duration of the
            provisioning timeout timer. The value is in minutes.
            Setting the timer to 0 disables it. The default value
            for the timer is 5."
    DEFVAL { 5 }
    ::= { cabhPsDevProv 1 }

cabhPsDevProvConfigFile OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..128))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The URL of the TFTP host for downloading provisioning and
            configuration parameters to this device. Returns NULL if
            the server address is unknown."
    ::= { cabhPsDevProv 2 }
```

```
cabhPsDevProvConfigHash OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0|20))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Hash of the contents of the PS config file, which is
            calculated by the NMS and sent to the PS. For the SHA-1
            authentication algorithm, the hash length is 160 bits. This
            hash value is encoded in binary format."
    ::= { cabhPsDevProv 3 }

cabhPsDevProvConfigFileSize OBJECT-TYPE
    SYNTAX      Integer32
    UNITS       "bytes"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Size of the configuration file."
    ::= { cabhPsDevProv 4 }

cabhPsDevProvConfigFileStatus OBJECT-TYPE
    SYNTAX      INTEGER
    {
        idle(1),
        busy(2)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object indicates the current status of the
            configuration file download process. It is provided to
            indicate to the management entity that the PS will reject
            PS Configuration File triggers (set request to
            cabhPsDevProvConfigFile) when busy."
    ::= { cabhPsDevProv 5 }

cabhPsDevProvConfigTLVProcessed OBJECT-TYPE
    SYNTAX      INTEGER (0..16383)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Number of TLVs processed in config file."
    ::= { cabhPsDevProv 6 }

cabhPsDevProvConfigTLVRejected OBJECT-TYPE
    SYNTAX      INTEGER (0..16383)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Number of TLVs rejected in config file."
    ::= { cabhPsDevProv 7 }

cabhPsDevProvSolicitedKeyTimeout OBJECT-TYPE
    SYNTAX      Integer32 (15..600)
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This timeout applies only when the Provisioning Server
            initiated key management (with a Wake Up message) for
            SNMPv3.  It is the period during which the PS will save
            a number (inside the sequence number field) from the sent
            out AP Request and wait for the matching AP Reply from the
            Provisioning Server."
```

```
    DEFVAL { 120 }
    ::= { cabhPsDevProv 8 }

cabhPsDevProvState OBJECT-TYPE
    SYNTAX      INTEGER
    {
        pass(1),
        inProgress(2),
        fail(3)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object indicates the completion state of the
            initialization process. Pass or Fail states occur after
            completion of the initialization flow. InProgress occurs
            from PS initialization start to PS initialization end."
    ::= { cabhPsDevProv 9 }

cabhPsDevProvAuthState OBJECT-TYPE
    SYNTAX      INTEGER
    {
        accepted(1),
        rejected(2)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object indicates the authentication state of the
            configuration file."
    ::= { cabhPsDevProv 10 }

cabhPsDevProvCorrelationId OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
            "Random value generated by the PS for use in registration
            authorization. It is for use only in the PS initialization
            messages and for PS configuration file download. This value
            appears in both cabhPsDevProvisioningStatus and
            cabhPsDevProvisioningEnrollmentReport informs to verify the
            instance of loading the configuration file."
    ::= { cabhPsDevProv 11 }

cabhPsDevTimeServerAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP address type of the Time server (RFC 868).
            IP version 4 is typically used."
    ::= { cabhPsDevProv 12 }

cabhPsDevTimeServerAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP address of the Time server (RFC 868). Returns
            0.0.0.0 if the time server IP address is unknown."
    ::= { cabhPsDevProv 13 }

--============================================================
```

```
--
--   PS Device Profile Group
--
--  The cabhPsDevPsProfile contains the Residential Gateway's
--  device attributes. This set of attributes is analogous to
--  some attributes of the BP Device profile.
--
--================================================================

cabhPsDevPsDeviceType OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The type of device, as defined in the CableHome
            specifications (Residential Gateway Device or CableHome
            Host Device), that implements this OID."
    DEFVAL { "CableHome Residential Gateway" }
    ::= { cabhPsDevPsAttrib 1 }

cabhPsDevPsManufacturerUrl OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Universal Resource Locator to the Residential Gateway
            device manufacturer's web site."
    ::= { cabhPsDevPsAttrib 3 }

cabhPsDevPsModelUrl OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Universal Resource Locator to the web site describing this
            CableHome compliant residential gateway device."
    ::= { cabhPsDevPsAttrib 7 }

cabhPsDevPsModelUpc OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Universal Product Code of the CableHome compliant
            residential gateway device.
            See: Uniform Code Council  www.uc-council.org"
    ::= { cabhPsDevPsAttrib 8 }

--================================================================
--
--   CableHome Host/BP Device Profile Table
--
--  The cabhPsDevBpProfile contains the list of the CableHome Host
--  device attributes provided to the PS by BPs passing their Device
--  Profile XML schema via SOAP/HTTP.
--
--================================================================

cabhPsDevBpProfileTable OBJECT-TYPE
    SYNTAX SEQUENCE OF CabhPsDevBpProfileEntry
    MAX-ACCESS  not-accessible
    STATUS      obsolete
    DESCRIPTION
            "This table contains the information for the CableHome Host
```

```
            Device Profiles. Attributes of a device make up a Device
            Profile."
    ::= { cabhPsDevBpAttrib 1 }


cabhPsDevBpProfileEntry OBJECT-TYPE
    SYNTAX      CabhPsDevBpProfileEntry
    MAX-ACCESS  not-accessible
    STATUS      obsolete
    DESCRIPTION
            "The table that describes the CableHome Host Device
            Profile."
    INDEX { cabhPsDevBpIndex }
    ::= { cabhPsDevBpProfileTable 1 }

CabhPsDevBpProfileEntry ::= SEQUENCE {
        cabhPsDevBpIndex                     INTEGER,
        cabhPsDevBpDeviceType                SnmpAdminString,
        cabhPsDevBpManufacturer              SnmpAdminString,
        cabhPsDevBpManufacturerUrl           SnmpAdminString,
        cabhPsDevBpSerialNumber              SnmpAdminString,
        cabhPsDevBpHardwareVersion           SnmpAdminString,
        cabhPsDevBpHardwareOptions           SnmpAdminString,
        cabhPsDevBpModelName                 SnmpAdminString,
        cabhPsDevBpModelNumber               SnmpAdminString,
        cabhPsDevBpModelUrl                  SnmpAdminString,
        cabhPsDevBpModelUpc                  SnmpAdminString,
        cabhPsDevBpModelSoftwareOs           SnmpAdminString,
        cabhPsDevBpModelSoftwareVersion      SnmpAdminString,
        cabhPsDevBpLanInterfaceType          IANAifType,
        cabhPsDevBpNumberInterfacePriorities INTEGER,
        cabhPsDevBpPhysicalLocation          SnmpAdminString,
        cabhPsDevBpPhysicalAddress           PhysAddress
        }

cabhPsDevBpIndex OBJECT-TYPE
    SYNTAX      INTEGER (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      obsolete
    DESCRIPTION
            "Integer index into the CableHome Host Device Profile
            Table."
    ::= { cabhPsDevBpProfileEntry 1 }

cabhPsDevBpDeviceType OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The type of device, as defined by the CableHome
            specifications (CableHome Residential Gateway or CableHome
            Host Device), that passed the Device Profile whose
            information is made available through this table row."
    DEFVAL { "CableHome Host" }
    ::= { cabhPsDevBpProfileEntry 2 }

cabhPsDevBpManufacturer OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The name of the CableHome Host Device's manufacturer."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 3 }
```

```
cabhPsDevBpManufacturerUrl OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "Universal Resource Locator to the CableHome Host device
            manufacturer's web site."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 4 }

cabhPsDevBpSerialNumber OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The serial number assigned by the manufacturer for this
            CableHome Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 5 }

cabhPsDevBpHardwareVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The hardware version number assigned by the manufacturer
            for this CableHome Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 6 }

cabhPsDevBpHardwareOptions OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The hardware options implemented on this CableHome Host
            Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 7 }

cabhPsDevBpModelName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The model name assigned by the manufacturer for this
            CableHome Host Device."
    DEFVAL  { "" }
    ::= { cabhPsDevBpProfileEntry 8 }

cabhPsDevBpModelNumber OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The model number assigned by the manufacturer for this
            CableHome Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 9 }

cabhPsDevBpModelUrl OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
```

```
    STATUS      obsolete
    DESCRIPTION
            "The Universal Resource Locator to the web site describing
            this CableHome Host Device model."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 10 }

cabhPsDevBpModelUpc OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "Universal Product Code of the CableHome Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 11 }

cabhPsDevBpModelSoftwareOs OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "Software operating system implemented on the CableHome
            Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 12 }

cabhPsDevBpModelSoftwareVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "Version of the operating system implemented on the
            CableHome Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 13 }

cabhPsDevBpLanInterfaceType OBJECT-TYPE
    SYNTAX      IANAifType
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The ifType for the LAN Interface implemented on the
            CableHome Host Device."
    REFERENCE
            "http://www.iana.org/assignments/ianaiftype-mib."
    DEFVAL { other }
    ::= { cabhPsDevBpProfileEntry 14 }

cabhPsDevBpNumberInterfacePriorities OBJECT-TYPE
    SYNTAX      INTEGER (1..8)
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "Number of QoS priorities supported by the LAN technology
            (Data Link Layer) implemented in the CableHome Host
            Device."
    DEFVAL { 1 }
    ::= { cabhPsDevBpProfileEntry 15 }

cabhPsDevBpPhysicalLocation OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
```

```
            "Physical location of the CableHome Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 16 }

cabhPsDevBpPhysicalAddress OBJECT-TYPE
    SYNTAX      PhysAddress (SIZE (0..16))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The CableHome Host Device's hardware address."
    DEFVAL { ''h }
    ::= { cabhPsDevBpProfileEntry 17 }

--================================================================
--
--  LAN IP Traffic Statistics Table
--
--  The cabhPsDevLanIpTrafficTable contains the Traffic Statistics
--  for all LAN IP Devices connected to the PS. When the PS learns a
--  new LAN IP address, an entry is added to this table.
--
--================================================================

cabhPsDevLanIpTrafficCountersReset OBJECT-TYPE
    SYNTAX      INTEGER
    {
        clearCounters(1),
        clearTable(2)
    }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Setting this object to clearCounters(1) resets all the
            traffic statistic counter entries to zero in the
            cabhPsDevLanIpTrafficTable. Setting this object to
            clearTable(2) removes all entries in the
            cabhPsDevLanIpTrafficTable. Reading this object always
            returns clearCounters(1)."
    DEFVAL { clearCounters }
    -- Default read value
    ::= { cabhPsDevStats 1 }

cabhPsDevLanIpTrafficCountersLastReset OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when
            cabhPsDevLanIpTrafficCountersReset was last written to.
            Zero if never written to."
    ::= { cabhPsDevStats 2 }

cabhPsDevLanIpTrafficEnabled OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Setting this object to true(1) turns on the IP traffic
            counters. Setting this object to false(2) turns off the IP
            traffic counters."
    DEFVAL { false } -- IP traffic counters are off by default
    ::= { cabhPsDevStats 3 }

cabhPsDevLanIpTrafficTable OBJECT-TYPE
```

```
    SYNTAX      SEQUENCE OF CabhPsDevLanIpTrafficEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains IP-layer Traffic Statistics for all
            LAN IP Devices connected to the PS."
    ::= { cabhPsDevStats 4 }

cabhPsDevLanIpTrafficEntry OBJECT-TYPE
    SYNTAX      CabhPsDevLanIpTrafficEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "List of Traffic Statistics for LAN IP Devices."
    INDEX { cabhPsDevLanIpTrafficIndex }
    ::= { cabhPsDevLanIpTrafficTable 1 }

CabhPsDevLanIpTrafficEntry ::= SEQUENCE {
    cabhPsDevLanIpTrafficIndex             INTEGER,
    cabhPsDevLanIpTrafficInetAddressType   InetAddressType,
    cabhPsDevLanIpTrafficInetAddress       InetAddress,
    cabhPsDevLanIpTrafficInOctets          ZeroBasedCounter32,
    cabhPsDevLanIpTrafficOutOctets         ZeroBasedCounter32
    }

cabhPsDevLanIpTrafficIndex OBJECT-TYPE
    SYNTAX      INTEGER   (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The Index into the LAN IP Traffic Statistics Table."
    ::= { cabhPsDevLanIpTrafficEntry 1 }

cabhPsDevLanIpTrafficInetAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The type of IP address assigned to the LAN IP device to
            which the statistics in this table row apply.  IP version
            4 is typically used."
    DEFVAL { ipv4 }
    ::= { cabhPsDevLanIpTrafficEntry 2 }

cabhPsDevLanIpTrafficInetAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP address of the LAN IP device to which the
            statistics in this table row apply.  An IPv4 IP
            address is typically used."
    ::= { cabhPsDevLanIpTrafficEntry 3 }

cabhPsDevLanIpTrafficInOctets OBJECT-TYPE
    SYNTAX      ZeroBasedCounter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The total number of octets the PS forwarded from the WAN
            interfaces to the LAN IP device associated with the value
            of cabhPsDevLanIpTrafficInetAddress. This counter object
            does not include LAN-to-LAN traffic."
    ::= { cabhPsDevLanIpTrafficEntry 4 }
```

```
cabhPsDevLanIpTrafficOutOctets OBJECT-TYPE
    SYNTAX      ZeroBasedCounter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The total number of octets the PS forwarded from the LAN
            IP device associated with the value of
            cabhPsDevLanIpTrafficInetAddress, to the WAN interfaces.
            This counter object does not include LAN-to-LAN traffic."
    ::= { cabhPsDevLanIpTrafficEntry 5 }

--=========================================================================
--
--    CableHome Interface Access Control Table
--
--  The cabhPsDevAccessControlTable lists the physical addresses
--  of all LAN IP Devices for which the PS will forward traffic to
--  or from an interface type for which the Table is enabled.
--  If an interface type is enabled, the PS will not forward traffic
--  to or from any device on that interface whose physical address
--  is not listed in the Access Control Table. If an interface type
--  is disabled, the PS does apply forwarding restrictions based on
--  entires of the Access Control Table.
--
--=========================================================================

cabhPsDevAccessControlEnable OBJECT-TYPE
    SYNTAX      BITS {
        hpna(0),  -- most significant bit
        ieee80211(1),
        ieee8023(2),
        homeplug(3),
        usb(4),
        ieee1394(5),
        scsi(6),
        other(7)
        }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object specifies the interface type(s) for which the
            PSDev Access Control Table access rules are enabled. If a
            bit field is set to 1, the PS MUST only forward traffic
            received through that interface type if the source physical
            address is an entry in the cabhPsDevAccessControlTable. If
            a bit field is set to 1, the PS MUST only forward traffic
            destined to a device on that interface type if the
            destination physical address is an entry in the
            cabhPsDevAccessControlTable. If the bit field for an
            interface type is not set, i.e., if it is equal to 0, the
            PS MUST NOT apply forwarding restrictions for that
            interface type based on the Access Control Table. The PS
            MUST implement cabhPsDevAccessControlEnable for bit 1
            (wireless LAN) and for bit 3 (HomePlug). If the PS does not
            implement cabhPsDevAccessControlEnable for any of the other
            defined bits, the PS MUST return inconsistent value error,
            and not allow the bit to be set, if an attempt is made to
            set a bit that is not implemented.

            If the PS implements a HomePNA interface and implements the
            PSDev Access Control Table enable functionality for the
            HomePNA interface, then if bit 0 is set, the PS MUST apply
            PSDev Access Control Table access rules to any PS interface
```

```
        of  IANAifType 220 (Home Phoneline Networking Alliance). If
        the PS does not implement PSDev Access Control Table enable
        functionality for the HomePNA interface, and an attempt is
        made to set bit 0 to value '1', the PS MUST return
        'Inconsistent Value' error and MUST NOT set bit 0 to
        value '1'.

        If bit 1 (ieee80211) is set, the PS MUST apply PSDev
        Access Control Table access rules to any PS interface of
        IANAifType 71 (radio spread spectrum).

        If the PS implements an IEEE 802.3/CSMA-CD interface and
        implements the PSDev Access Control Table enable
        functionality for the IEEE 802.3/CSMA-CD interface, then
        if bit 2 is set, the PS MUST apply PSDev Access Control
        Table access rules to any PS interface of  IANAifType 6
        (ethernetCsmacd). If the PS does not implement PSDev
        Access Control Table enable functionality for a
        IEEE 802.3/CSMA-CD interface, and an attempt is made to set
        bit 2 to value '1', the PS MUST return 'Inconsistent
        Value' error and MUST NOT set bit 2 to value '1'.

        If bit 3 (homeplug) is set, the PS MUST apply PSDev
        Access Control Table access rules to any PS HomePlug
        Powerline Alliance (HomePlug) interface as defined by
        HomePlug Powerline Alliance (www.homeplug.org).

        If the PS implements a USB interface and implements the
        PSDev Access Control Table enable functionality for the
        USB interface, then if bit 4 is set, the PS MUST apply
        PSDev Access Control Table access rules to any PS
        interface of  IANAifType 160 (USB). If the PS does not
        implement PSDev Access Control Table enable functionality
        for the USB interface, and an attempt is made to set
        bit 4 to value '1', the PS MUST return 'Inconsistent Value'
        error and MUST NOT set bit 4 to value '1'.

        If the PS implements an IEEE 1394 interface and
        implements the PSDev Access Control Table enable
        functionality for the IEEE 1394 interface, then if bit 5
        is set, the PS MUST apply PSDev Access Control Table
        access rules to any PS interface of  IANAifType 144
        (IEEE 1394 High Performance Serial Bus). If the PS does
        not implement PSDev Access Control Table enable
        functionality for the IEEE 1394 interface, and an attempt
        is made to set bit 5 to value '1', the PS MUST return
        'Inconsistent Value' error and MUST NOT set bit 5 to
        value '1'.

        If the PS implements a SCSI interface and implements the
        PSDev Access Control Table enable functionality for the
        SCSI interface, then if bit 6 is set, the PS MUST apply
        PSDev Access Control Table access rules to any PS SCSI-2
        or SCSI-3 interface. If the PS does not implement PSDev
        Access Control Table enable functionality for the SCSI
        interface, and an attempt is made to set bit 6 to value
        '1', the PS MUST return 'Inconsistent Value' error and
        MUST NOT set bit 6 to value '1'.

        If bit 7 (other) is set, the PS MAY apply PSDev Access
        Control Table filter access to any PS interface of a type
        other than the types defined by bits 0 - 6."
DEFVAL { '00'h }  -- null, all interface types disabled
::= { cabhPsDevAccessControl 1 }
```

```
cabhPsDevAccessControlTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhPsDevAccessControlEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains a list of the physical addresses of
            LAN IP Devices to and from which the PS will forward
            traffic through a LAN interface if
            cabhPsDevAccessControlEnable is enabled(1) for that
            interface type."
    REFERENCE
            "CableHome specification, Packet Handling & Address
            Translation section."
    ::= { cabhPsDevAccessControl 2 }

cabhPsDevAccessControlEntry OBJECT-TYPE
    SYNTAX      CabhPsDevAccessControlEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "List of the physical addresses for LAN IP Devices
            to and from which the PS will forward traffic when
            the PSDev Access Control Table is enabled."
    INDEX { cabhPsDevAccessControlIndex }
    ::= { cabhPsDevAccessControlTable 1 }

CabhPsDevAccessControlEntry ::= SEQUENCE {
    cabhPsDevAccessControlIndex     INTEGER,
    cabhPsDevAccessControlPhysAddr  PhysAddress,
    cabhPsDevAccessControlRowStatus RowStatus
    }

cabhPsDevAccessControlIndex OBJECT-TYPE
    SYNTAX      INTEGER (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Integer index into the CableHome PSDev Access Control
            Table."
    ::= { cabhPsDevAccessControlEntry 1 }

cabhPsDevAccessControlPhysAddr OBJECT-TYPE
    SYNTAX      PhysAddress (SIZE (1..16))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The physical address of the LAN IP Device for which the PS
            will forward traffic when the PSDev Access Control
            Table is enabled. The PS will not forward traffic
            from any LAN IP Device whose physical address is
            not an entry of the PSDev Access Control Table when the
            PSDev Access Control Table is enabled for the
            corresponding interface."
    ::= { cabhPsDevAccessControlEntry 2 }

cabhPsDevAccessControlRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The RowStatus interlock for the creation and deletion
            of a cabhPsDevAccessControlTable entry. Any writable
            object in each row of the cabhPsDevAccessControlTable
```

```
            can be modified at any time while the row is active(1)."
    ::= { cabhPsDevAccessControlEntry 3 }

--========================================================================
--
--    CableHome Miscellaneous MIB
--
--  This branch of cabhPsDevMib contains extensions related to
--  functionalities defined for other standards bodies or outside
--  of CableHome fully defined features.
--
--========================================================================

--========================================================================
--
--    CableHome User Interface Miscellaneous MIB
--
--  PS MIB objects for controlling features of the CableHome compliant
--  residential gateways User Interface (UI) if present.
--
--========================================================================

cabhPsDevUILogin OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..32))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This parameter specifies the value of the user login name
            required for access to the CableHome compliant residential
            gateway device's user interface."
    ::= { cabhPsDevUI 1 }

cabhPsDevUIPassword OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(4..32))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This parameter specifies the value of the user password
            required for access to the CableHome compliant residential
            gateway device's user interface."
    ::= { cabhPsDevUI 2 }

cabhPsDevUISelection OBJECT-TYPE
    SYNTAX      INTEGER {
                    manufacturerLocal(1),
                    cableOperatorLocal(2),
                    cableOperatorServer(3),
                    disabledUI(4)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Indicates the type of Web user interface (UI)
            to present to the user if Web interface is supported:
            manufacturerLocal:
              PS uses the vendor UI shipped with the device.
            cableOperatorLocal:
              PS uses a cable operator defined UI interface.
              To operate properly, it should require a special code
              image downloaded into the PS.  By default, if no cable
              operator UI is being defined, selecting this option
              points to 'manufacturerLocal' selection.
            cableOperatorServer:
              PS redirects HTTP requests to its UI to the URL specified
```

```
              in cabhPsDevUIServerUrl.
            disabledUI:
              PS responds to HTTP requests to its UI with an HTTP page
              containing the value of
              cabhPsDevUISelectionDisabledBodyText as the body tag;
              or with a vendor specific message or HTTP error if that
              value is null."
    DEFVAL { manufacturerLocal }
    ::= { cabhPsDevUI 3 }

cabhPsDevUIServerUrl OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..255))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Uniform Resource Locator (URL) provisioned by the cable
            operator to which the PS re-directs the subscriber's LAN IP Device
            for presentation of the PS User Interface when the value of
            cabhPsDevUISelection is cableOperatorServer(3). This object is valid
            and applicable only when the value of cabhPsDevUISelection is
            cableOperatorServer(3)."
    DEFVAL { "" }
    ::= { cabhPsDevUI 4 }

cabhPsDevUISelectionDisabledBodyText OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..255))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Default text for the HTTP body tag to include in the
            response to UI requests when the object
            cabhPsDevUISelection is set to 'disabledUI'.
            An example of a body tag is below:
            <body>Feature currently disabled by Cable Operator</body>."
    ::= { cabhPsDevUI 5 }

-- ========================================================
-- IEEE802dot11-MIB CableHome extension
-- ========================================================

cabhPsDev802dot11BaseTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhPsDev802dot11BaseEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "CableHome specifics controls for 80211 wireless
            interfaces."
    ::= { cabhPsDev802dot11 1 }

cabhPsDev802dot11BaseEntry OBJECT-TYPE
    SYNTAX      CabhPsDev802dot11BaseEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry in cabhPsDev802dot11BaseTable associated to a
            wireless interface of IANAifType ieee80211.(71)"
    INDEX { ifIndex }
    ::= { cabhPsDev802dot11BaseTable 1 }

CabhPsDev802dot11BaseEntry ::=
    SEQUENCE {
              cabhPsDev802dot11BaseSetToDefault     TruthValue,
              cabhPsDev802dot11BaseLastSetToDefault TimeStamp,
              cabhPsDev802dot11BaseAdvertiseSSID    TruthValue,
```

```
            cabhPsDev802dot11BasePhyCapabilities  BITS,
            cabhPsDev802dot11BasePhyOperMode      INTEGER
           }

cabhPsDev802dot11BaseSetToDefault OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "When set  to true(1), the PS MUST reset to default values
            the MIB objects of IEEE802dot11-MIB module and others under
            cabhPsDev802dot11 for this entry related IfIndex.
            Reading this object always return false(2)."
    DEFVAL { false }
    ::= { cabhPsDev802dot11BaseEntry 1 }

cabhPsDev802dot11BaseLastSetToDefault OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when
            cabhPsDev802dot11MIBSetToDefault was last set to true.
            Zero if never reset."
    ::= { cabhPsDev802dot11BaseEntry 2 }

cabhPsDev802dot11BaseAdvertiseSSID OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "When set to false(2) the PS does not advertise the BSS
            SSID in a proprietary manner. To avoid interoperability
            problems and service disruption, it is RECOMMENDED to set
            this object always to true. This feature does not provide
            any security, and does not prevent Wireless Stations to
            obtain the SSID by sniffing frames from other stations in
            the ESS. If the device does not support the feature of
            turning on/off the SSID advertisement, this object always
            reports 'true(1)' and reports the error 'wrongValue' when
            set to 'false(2)."
    DEFVAL { true }
    ::= { cabhPsDev802dot11BaseEntry 3 }

cabhPsDev802dot11BasePhyCapabilities OBJECT-TYPE
    SYNTAX      BITS {
                    --ieee80211DSSS(0) , not interest
                      ieee80211a(0),
                      ieee80211b(1),
                      ieee80211g(2)
                    --ieee80211FHSS(8),
                    --ieee80211IR(16)
                    --values with comments are not requirements
                    --included for completeness of 80211 spec.
                    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Indicates the PHY capabilities of the wireless interface."
    ::= { cabhPsDev802dot11BaseEntry 4 }

cabhPsDev802dot11BasePhyOperMode OBJECT-TYPE
    SYNTAX      INTEGER {
                        ieee80211a(1),
```

```
                        ieee80211b(2),
                        ieee80211g(4),
                        ieee80211bg(24)
                       }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Indicates the PHY mode of operation being set for the
            wireless interface. Setting this object will update the
            value of dot11PhyType. Accordingly (if implemented), as
            well as the object dot11OperationalRateSet to the 80211
            mandatory rates for dot11PhyType.

            It is left to vendors the option to update the values of
            PS optional dot11SupportedDataRatesTxEntry and
            dot11SupportedDataRatesRxEntry tables based on the
            operational mode.

            In the case of selecting ieee80211bg(14), dot11PhyType
            reports erp(6) and dot11OperationalRateSet should report
            HRDSSS and ERP mandatory rates and in addition 54 Mbit/s rate
            if supported by PS. e.g. : (this example assumes 54 Mbit/s
            OFDM is supported.
            HR-DSSS :
              Mandatory:
                     1 Mbit/s '80'H + '01'H
                     2 Mbit/s '80'H + '02'H
                     5.5 Mbit/s '80'H + '0B'H
                    11 Mbit/s '80'H + '16'H
            ERP :
              Mandatory:
                     6 Mbit/s '80'H + '0C'H
                    12 Mbit/s '80'H + '18'H
                    24 Mbit/s '80'H + '30'H
     (if supported) 54 Mbit/s '80'H + '6C'
              Optional:
                    22 Mbit/s '00'H + '2C'H
                    33 Mbit/s '00'H + '42'H
                    18 Mbit/s '00'H + '24'H
                    36 Mbit/s '00'H + '48'H
                    48 Mbit/s '00'H + '60'H

          Combined operational rates in :

            dot11OperationalRateSet value in rate order regardless
            of '80'H flag and using dots for clarity :
            + means flagged '80'H, - not flagged.
          Rates Mbit/s: +1,+2,+5.5,+6,+11,+12,-18,-22,+24,-33,-36,-48,+54
                Hex:  '81.82.8B.8C.96.98. 24.2C.B0.48.42. 60.EC'H

            The default value of this object is left to the vendor to
            accommodate the factory defaults for the device."
    REFERENCE
            "IEEE Std 802.11, 1999 Edition,
            IEEE Std 802.11a-1999,
            IEEE Std 802.11b-1999/Cor 1-2001,
            IEEE Std 802.11g-2003."
    ::= { cabhPsDev802dot11BaseEntry 5 }

-- ============================================================
-- IEEE802dot11MIB CableHome extension for security configuration
-- ============================================================

cabhPsDev802dot11SecTable OBJECT-TYPE
```

```
    SYNTAX      SEQUENCE OF CabhPsDev802dot11SecEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "CableHome specifics controls for configuring the
            security mechanisms of 80211 wireless interfaces."
    ::= { cabhPsDev802dot11 2 }

cabhPsDev802dot11SecEntry OBJECT-TYPE
    SYNTAX      CabhPsDev802dot11SecEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry in cabhPsDev802dot11SecTable associated to a
            wireless interface of IANAifType ieee80211(71)."
    INDEX { ifIndex }
    ::= { cabhPsDev802dot11SecTable 1 }

CabhPsDev802dot11SecEntry ::=
    SEQUENCE {
              cabhPsDev802dot11SecCapabilities              BITS,
              cabhPsDev802dot11SecOperMode                  BITS,
              cabhPsDev802dot11SecPassPhraseToWEPKey        OCTET STRING,
              cabhPsDev802dot11SecUsePassPhraseToWEPKeyAlg  TruthValue,
              cabhPsDev802dot11SecPSKPassPhraseToKey        OCTET STRING,
              cabhPsDev802dot11SecWPAPreSharedKey           OCTET STRING,
              cabhPsDev802dot11SecWPARekeyTime              Unsigned32,
              cabhPsDev802dot11SecControl                   INTEGER,
              cabhPsDev802dot11SecCommitStatus              INTEGER
             }

cabhPsDev802dot11SecCapabilities OBJECT-TYPE
    SYNTAX      BITS {
                      wep64(0),
                      wep128(1),
                      wpaPSK(2)
                    --wpa2PSK(3)
                     }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The PS capabilities for Authentication and encryption used
            to authenticate 802.11 clients."
    ::= { cabhPsDev802dot11SecEntry 1 }

cabhPsDev802dot11SecOperMode OBJECT-TYPE
    SYNTAX      BITS {
                      wep64(0),
                      wep128(1),
                      wpaPSK(2)
                   -- wpa2PSK(3)
                     }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Indicates the Authentication and encryption mechanism to
            be enabled for the users and advertised in Beacon messages.
            Bits set to this object and not supported by the PS in
            cabhPsDev802dot11SecCapabilities are set to '0' without
            failing the SNMP set. Setting two bits that the PS does not
            support in combination returns an error 'wrongValue'.
            In particular:
              Setting to '1' both wep64(0)and wep128(1) bits returns an
                error'wrongValue'.
```

```
              Setting a combination of WEP bits (wep64(0) or wep128(1))
                and wpaPSK bit returns is not a mandatory requirement,
                therefore an error 'wrongValue' may be reported.

            Setting any bit to '1' must not affect the value of object
            dot11PrivacyInvoked.

            If dot11PrivacyInvoked is set to 'false', the 80211 WEP
            security mechanism is disabled (see dot11PrivacyInvoked
            description) and the value of this object is not used.

            Setting the wpaPSK(2) bit to '1' indicates the usage of
            WPA-PSK TKIP.

            Note that to enable the PSK security mechanism, the value
            of cabhPsDev802dot11SecWPAPreSharedKey must be a non-zero
            length string."
    ::= { cabhPsDev802dot11SecEntry 2 }

cabhPsDev802dot11SecPassPhraseToWEPKey OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0|5..63))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Password used for PS to derive WEP encryption keys.
            After a successful set, the values of
            dot11WEPDefaultKeyValue are populated as described below:

            For wep64:
              If cabhPsDev802dot11SecOperMode wep64 bit is set to '1'
              This object value (x) is used as a generator of a 4-octet
              seed.

              seed[i%4] = XOR(seed[i%4],x[i]); i from 1 to len(x) -1

            The values of the four dot11WEPDefaultKeyValue are
            calculated as indicated below :
              loop j 1..4
              loop k 0..4
              seed = seed * (((26*8+1)*256-1)*4+1) + 2531011
              The value is always truncated at 32 bits.
              OCTETk = (seed >> 16 )& 0xFF  -lowest octet-
              end loop
              dot11WEPDefaultKeyValue(j) = OCTET0,OCTET1, ... OCTET4
              end loop

              Note that seed value is constantly re-computed when
              calculating each octet of each default WEP key.

            For wep128:
              If cabhPsDev802dot11SecOperMode wep128 bit is set to '1'
              This object value (x) fills a 64-octet buffer y :
              y = x,x,x...up to 64 octets.
              Calculate the 128-bit MD5 digest of y
              the values of all dot11WEPDefaultKeyValue (1..4)
              are calculated by truncating the first 13 octets
              of MD5y.

            dot11WEPDefaultKeyValue = MD5y0,MD5y1, .. MD5y12

              This object value is normally read by issuing SNMP
              request PDUs. This object can be cleared with an SNMP
              SET to an empty string Value and the PS MUST not update
              the type of keys being set to '1' in
```

```
   cabhPsDev802dot11SecOperMode.

 If cabhPsDev802dot11SecUsePassPhraseToKeyAlg is set to
 false(2), the behaviour of a SET to this object depends
 on the bits set for cabhPsDev802dot11SecOperMode as
 follows:


   If cabhPsDev802dot11SecOperMode bit wep64 is set to '1'
   and this object value length is 5 octets, the MIB object
   dot11WEPDefaultKeyValue.1 (WEP key 0) is populated with
   this object value, otherwise an error 'inconsistentValue'
   is reported.

   If cabhPsDev802dot11SecOperMode bit wep128 is set to '1'
   and this object value length is 13 octets, the MIB object
   dot11WEPDefaultKeyValue.1 (WEP key 0) is populated with
   this object value, otherwise an error 'inconsistentValue'
   is reported.

 Vector examples for wep64 and wep128 key derivation:

   Note:
   % refers to the module operation (reminder of the
   quotient of i and 4); XOR is the OR exclusive boolean
   operation.

For wep64:
passphrase:
        'ABCD4321' ( hex code 0x41.42.43.44.34.33.32.31 )


First loop: (octets 0..3)
   XOR (0x00,A) -> XOR(0x00,0x41) -> 0x41
   XOR (0x00,B) -> XOR(0x00,0x42) -> 0x42
   XOR (0x00,C) -> XOR(0x00,0x43) -> 0x43
   XOR (0x00,D) -> XOR(0x00,0x44) -> 0x44

Second loop: (octets 4..7)
   XOR (A,4) -> XOR(0x41,0x34) -> 0x75
   XOR (B,3) -> XOR(0x42,0x33) -> 0x71
   XOR (C,2) -> XOR(0x43,0x32) -> 0x71
   XOR (D,1) -> XOR(0x44,0x31) -> 0x75

 initial seed 0x75717175 -> 1970368885

 DefaultKeys calculation

 key1
 seed : 0x16545E64 -> 2nd MSB byte : 0x54
 seed : 0x41681397 -> 2nd MSB byte : 0x68
 seed : 0x1BE77FFE -> 2nd MSB byte : 0xE7
 seed : 0xAA6996C9 -> 2nd MSB byte : 0x69
 seed : 0xD1523E68 -> 2nd MSB byte : 0x52
 dot11WEPDefaultKeyValue.1 = 0x5468E76952

 key2
 seed : 0x1FFB838B -> 2nd MSB byte : 0xFb
 seed : 0xF9C60022 -> 2nd MSB byte : 0xC6
 seed : 0xAB43A65D -> 2nd MSB byte : 0x43
 seed : 0xE9A35FAC -> 2nd MSB byte : 0xA3
 seed : 0xE7AA2FBF -> 2nd MSB byte : 0xAA
 dot11WEPDefaultKeyValue.2 = 0xFBC643A3AA
```

```
            key3
            seed : 0x6D13CB86 -> 2nd MSB byte : 0x13
            seed : 0x5D8CD431 -> 2nd MSB byte : 0x8C
            seed : 0xCC702630 -> 2nd MSB byte : 0x70
            seed : 0xD78AEC33 -> 2nd MSB byte : 0x8A
            seed : 0x24DC662A -> 2nd MSB byte : 0xDC
            dot11WEPDefaultKeyValue.3 = 0x138C708ADC

            key4
            seed : 0x4F329445 -> 2nd MSB byte : 0x32
            seed : 0x3EC035F4 -> 2nd MSB byte : 0xC0
            seed : 0xF416CCE7 -> 2nd MSB byte : 0x16
            seed : 0x9904940E -> 2nd MSB byte : 0x04
            seed : 0x28969A99 -> 2nd MSB byte : 0x96
            dot11WEPDefaultKeyValue.4 = 0x32C0160496

            For wep128:
            passphrase:
                   'ABCD4321' ( hex code 0x41.42.43.44.34.33.32.31 )
            128-bit MD-5 digest 0xFECBACF05B42F7A138A5F3928E
            dot11WEPDefaultKeyValue.1..4 = 0xFECBACF05B42F7A138A5"
    ::= { cabhPsDev802dot11SecEntry 3 }

cabhPsDev802dot11SecUsePassPhraseToWEPKeyAlg OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "When this object value is true(1), the WEP Pass Phrase to
            key mechanism described in
            cabhPsDev802dot11SecPassPhraseToWEPKey applies. When this
            object is set to false(2), the Pass Phrase to WEP Key
            mechanism is ignored and the password is used as WEP key
            to populate the MIB object keydot11WEPDefaultKeyValue
            object as indicated in
            cabhPsDev802dot11SecPassPhraseToWEPKey description."
    DEFVAL { true }
    ::= { cabhPsDev802dot11SecEntry 4 }

cabhPsDev802dot11SecPSKPassPhraseToKey OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(8..63))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Password used for PS to derive WPA PSK encryption key.
            After a successful set, the values of
            cabhPsDev802dot11SecWPAPreSharedKey are updated as described
            below:

            For wpaPSK:
            If cabhPsDev802dot11SecOperMode wpaPSK bit is set to '1',
            the value of cabhPsDev802dot11SecWPAPreSharedKey is updated
            with the Password Base Key Derivation Function from  the
            Password-based Cryptographic Specification PKCS #5 v2.0
            RFC 2898 (PBKDF2) with the following specific parameters:

            PSK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256);
            PassPhrase is the value of this object;
            ssid is the PS SSID value used as the function salt;
            ssidLength is the number of octets of ssid;
            the iterations count is 4096 and the key generation length
            is 256 bits (32 octets).

            This object value is normally read by issuing SNMP request
```

```
            PDUs. This object can be cleared with an SNMP SET to an
            empty string Value and the PS MUST not update the type of
            keys being set to '1' in cabhPsDev802dot11SecOperMode.

            Vector examples for wpaPSK:

            for wpaPSK:
            passphrase:
                   'ABCD4321' ( hex code 0x41.42.43.44.34.33.32.31 )
            SSID: 'ABCD4321' ( hex code 0x41.42.43.44.34.33.32.31 )

            256 bit PBKDF2('ABCD4321', 'ABCD4321', 8, 4096, 32)
            cabhPsDev802dot11SecWPAPreSharedKey =
            0x7C199CF2FEF9AF206C8EE0E9703920C2
              3517068B3F96B011E0F975C9131BDB58"
    ::= { cabhPsDev802dot11SecEntry 5 }

cabhPsDev802dot11SecWPAPreSharedKey OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0|32))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Pre-shared key used for the PS when the bit 'wpaPSK'
            is set to '1'. This object can be set directly or derived
            from the password phrase set in
            cabhPsDev802dot11SecPSKPassPhraseToKey. This object is
            meaningful when the bit wpaPSK is set to '1'.

            If the value of this object is the zero-length string, the
            PS must not activate the PSK security mechanism."
    DEFVAL { ''H }
    ::= { cabhPsDev802dot11SecEntry 6 }

cabhPsDev802dot11SecWPARekeyTime OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Time interval to initiate WPA Group Keys (GTK) updates."
    DEFVAL { 86400 }
    ::= { cabhPsDev802dot11SecEntry 7 }

cabhPsDev802dot11SecControl OBJECT-TYPE
    SYNTAX INTEGER {
        restoreConfig(1),
        commitConfig(2)
        }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The control for the indexed 80211 device configuration.
            All changes to the cabhPsDev802dot11SecEntry MIB objects
            are reflected when reading the value of the MIB objects;
            however, those changes are NOT applied to the running
            configuration of the indexed 80211 device until they are
            successfully committed via use of the
            cabhPsDev802dot11SecControl object.

            If changes are made to the cabhPsDev802dot11SecEntry MIB
            objects which are not yet successfully committed to the
            indexed 80211 device, the cabhPsDev802dot11SecControl
            object can be used to roll back all changes to the last
            valid 80211 device configuration and discard all
```

```
            intermediate changes.

            restoreConfig - Setting cabhPsDev802dot11SecControl to this
            value will cause any changes to the
            cabhPsDev802dot11SecEntry objects not yet committed be
            reset to the values from the current running
            configuration of the indexed 80211 device.

            commitConfig - Setting cabhPsDev802dot11SecControl to this
            value will cause the indexed 80211 device to validate and
            apply the valid cabhPsDev802dot11SecEntry MIB settings to
            its running configuration. The
            cabhPsDev802dot11SecCommitStatus object will detail the
            status of this operation."
    DEFVAL { restoreConfig }
    ::= { cabhPsDev802dot11SecEntry 8 }

cabhPsDev802dot11SecCommitStatus OBJECT-TYPE
    SYNTAX INTEGER {
        commitSucceeded(1),
        commitNeeded(2),
        commitFailed(3)
        }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Indicates the status of committing the current
            cabhPsDev802dot11SecEntry MIB object values to the running
            configuration of the indexed 80211 device.

            commitSucceeded - indicates the current
            cabhPsDev802dot11SecEntry MIB object values are valid and
            have been successfully committed to the running
            configuration of the indexed 80211 device.

            commitNeeded - indicates that the value of one or more
            objects in cabhPsDev802dot11SecEntry MIB group have been
            changed but not yet committed to the running configuration
            of the indexed 80211 device.

            commitFailed - indicates the PS was unable to commit the
            cabhPsDev802dot11SecEntry MIB object values to the running
            configuration of the indexed 80211 device due to conflicts
            in those values."
    DEFVAL { commitSucceeded }
    ::= { cabhPsDev802dot11SecEntry 9 }

-- ============================================================
--
-- UPnP Services
-- Contains CableHome Portal Server UPnP information of LAN hosts
--
-- ============================================================

cabhPsDevUpnpEnabled OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Setting this object to false(1) disables PS UPnP
            services and UPnP MIB objects related functionality.
            When this object reports 'false', any set to
            UPnP read-write or read-create objects returns error
            'InconsistentValue'.  Transitions of this object from
```

```
            'true' to 'false' and vice versa does not alter the content
            of persistent MIB objects and may clear dynamically UPnP
            created entries. This object value persists upon system
            reinitialization."
    DEFVAL { true }
    ::= { cabhPsDevUpnpBase 1 }

cabhPsDevUpnpCommandIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The type of InetAddress for cabhPsDevUpnpCommandIp."
    DEFVAL { ipv4 }
    ::= { cabhPsDevUpnpCommands 1 }

cabhPsDevUpnpCommandIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP address of the device for which the UPnP
            information is being requested. This may be an IPv4 or
            IPv6 prefix. When quering specific information about the
            PS itself, the PS router IP address 192.168.0.1
            should be specified ."
    DEFVAL { 'C0A80001'h } -- 192.168.0.1
    ::= { cabhPsDevUpnpCommands 2 }

cabhPsDevUpnpCommand OBJECT-TYPE
    SYNTAX      INTEGER {
        discoveryInfo(1),
        qosDeviceCapabilities(2),
        qosDeviceState(3)
        }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The type of information to be retrieved from the Upnp
            Devices in the LAN side and stored in
            cabhPsDevUpnpInfoTable.
            The following selections are supported:

            - discoveryInfo:
            PS retrieves the Discovery information of UPnP devices.
            If the Ip address specified in
            cabhPsDevUpnpCommandIp is 255.255.255.255,
            the PS executes an M-search command and then
            retrieves the discovery information of the
            responding devices. The data stored in
            cabhPsDevUpnpInfoTable also contain UPnP
            discovery data of the PS itself.

            - qosDeviceCapabilities:
            This command is executed for unicast address only
            and will trigger the PS to retrieve the QoS device
            information pertaining to QoS capabilities.

            - qosDeviceState:
            This command is executed for unicast address only
            and will trigger the PS to retrieve the QoS device
            information pertaining to QoS Device state."
    DEFVAL { discoveryInfo }
    ::= { cabhPsDevUpnpCommands 3 }
```

```
cabhPsDevUpnpCommandUpdate OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "If set to 'true' triggers the execution of the command
            indicated in cabhPsDevUpnpCommand for the host(s) in
            cabhPsDevUpnpCommandIp. Setting to true this object will
            return error 'wrongValue'  if host IP corresponds to
            255.255.255.255 and cabhPsDevUpnpCommand value is not
            'discoveryInfo'. Reading this value always returns 'false'."
    ::= { cabhPsDevUpnpCommands 4 }

cabhPsDevUpnpLastCommandUpdate OBJECT-TYPE
    SYNTAX      TimeTicks
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The sysUpTime value of the last time the object
            cabhPsDevUpnpLastCommandUpdate was set to 'true'."
    ::= { cabhPsDevUpnpCommands 5 }

cabhPsDevUpnpCommandStatus OBJECT-TYPE
    SYNTAX      INTEGER {
        none(1),
        inProgress(2),
        complete(3),
        failed(4)
        }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The status of cabhPsDevUpnpCommandUpdate trigger
            none(1)
            initial state.
            inProgress(2)
            the information is being acquired by the
            device, PS does not change from 'inProgress'
            to the final state (complete, failed)
            until the execution has finished.
            complete(3) The overall execution is finished with
            no error conditions.
            failed(4).
            The UPnP Device has experienced a timeout. In the
            case of multiple devices query
            (cabhPsDevUpnpCommand set to 'discoveryInfo')
            The failed devices are stored with content information
            empty. At system initialization this object returns
            'none'."
    DEFVAL { none }
    ::= { cabhPsDevUpnpCommands 6}

cabhPsDevUpnpInfoTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhPsDevUpnpInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains QoS related information of LAN
            UPnP devices or the PS itself."
    ::= { cabhPsDevUpnpCommands 7 }

cabhPsDevUpnpInfoEntry OBJECT-TYPE
    SYNTAX      CabhPsDevUpnpInfoEntry
```

```
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The Indexes for this entries
            Entries are created after setting to 'true' the
            value of cabhPsDevUpnpCommand."
    INDEX { cabhPsDevUpnpInfoIpType, cabhPsDevUpnpInfoIp,
            cabhPsDevUpnpInfoXmlFragmentIndex }
    ::= { cabhPsDevUpnpInfoTable 1 }

CabhPsDevUpnpInfoEntry::= SEQUENCE {
    cabhPsDevUpnpInfoIpType            InetAddressType,
    cabhPsDevUpnpInfoIp                InetAddress,
    cabhPsDevUpnpInfoXmlFragmentIndex  Unsigned32,
    cabhPsDevUpnpInfoXmlFragment       OCTET STRING
    }

cabhPsDevUpnpInfoIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The type of InetAddress for cabhPsDevUpnpInfoIp."
    ::= { cabhPsDevUpnpInfoEntry 1 }

cabhPsDevUpnpInfoIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The IP address of the device for which the UPnP
            information is being stored. This may be a DNS name
            (LAN Host name), an IPv4 or IPv6 prefix. Information
            pertaining to the PS itself is indicated by the PS
            well-known LAN IP address interface 192.168.0.1."
    ::= { cabhPsDevUpnpInfoEntry 2 }

cabhPsDevUpnpInfoXmlFragmentIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index of the sequence of entries of
            cabhPsDevUpnpInfoXmlFragment for a specific
            cabhPsDevUpnpInfoIp IP address starting with '1'."
    ::= { cabhPsDevUpnpInfoEntry 3 }

cabhPsDevUpnpInfoXmlFragment OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..400))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The UPnP Device information being requested by
            cabhPsDevUpnpCommand for the IP addresses specified
            in cabhPsDevUpnpInfoIp for LAN host(s). If the
            information is greater than 400 bytes,
            cabhPsDevUpnpInfoXmlFragmentIndex indicates the
            sequence of the consecutive portions per host identified in
            the table."
    ::= { cabhPsDevUpnpInfoEntry 4 }

--

cabhPsNotification     OBJECT IDENTIFIER ::= { cabhPsDevMib 2 }
```

```
cabhPsDevNotifications OBJECT IDENTIFIER ::= { cabhPsNotification 0 }
cabhPsConformance      OBJECT IDENTIFIER ::= { cabhPsDevMib 3 }
cabhPsCompliances      OBJECT IDENTIFIER ::= { cabhPsConformance 1 }
cabhPsGroups           OBJECT IDENTIFIER ::= { cabhPsConformance 2 }

--
--    Notification Group
--

cabhPsDevInitTLVUnknownTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
        }
    STATUS      current
    DESCRIPTION
            "Event due to detection of unknown TLV during the TLV
            parsing process. The values of docsDevEvLevel, docsDevId,
            and docsDevEvText are from the entry which logs this event
            in the docsDevEventTable.  The value of
            cabhPsDevWanManMacAddress indicates the WAN-Man MAC address
            of the PS. This part of the information is uniform across
            all PS Traps."
    ::= { cabhPsDevNotifications 1 }

cabhPsDevInitTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        cabhPsDevProvConfigFile,
        cabhPsDevProvConfigTLVProcessed,
        cabhPsDevProvConfigTLVRejected
    }
    STATUS      current
    DESCRIPTION
            "This inform is issued to confirm the successful completion
            of the CableHome provisioning process."
    ::= { cabhPsDevNotifications 2 }

cabhPsDevInitRetryTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "An event to report a failure happened during the
            initialization process and was detected in the PS."
    ::= { cabhPsDevNotifications 3 }

cabhPsDevDHCPFailTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        cabhCdpServerDhcpAddress
    }
```

```
    STATUS      current
    DESCRIPTION
            "An event to report the failure of a DHCP server. The
            value of cabhCdpServerDhcpAddress is the IP address of
            the DHCP server."
    ::= { cabhPsDevNotifications 4 }

cabhPsDevSwUpgradeInitTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        docsDevSwFilename,
        docsDevSwServer
    }
    STATUS      current
    DESCRIPTION
            "An event to report a software upgrade initiated event.
            The values of docsDevSwFilename, and docsDevSwServer
            indicate the software image name and the IP address of the
            server from which the image was downloaded."
    ::= { cabhPsDevNotifications 5 }

cabhPsDevSwUpgradeFailTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        docsDevSwFilename,
        docsDevSwServer
    }
    STATUS      current
    DESCRIPTION
            "An event to report the failure of a software upgrade
            attempt. The values of docsDevSwFilename, and
            docsDevSwServer indicate the software image name and the IP
            address of the server from which the image was downloaded."
    ::= { cabhPsDevNotifications 6 }

cabhPsDevSwUpgradeSuccessTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        docsDevSwFilename,
        docsDevSwServer
    }
    STATUS      current
    DESCRIPTION
            "An event to report the Software upgrade success event.
            The values of docsDevSwFilename, and docsDevSwServer
            indicate the software image name and the IP address of the
            server from which the image was downloaded."
    ::= { cabhPsDevNotifications 7 }

cabhPsDevSwUpgradeCVCFailTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
```

```
    }
    STATUS      current
    DESCRIPTION
            "An event to report the failure of the verification of code
            file happened during a secure software upgrade attempt."
    ::= { cabhPsDevNotifications 8 }

cabhPsDevTODFailTrap NOTIFICATION-TYPE
    OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevTimeServerAddr,
       cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "An event to report the failure of a time of day server.
            The value of cabhPsDevTimeServerAddr indicates the server
            IP address."
    ::= { cabhPsDevNotifications 9 }

cabhPsDevCdpWanDataIpTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhCdpWanDataAddrClientId,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "An event to report the failure of PS to obtain all
            needed WAN-Data Ip Addresses.
            cabhCdpWanDataAddrClientId indicates the ClientId for
            which the failure occurred."
    ::= { cabhPsDevNotifications 10 }

cabhPsDevCdpThresholdTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        cabhCdpLanTransThreshold
    }
    STATUS      current
    DESCRIPTION
            "An event to report that the LAN-Trans address assignment
            threshold has been exceeded."
    ::= { cabhPsDevNotifications 11 }

cabhPsDevCspTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "To report an event with the CableHome Security Portal."
    ::= { cabhPsDevNotifications 12 }
```

```
cabhPsDevCapTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "To report an event with the CableHome Address Portal."
    ::= { cabhPsDevNotifications 13 }

cabhPsDevCtpTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "To report an event with the CableHome Test Portal."
    ::= { cabhPsDevNotifications 14 }

cabhPsDevProvEnrollTrap NOTIFICATION-TYPE
    OBJECTS {
        cabhPsDevHardwareVersion,
        docsDevSwCurrentVers,
        cabhPsDevTypeIdentifier,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "This notification is issued to initiate the CableHome
            provisioning process for SNMP Provisioning Mode."
    ::= { cabhPsDevNotifications 15 }

cabhPsDevCdpLanIpPoolTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        cabhCdpLanTransCurCount
    }
    STATUS      current
    DESCRIPTION
            "An event to report that the pool of IP addresses for LAN
            clients, as defined by cabh CdpLanPoolStart and
            cabhCdpLanPoolEnd, is exhausted."
    ::= { cabhPsDevNotifications 16 }

cabhPsDevUpnpMultiplePHTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhQos2NumActivePolicyHolder,
        cabhQos2PolicyHolderEnabled,
        cabhQos2PolicyAdmissionControl
    }
    STATUS      current
    DESCRIPTION
```

```
            "To report that more than one active UPnP Policy Holders
            have been detected.
            This notification is triggered in the case the PS
            has cabhPsDevUpnpEnabled true."
    ::= { cabhPsDevNotifications 17 }

-- compliance statements

cabhPsBasicCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for devices that implement the
            CableHome Portal Services logical element."
    MODULE   -- cabhPsMib

-- unconditionally mandatory groups

MANDATORY-GROUPS {
        cabhPsDevBaseGroup,
        cabhPsDevProvGroup,
        cabhPsNotificationGroup,
        cabhPsDevAttribGroup,
        cabhPsDevStatsGroup,
        cabhPsDevAccessControlGroup,
        cabhPsDevUpnpGroup
        }

--  conditionally mandatory groups

GROUP cabhPsDev802dot11Group
    DESCRIPTION
            "This group is implemented only if PS
            supports interfaces of ifType ieee80211(71)."

GROUP cabhPsDevUIGroup
    DESCRIPTION
            "This group is implemented only in CableHome compliant
            residential gateways that implement a User Interface (UI)."

OBJECT cabhPsDevTimeServerAddrType
    SYNTAX      InetAddressType { ipv4(1) }
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses. "

OBJECT cabhPsDevTimeServerAddr
    SYNTAX      InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

OBJECT cabhPsDevLanIpTrafficInetAddress
    SYNTAX      InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

OBJECT cabhPsDevUpnpCommandIpType
    SYNTAX      InetAddressType { ipv4(1) }
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

OBJECT cabhPsDevUpnpCommandIp
```

```
    SYNTAX      InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."


OBJECT cabhPsDevUpnpInfoIpType
    SYNTAX      InetAddressType { ipv4(1) }
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses. "

OBJECT cabhPsDevUpnpInfoIp
    SYNTAX      InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

    ::= { cabhPsCompliances 1 }

cabhPsDeprecatedCompliance MODULE-COMPLIANCE
    STATUS      deprecated
    DESCRIPTION
            "The compliance statement for deprecated MIB objects."
    MODULE   -- cabhPsMib

-- deprecated groups

GROUP cabhPsDevDeprecatedGroup
    DESCRIPTION
            "Group containing deprecated MIB objects."
    ::= { cabhPsCompliances 2 }

cabhPsObsoleteCompliance MODULE-COMPLIANCE
    STATUS      obsolete
    DESCRIPTION
            "The compliance statement for obsolete MIB objects."
    MODULE   -- cabhPsMib

GROUP cabhPsDevObsoleteGroup
    DESCRIPTION
            "Group containing obsolete MIB objects."

    ::= { cabhPsCompliances 3 }

cabhPsDevBaseGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevDateTime,
        cabhPsDevResetNow,
        cabhPsDevSerialNumber,
        cabhPsDevHardwareVersion,
        cabhPsDevWanManMacAddress,
        cabhPsDevWanDataMacAddress,
        cabhPsDevTypeIdentifier,
        cabhPsDevSetToFactory,
        cabhPsDevTodSyncStatus,
        cabhPsDevProvMode,
        cabhPsDevLastSetToFactory,
        cabhPsDevTrapControl
    }
    STATUS      current
    DESCRIPTION
            "A collection of objects for providing device status and
            control."
```

```
    ::= { cabhPsGroups 1 }

cabhPsDevProvGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevProvisioningTimer,
        cabhPsDevProvConfigFile,
        cabhPsDevProvConfigHash,
        cabhPsDevProvConfigFileSize,
        cabhPsDevProvConfigFileStatus,
        cabhPsDevProvConfigTLVProcessed,
        cabhPsDevProvConfigTLVRejected,
        cabhPsDevProvSolicitedKeyTimeout,
        cabhPsDevProvState,
        cabhPsDevProvAuthState,
        cabhPsDevTimeServerAddrType,
        cabhPsDevTimeServerAddr
    }
    STATUS      current
    DESCRIPTION
            "A collection of objects for controlling and providing
            status on provisioning."
    ::= { cabhPsGroups 2 }

cabhPsDevAttribGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevPsDeviceType,
        cabhPsDevPsManufacturerUrl,
        cabhPsDevPsModelUrl,
        cabhPsDevPsModelUpc
    }
    STATUS      current
    DESCRIPTION
            "A collection of objects for providing information on
            LAN IP devices known to the PS."
    ::= { cabhPsGroups 3 }

cabhPsDevStatsGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevLanIpTrafficCountersReset,
        cabhPsDevLanIpTrafficCountersLastReset,
        cabhPsDevLanIpTrafficEnabled,
        cabhPsDevLanIpTrafficInetAddressType,
        cabhPsDevLanIpTrafficInetAddress,
        cabhPsDevLanIpTrafficInOctets,
        cabhPsDevLanIpTrafficOutOctets
    }
    STATUS      current
    DESCRIPTION
            "A collection of objects for providing information
            on LAN IP traffic."
    ::= { cabhPsGroups 4 }

cabhPsDevDeprecatedGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevWanManClientId,
        cabhPsDevProvCorrelationId
    }
    STATUS      deprecated
    DESCRIPTION
            "Group of deprecated PSDev MIB objects."
    ::= { cabhPsGroups 5 }

cabhPsNotificationGroup NOTIFICATION-GROUP
    NOTIFICATIONS {
```

```
        cabhPsDevInitTLVUnknownTrap,
        cabhPsDevInitTrap,
        cabhPsDevInitRetryTrap,
        cabhPsDevDHCPFailTrap,
        cabhPsDevSwUpgradeInitTrap,
        cabhPsDevSwUpgradeFailTrap,
        cabhPsDevSwUpgradeSuccessTrap,
        cabhPsDevSwUpgradeCVCFailTrap,
        cabhPsDevTODFailTrap,
        cabhPsDevCdpWanDataIpTrap,
        cabhPsDevCdpThresholdTrap,
        cabhPsDevCspTrap,
        cabhPsDevCapTrap,
        cabhPsDevCtpTrap,
        cabhPsDevProvEnrollTrap,
        cabhPsDevCdpLanIpPoolTrap,
        cabhPsDevUpnpMultiplePHTrap
    }
    STATUS      current
    DESCRIPTION
            "These notifications indicate change in status of the
            Portal Services set of functions in a device complying
            with ITU-T Rec. J.192."
    ::= { cabhPsGroups 6 }

cabhPsDevAccessControlGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevAccessControlEnable,
        cabhPsDevAccessControlPhysAddr,
        cabhPsDevAccessControlRowStatus
    }
    STATUS      current
    DESCRIPTION
            "Group of Access Control objects for the CableHome PSDev
            MIB."
    ::= { cabhPsGroups 7 }

cabhPsDevUIGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevUILogin,
        cabhPsDevUIPassword,
        cabhPsDevUISelection,
        cabhPsDevUIServerUrl,
        cabhPsDevUISelectionDisabledBodyText
    }
    STATUS      current
    DESCRIPTION
            "A collection of objects for configuring the selection and
            operation of the User Interface displayed to an HTTP
            client, if a UI is implemented."
    ::= { cabhPsGroups 8 }

cabhPsDev802dot11Group OBJECT-GROUP
    OBJECTS {
               cabhPsDev802dot11BaseSetToDefault,
               cabhPsDev802dot11BaseLastSetToDefault,
               cabhPsDev802dot11BaseAdvertiseSSID,
               cabhPsDev802dot11BasePhyCapabilities,
               cabhPsDev802dot11BasePhyOperMode,
               cabhPsDev802dot11SecCapabilities,
               cabhPsDev802dot11SecOperMode,
               cabhPsDev802dot11SecPassPhraseToWEPKey,
               cabhPsDev802dot11SecUsePassPhraseToWEPKeyAlg,
               cabhPsDev802dot11SecPSKPassPhraseToKey,
```

```
                cabhPsDev802dot11SecWPAPreSharedKey,
                cabhPsDev802dot11SecWPARekeyTime,
                cabhPsDev802dot11SecControl,
                cabhPsDev802dot11SecCommitStatus
              }
    STATUS      current
    DESCRIPTION
            "Group of CableHome proprietary objects for the
            management of IEEE 80211 interfaces."
    ::= { cabhPsGroups 9 }

cabhPsDevUpnpGroup OBJECT-GROUP
    OBJECTS {
                cabhPsDevUpnpEnabled,
                cabhPsDevUpnpCommandIpType,
                cabhPsDevUpnpCommandIp,
                cabhPsDevUpnpCommand,
                cabhPsDevUpnpCommandUpdate,
                cabhPsDevUpnpLastCommandUpdate,
                cabhPsDevUpnpCommandStatus,
                cabhPsDevUpnpInfoXmlFragment
              }
    STATUS      current
    DESCRIPTION
            "Group of MIB objects for the
            management interface of UPnP Services."
    ::= { cabhPsGroups 10 }

cabhPsDevObsoleteGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevBpDeviceType,
        cabhPsDevBpManufacturer,
        cabhPsDevBpManufacturerUrl,
        cabhPsDevBpSerialNumber,
        cabhPsDevBpHardwareVersion,
        cabhPsDevBpHardwareOptions,
        cabhPsDevBpModelName,
        cabhPsDevBpModelNumber,
        cabhPsDevBpModelUrl,
        cabhPsDevBpModelUpc,
        cabhPsDevBpModelSoftwareOs,
        cabhPsDevBpModelSoftwareVersion,
        cabhPsDevBpLanInterfaceType,
        cabhPsDevBpNumberInterfacePriorities,
        cabhPsDevBpPhysicalLocation,
        cabhPsDevBpPhysicalAddress
    }
    STATUS      obsolete
    DESCRIPTION
            "Group of BP related objects with obsoleted status."
    ::= { cabhPsGroups 11 }

END
```

E.5 IPCable2Home Security (SEC) MIB requirement

The CableHome™ SEC MIB MUST be implemented as defined below.

```
CABH-SEC-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    Unsigned32,
    zeroDotZero,
```

```
    Counter32,
    OBJECT-TYPE                FROM SNMPv2-SMI  -- RFC 2578

    DateAndTime,
    TruthValue,
    TimeStamp,
    RowStatus,
    VariablePointer            FROM SNMPv2-TC  -- RFC 2579

    OBJECT-GROUP,
    MODULE-COMPLIANCE          FROM SNMPv2-CONF -- RFC 2580
    InetPortNumber,
    InetAddress                FROM INET-ADDRESS-MIB -- RFC 3291

    SnmpAdminString            FROM SNMP-FRAMEWORK-MIB -- RFC 2571

    X509Certificate            FROM DOCS-BPI2-MIB

    ZeroBasedCounter32         FROM RMON2-MIB
    docsDevFilterIpEntry       FROM DOCS-CABLE-DEVICE-MIB
    InterfaceIndexOrZero       FROM IF-MIB

    clabProjCableHome          FROM CLAB-DEF-MIB;

    cabhSecMib MODULE-IDENTITY
    LAST-UPDATED    "200408060000Z" -- August 6, 2004
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
            858 Coal Creek Circle
            Louisville, Colorado 80027
            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com; mibs@cablelabs.com"
    DESCRIPTION
            "This MIB module supplies the basic management
            objects for the Security Portal Services."
    ::=  { clabProjCableHome 2 }


-- Textual conventions

   cabhSecMibObjects  OBJECT IDENTIFIER ::= { cabhSecMib 5 }
   cabhSecFwObjects   OBJECT IDENTIFIER ::= { cabhSecMib 1 }
   cabhSecFwBase      OBJECT IDENTIFIER ::= { cabhSecFwObjects 1 }
   cabhSecFwLogCtl    OBJECT IDENTIFIER ::= { cabhSecFwObjects 2 }

   cabhSecCertObjects OBJECT IDENTIFIER ::= { cabhSecMib 2 }
   cabhSecKerbObjects OBJECT IDENTIFIER ::= { cabhSecMibObjects 3 }
   cabhSecKerbBase    OBJECT IDENTIFIER ::= { cabhSecKerbObjects 1 }

   cabhSec2FwObjects  OBJECT IDENTIFIER ::= { cabhSecMibObjects 4 }
   cabhSec2FwBase     OBJECT IDENTIFIER ::= { cabhSec2FwObjects 1 }
   cabhSec2FwEvent    OBJECT IDENTIFIER ::= { cabhSec2FwObjects 2 }
   cabhSec2FwLog      OBJECT IDENTIFIER ::= { cabhSec2FwObjects 3 }
   cabhSec2FwFilter   OBJECT IDENTIFIER ::= { cabhSec2FwObjects 4 }

--
--    CableHome 1.0 Base Firewall Functions
--

cabhSecFwPolicyFileEnable OBJECT-TYPE
```

```
    SYNTAX      INTEGER {
                    enable (1),
                    disable(2)
                }
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "This parameter indicates whether or not to enable
            the firewall functionality."
    DEFVAL { enable }
    ::= { cabhSecFwBase 1 }

cabhSecFwPolicyFileURL OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "A policy rule set file download is triggered when the
            value used to set this object is different than the value
            in the cabhSecFwPolicySuccessfulFileURL object."
    REFERENCE
            "CableHome 1.0 Specification, CH-SP-CH1.0-I05-030801,
            11.3.5.2 of ITU-T Rec. J.191, Firewall Rule Set Management
            Parameters."
    DEFVAL { "" }
    ::= { cabhSecFwBase 2 }

cabhSecFwPolicyFileHash OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0|20))
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "Hash of the contents of the rules set file,
            calculated and sent to the PS prior to sending
            the rules set file. For the SHA-1 authentication
            algorithm, the length of the hash is 160 bits.
            This hash value is encoded in binary format."
    DEFVAL { ''h }
    ::= { cabhSecFwBase 3 }

cabhSecFwPolicyFileOperStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                    inProgress(1),
                    complete(2),
                 -- completeFromMgt(3), deprecated
                    failed(4)
                }
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
            "inProgress(1) indicates a firewall configuration
            file download is under way.
            complete (2) indicates the firewall configuration
            file downloaded and configured successfully.
            completeFromMgt(3). This state is deprecated.
            failed(4) indicates the last attempted firewall
            configuration file download or processing
            failed ordinarily due to TFTP timeout."
    ::= { cabhSecFwBase 4 }

cabhSecFwPolicyFileCurrentVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      deprecated
```

```
    DESCRIPTION
            "The rule set version currently operating in the
            PS device. This object should be in the syntax
            used by the individual vendor to identify software
            versions. Any PS element MUST return a string
            descriptive of the current rule set file load.
            If this is not applicable, this object MUST
            contain an empty string."
    ::= { cabhSecFwBase 5 }

cabhSecFwPolicySuccessfulFileURL OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
            "Contains the location of the last successful downloaded
            policy rule set file in the format pointed in the
            reference. If a successful download has never occurred,
            this MIB object MUST report empty string."
    REFERENCE
            "CableHome 1.0 Specification, CH-SP-CH1.0-I05-030801,
            11.3.5.2 of ITU-T Rec. J.191, Firewall Rule Set Management
            Parameters."
    DEFVAL { "" }
    ::= { cabhSecFwBase 6 }

--
-- CableHome 1.0 Firewall Event MIBs
--

cabhSecFwEventType1Enable OBJECT-TYPE
    SYNTAX      INTEGER {
                    enable(1), -- log event
                    disable(2) -- do not log event
                }
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "This object enables or disables logging of type 1
            firewall event messages. Type 1 event messages report
            attempts from both private and public clients to
            traverse the firewall that violate the Security
            Policy."
    DEFVAL { disable }
    ::= { cabhSecFwLogCtl 1 }

cabhSecFwEventType2Enable OBJECT-TYPE
    SYNTAX      INTEGER {
                    enable(1), -- log event
                    disable(2) -- do not log event
                }
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "This object enables or disables logging of
            type 2 firewall event messages. Type 2 event
            messages report identified Denial of Service
            attack attempts."
    DEFVAL { disable }
    ::= { cabhSecFwLogCtl 2 }

cabhSecFwEventType3Enable OBJECT-TYPE
    SYNTAX      INTEGER {
                    enable(1), -- log event
```

```
                    disable(2) -- do not log event
                }
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "Enables or disables logging of type 3 firewall
            event messages. Type 3 event messages report
            changes made to the following firewall management
            parameters: cabhSecFwPolicyFileURL,
            cabhSecFwPolicyFileCurrentVersion,
            cabhSecFwPolicyFileEnable"
    DEFVAL { disable }
    ::= { cabhSecFwLogCtl 3 }

cabhSecFwEventAttackAlertThreshold OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "If the number of type 1 or 2 hacker attacks
            exceeds this threshold in the period defined
            by cabhSecFwEventAttackAlertPeriod, a firewall
            message event MUST be logged with priority
            level 4."
    DEFVAL { 65535 }
    ::= { cabhSecFwLogCtl 4 }

cabhSecFwEventAttackAlertPeriod OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "Indicates the period to be used (in hours) for
            the cabhSecFwEventAttackAlertThreshold. This MIB
            variable should always keep track of the last x
            hours of events meaning that if the variable is
            set to track events for 10 hours then, when the
            11th hour is reached, the 1st hour of events is
            deleted from the tracking log. A default value
            is set to zero, meaning zero time, so that this
            MIB variable will not track any events unless
            configured."
    DEFVAL { 0 }
    ::= { cabhSecFwLogCtl 5 }

--
-- CableHome PS device certificate
--

    cabhSecCertPsCert OBJECT-TYPE
    SYNTAX      X509Certificate
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The X509 DER-encoded PS certificate."
    ::= { cabhSecCertObjects 1 }

--
--  CableHome 1.1 Firewall Management MIBs
--

cabhSec2FwEnable OBJECT-TYPE
    SYNTAX      INTEGER    {
                    enabled(1),
```

```
                    disabled(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This parameter indicates whether to enable or disable the
            firewall."
    DEFVAL { enabled }
    ::= { cabhSec2FwBase 1 }

cabhSec2FwPolicyFileURL OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "A policy rule set file download is triggered when the
            value used to set this object is different than the value
            in the cabhSec2FwPolicySuccessfulFileURL object."
    REFERENCE
            "CableHome 1.1 Specification, CH-SP-CH1.1-I05-040806,
            11.6.4.9.1 of ITU-T Rec. J.192, Firewall Rule Set Management
            MIB Objects."
    DEFVAL { "" }
    ::= { cabhSec2FwBase 2 }

cabhSec2FwPolicyFileHash OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0|20))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Hash of the contents of the firewall
            configuration file. For the SHA-1 authentication
            algorithm, the length of the hash is 160 bits.
            This hash value is encoded in binary format."
    DEFVAL { ''h }
    ::= { cabhSec2FwBase 3 }

cabhSec2FwPolicyFileOperStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                    inProgress(1),
                    complete(2),
                    failed(3)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "InProgress(1) indicates a firewall configuration
            file download is under way. Complete(2) indicates
            the firewall configuration file was downloaded
            and processed successfully. Failed(3) indicates
            that the last attempted firewall configuration
            file download or processing failed."
    ::= { cabhSec2FwBase 4 }

cabhSec2FwPolicyFileCurrentVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "A label set by the cable operator that can be
            used to track various versions of configured
            rulesets. Once the label is set and configured
            rules are changed, it may not accurately reflect
            the version of configured rules running on the box.
```

```
            If this object has never been configured, it MUST
            contain an empty string."
    DEFVAL { "" }
    ::= { cabhSec2FwBase 5 }

cabhSec2FwClearPreviousRuleset OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "If set to 'true', the PS MUST clear all entries in the
            docsDevFilterIpTable. Reading this value always returns
            false."
    REFERENCE
            "CableHome specification - Security section"
    DEFVAL { false }
    ::= { cabhSec2FwBase 6 }

cabhSec2FwPolicySelection OBJECT-TYPE
    SYNTAX      INTEGER {
                    factoryDefault(1),
                    configuredRulesetBoth(2),
                    factoryDefaultAndConfiguredRulesetBoth(3),
                    configuredRulesetDocsDevFilterIpTable(4),
                    configuredRulesetCabhSec2FwLocalFilterIpTable (5),
                    factoryDefaultAndDocsDevFilterIpTable (6),
                    factoryDefaultAndCabhSec2FwLocalFilterIpTable (7)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object allows for selection of the filtering policy
            as defined by the following options:

            factoryDefault (1) The firewall filters against the Factory
            Default Ruleset in the cabhSec2FwFactoryDefaultFilterTable.

            configuredRulesetBoth (2) The firewall filters against the
            Configured Ruleset defined by both the
            docsDevFilterIpTable and the cabhSec2FwLocalFilterIpTable.

            factoryDefaultAndConfiguredRulesetBoth (3) The firewall
            filters against the CableHome specified Factory Default
            Ruleset in the cabhSec2FwFactoryDefaultFilterTable and
            the Configured Ruleset in the docsDevFilterIpTable and
            the cabhSec2FwLocalFilterIpTable.

            configuredRulesetDocsDevFilterIpTable(4) The firewall
            filters against the Configured Ruleset defined by the
            docsDevFilterIpTable.

            configuredRulesetCabhSec2FwLocalFilterIpTable (5) The
            firewall filters against the Configured Ruleset defined by
            the cabhSec2FwLocalFilterIpTable.

            factoryDefaultAndDocsDevFilterIpTable (6) The firewall
            filters against the Factory Default Ruleset and the
            Configured Ruleset defined by the DocsDevFilterIpTable.

            factoryDefaultAndCabhSec2FwLocalFilterIpTable (7) The
            firewall filters against the Factory Default Ruleset and
            the Configured Ruleset defined by the
            cabhSec2FwLocalFilterIpTable."
```

```
    REFERENCE
            "CableHome specification - Security section."
    DEFVAL { factoryDefault }
    ::= { cabhSec2FwBase 7 }

cabhSec2FwEventSetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "If set to 'true', entries in cabhSec2FwEventControlEntry
            are set to their default values.
            Reading this value always returns false."
    DEFVAL { false }
    ::= { cabhSec2FwBase 8 }

cabhSec2FwEventLastSetToFactory OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when cabhSec2FwEventSetToFactory
            was Last set to true. Zero if never reset."
    ::= { cabhSec2FwBase 9 }

cabhSec2FwPolicySuccessfulFileURL OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Contains the location of the last successful downloaded
            policy rule set file in the format pointed in the
            reference. If a successful download has not yet
            occurred, this MIB object should report empty string."
    REFERENCE
            "CableHome 1.1 Specification, CH-SP-CH1.1-I05-040806,
            11.6.4.9.1 of ITU-T Rec. J.192, Firewall Rule Set Management MIB
Objects."
    DEFVAL { "" }
    ::= { cabhSec2FwBase 10 }

cabhSec2FwConfiguredRulesetPriority OBJECT-TYPE
    SYNTAX      INTEGER {
                    docsDevFilterIpTable (1),
                    cabhSec2FwLocalFilterIpTable (2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object defines which Configured Ruleset filter rule
             has priority when a conflict exists between a filter rule
             in the docsDevFilterIpTable and a filter rule in the
             cabhSec2FwLocalFilterIpTable as indicated by the following
             options:

             docsDevFilterIpTable (1) - indicates that filter rules in
             the docsDevFilterIpTable have priority over any
             conflicting filters that may exist in the
             cabhSec2FwLocalFilterIpTable.

             cabhSec2FwLocalFilterIpTable (2) - indicates that filter
             rules in the cabhSec2FwLocalFilterIpTable have priority
             over any conflicting filters that may exist in the
             docsDevFilterIpTable."
```

```
    REFERENCE
             "CableHome specification - Security section."
    DEFVAL { cabhSec2FwLocalFilterIpTable }
    ::= { cabhSec2FwBase 11 }

cabhSec2FwClearLocalRuleset OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "If set to 'true', the PS MUST clear all entries in the
            cabhSec2FwLocalFilterIpTable. Reading this value always
            returns false."
    REFERENCE
            "CableHome specification - Security section"
    DEFVAL { false }
    ::= { cabhSec2FwBase 12 }

-- ++++++++++

--
-- CableHome 1.1 Firewall Event MIBs
--


cabhSec2FwEventControlTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhSec2FwEventControlEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table controls the reporting of the
            Firewall Attacks events"
    ::= { cabhSec2FwEvent 1 }

cabhSec2FwEventControlEntry OBJECT-TYPE
    SYNTAX      CabhSec2FwEventControlEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Allows configuration of the reporting mechanisms
            for a particular type of attack."
    INDEX { cabhSec2FwEventType }
    ::= { cabhSec2FwEventControlTable 1 }

CabhSec2FwEventControlEntry ::= SEQUENCE {
    cabhSec2FwEventType         INTEGER,
    cabhSec2FwEventEnable       INTEGER,
    cabhSec2FwEventThreshold    Unsigned32,
    cabhSec2FwEventInterval     Unsigned32,
    cabhSec2FwEventCount        ZeroBasedCounter32,
    cabhSec2FwEventLogReset     TruthValue,
    cabhSec2FwEventLogLastReset TimeStamp
    }

cabhSec2FwEventType OBJECT-TYPE
    SYNTAX      INTEGER     {
                    type1(1),
                    type2(2),
                    type3(3),
                    type4(4),
                    type5(5),
                    type6(6)
                }
    MAX-ACCESS  not-accessible
```

```
    STATUS      current
    DESCRIPTION
            "Classification of the different types of
            attacks.
            Type 1  logs all attempts from both LAN and WAN
            clients to traverse the Firewall that violate the
            Security Policy.
            Type 2 logs identified Denial of Service attack
            attempts.
            Type 3 logs all changes made to the
            cabhSec2FwPolicyFileURL,
            cabhSec2FwPolicyFileCurrentVersion or
            cabhSec2FwPolicyFileEnable objects.
            Type 4 logs all failed attempts to modify
            cabhSec2FwPolicyFileURL and
            cabhSec2FwPolicyFileEnable objects.
            Type 5 logs allowed inbound packets from the WAN.
            Type 6 logs allowed outbound packets from the
            LAN."
    ::= { cabhSec2FwEventControlEntry 1 }

cabhSec2FwEventEnable OBJECT-TYPE
    SYNTAX      INTEGER    {
                    enabled(1),
                    disabled(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Enables or disables counting and logging of
            firewall events by type as assigned by
            cabhSec2FwEventType."
    DEFVAL { disabled }
    ::= { cabhSec2FwEventControlEntry 2 }

cabhSec2FwEventThreshold OBJECT-TYPE
    SYNTAX       Unsigned32 (0..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
            "Number of attacks to count before sending the
            appropriate event by type as assigned by
            cabhSec2FwEventType."
    DEFVAL { 0 }
    ::= { cabhSec2FwEventControlEntry 3 }

cabhSec2FwEventInterval OBJECT-TYPE
    SYNTAX      Unsigned32 (0..744)
    UNITS       "hours"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Indicates the time interval in hours to count and log
            occurrences of a firewall event type as assigned in
            cabhSec2FwEventType. If this MIB has a value of zero,
            then there is no interval assigned and the PS will not
            count or log events."
    DEFVAL { 0 }
    ::= { cabhSec2FwEventControlEntry 4 }

cabhSec2FwEventCount OBJECT-TYPE
    SYNTAX       ZeroBasedCounter32
    MAX-ACCESS   read-only
    STATUS       current
```

```
    DESCRIPTION
           "Indicates the current count up to the
            cabhSec2FwEventThreshold value by type as
            assigned by cabhSec2FwEventType."
    ::= { cabhSec2FwEventControlEntry 5 }

cabhSec2FwEventLogReset OBJECT-TYPE
    SYNTAX       TruthValue
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
            "Setting this object to true clears the log table
            for the specified event type. Reading this object
            always returns false."
    DEFVAL { false }
    ::= { cabhSec2FwEventControlEntry 6 }

cabhSec2FwEventLogLastReset OBJECT-TYPE
    SYNTAX       TimeStamp
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
            "The value of sysUpTime when cabhSec2FwEventLogReset was
            last set to true. Zero if never reset."
    ::= { cabhSec2FwEventControlEntry 7 }

--
-- CableHome 1.1 Firewall Log Tables
--

cabhSec2FwLogTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhSec2FwLogEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Contains a log of packet information as related
            to events enabled by the cable operator. The types
            are defined in the CableHome 1.1 specification and
            require various objects to be included in the log.
            The following is a description for what is
            expected in the log for each type Type 1, Type 2,
            Type 5 and Type 6 table MUST include
            cabhSec2FwEventType, cabhSec2FwEventPriority,
            cabhSec2FwEventId, cabhSec2FwLogTime,
            cabhSec2FwIpProtocol, cabhSec2FwIpSourceAddr,
            cabhSec2FwIpDestAddr, cabhSec2FwIpSourcePort,
            cabhSec2FwIpDestPort, cabhSec2Fw,
            cabhSec2FwReplayCount.  The other values not used
            by Types 1, 2, 5 and 6 are default values. Type 3
            and Type 4 MUST include cabhSec2FwEventType,
            cabhSec2FwEventPriority, cabhSec2FwEventId,
            cabhSec2FwLogTime, cabhSec2FwIpSourceAddr,
            cabhSec2FwLogMIBPointer.  The other values not used
            by type 3 and 4 are default values. When applicable,
            Type 1, Type 5,and Type 6 MUST also include
            cabhSec2FwLogMatchingFilterTableName,
            cabhSec2FwLogMatchingFilterTableIndex,
            cabhSec2FwLogMatchingFilterDescr."
    ::= { cabhSec2FwLog 1 }

cabhSec2FwLogEntry OBJECT-TYPE
    SYNTAX      CabhSec2FwLogEntry
    MAX-ACCESS  not-accessible
    STATUS      current
```

```
    DESCRIPTION
            "Each entry contains the log of firewall events"
    INDEX {cabhSec2FwLogIndex}
    ::= { cabhSec2FwLogTable 1 }

CabhSec2FwLogEntry ::= SEQUENCE {
    cabhSec2FwLogIndex                      Unsigned32,
    cabhSec2FwLogEventType                  INTEGER,
    cabhSec2FwLogEventPriority              INTEGER,
    cabhSec2FwLogEventId                    Unsigned32,
    cabhSec2FwLogTime                       DateAndTime,
    cabhSec2FwLogIpProtocol                 Unsigned32,
    cabhSec2FwLogIpSourceAddr               InetAddress,
    cabhSec2FwLogIpDestAddr                 InetAddress,
    cabhSec2FwLogIpSourcePort               InetPortNumber,
    cabhSec2FwLogIpDestPort                 InetPortNumber,
    cabhSec2FwLogMessageType                Unsigned32,
    cabhSec2FwLogReplayCount                Unsigned32,
    cabhSec2FwLogMIBPointer                 VariablePointer,
    cabhSec2FwLogMatchingFilterTableName    INTEGER,
    cabhSec2FwLogMatchingFilterTableIndex   Unsigned32,
    cabhSec2FwLogMatchingFilterDescr        SnmpAdminString
    }

cabhSec2FwLogIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..2147483647)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "A sequence number for the specific events
            under a cabhSec2FwEventType."
    ::= { cabhSec2FwLogEntry 1 }

cabhSec2FwLogEventType OBJECT-TYPE
    SYNTAX INTEGER     {
               type1(1),
               type2(2),
               type3(3),
               type4(4),
               type5(5),
               type6(6)
           }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Classification of the different types of
            attacks.
            Type 1 logs all attempts from both LAN and WAN
            clients to traverse the Firewall that violate
            the Security Policy.
            Type 2 logs identified Denial of Service attack
            attempts.
            Type 3 logs all changes made to the
            cabhSec2FwPolicyFileURL,
            cabhSec2FwPolicyFileCurrentVersion or
            cabhSec2FwPolicyFileEnable objects.
            Type 4 logs all failed attempts to modify
            cabhSec2FwPolicyFileURL and
            cabhSec2FwPolicyFileEnable objects.
            Type 5 logs allowed inbound packets from the WAN.
            Type 6 logs allowed outbound packets from the
            LAN."
    ::= { cabhSec2FwLogEntry 2 }
```

```
cabhSec2FwLogEventPriority OBJECT-TYPE
    SYNTAX     INTEGER     {
                   emergency(1),
                   alert(2),
                   critical(3),
                   error(4),
                   warning(5),
                   notice(6),
                   information(7),
                   debug(8)
               }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The priority level of this event as defined
            by CableHome Specification. If a priority is
            not assigned in the CableHome specification for
            a particular event, then the vendor or cable
            operator may assign priorities. These are
            ordered from most serious (emergency)to least
            serious (debug)."
    ::= { cabhSec2FwLogEntry 3 }

cabhSec2FwLogEventId  OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The assigned event ID."
    ::= { cabhSec2FwLogEntry 4 }

cabhSec2FwLogTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The time that this entry was created by the PS."
    ::= { cabhSec2FwLogEntry 5 }

cabhSec2FwLogIpProtocol OBJECT-TYPE
    SYNTAX      Unsigned32 (0..256)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP Protocol."
    ::= { cabhSec2FwLogEntry 6 }

cabhSec2FwLogIpSourceAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The Source IP Address of the packet logged."
    ::= { cabhSec2FwLogEntry 7 }

cabhSec2FwLogIpDestAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The Destination IP Address of the packet logged."
    ::= { cabhSec2FwLogEntry 8 }

cabhSec2FwLogIpSourcePort OBJECT-TYPE
```

```
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The Source IP Port of the packet logged."
    ::= { cabhSec2FwLogEntry 9 }

cabhSec2FwLogIpDestPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The Source IP Port of the packet logged."
    ::= { cabhSec2FwLogEntry 10 }

cabhSec2FwLogMessageType OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The ICMP defined types."
    ::= { cabhSec2FwLogEntry 11}

cabhSec2FwLogReplayCount OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of identical attack packets that
            were seen by the firewall based on
            cabhSec2FwLogIpProtocol, cabhSec2FwLogIpSourceAddr,
            cabhSec2FwLogIpDestAddr, cabhSec2FwLogIpSourcePort,
            cabhSec2FwLogIpDestPort and cabhSec2FwLogMessageType."
    DEFVAL { 0 }
    ::= { cabhSec2FwLogEntry 12 }

cabhSec2FwLogMIBPointer OBJECT-TYPE
    SYNTAX      VariablePointer
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Identifies if the cabhSec2FwPolicyFileURL or the
            cabhSec2FwEnable MIB object changed or an attempt
            was made to change it."
    DEFVAL { zeroDotZero }
    ::= { cabhSec2FwLogEntry 13 }

cabhSec2FwLogMatchingFilterTableName OBJECT-TYPE
    SYNTAX      INTEGER     {
                   cabhSec2FwFactoryDefaultFilterTable(1),
                   docsDevFilterIpTable(2),
                   cabhSec2FwLocalFilterIpTable(3),
                   none(4)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "When applicable, cabhSec2FwLogMatchingFilterTableName
            indicates the filter table name containing the last filter
            rule matched that caused the event to be generated."
    DEFVAL { none }
    ::= { cabhSec2FwLogEntry 14 }

cabhSec2FwLogMatchingFilterTableIndex OBJECT-TYPE
```

```
    SYNTAX      Unsigned32 (0..2147483647)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "When applicable, cabhSec2FwLogMatchingFilterTableIndex
            indicates the filter table index if the last filter
            rule matched that caused the event to be generated. If
            the value is 0, the event was not caused by a filter
            rule match. "
    DEFVAL { 0 }
    ::= { cabhSec2FwLogEntry 15 }

cabhSec2FwLogMatchingFilterDescr OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "When applicable, cabhSec2FwLogMatchingFilterDesc
            contains the description value found in the
            cabhSec2FwFilterScheduleDesc MIB object or the
            cabhSec2FwLocalFilterIpDesc MIB object of the last
            filter rule matched that caused the event to be
            generated."
    DEFVAL { "" }
    ::= { cabhSec2FwLogEntry 16 }

-- ============================================================
--
--  CableHome 1.1 PS IP Filter Scheduling Table
--
--  The cabhSec2FwFilterScheduleTable contains the firewall
--  policy identification and links that policy as defined
--  in RFC 2669 to specific time of day restrictions.
--
-- ============================================================

cabhSec2FwFilterScheduleTable OBJECT-TYPE
    SYNTAX SEQUENCE OF CabhSec2FwFilterScheduleEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Extends the filtering matching parameters of
            docsDevFilterIpTable defined in RFC 2669 for CableHome
            Residential Gateways to include time day intervals and days
            of the week."
    ::= { cabhSec2FwFilter 1 }


cabhSec2FwFilterScheduleEntry OBJECT-TYPE
    SYNTAX      CabhSec2FwFilterScheduleEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Extended values for entries of docsDevFilterIpTable.
            If the PS has not acquired ToD, the entire
            docsDevFilterIpEntry rule set is ignored.
            Note - A filter time period may include two days
            (e.g., from 10 PM to 4 AM).  A filter time period that
            includes two days is identified by the absolute value
            of the cabhSec2FwFilterScheduleEndTime being less than the
            absolute value of the cabhSec2FwFilterScheduleStartTime.
            The cabhSec2FwFilterScheduleDOW setting and the
            cabhSec2FwFilterScheduleStartTime value indicate what day
            and time the filter becomes active. The
```

```
            cabhSec2FwFilterScheduleEndTime indicates when the filter
            becomes inactive on the second day. The maximum filter
            time period that includes two days is 24 hours.
            If cabhSec2FwFilterScheduleStartTime is less than or
            equal to the cabhSec2FwFilterScheduleEndTime, the time
            period of the filter falls in the same day."
    AUGMENTS { docsDevFilterIpEntry }
    ::= { cabhSec2FwFilterScheduleTable 1 }

CabhSec2FwFilterScheduleEntry ::= SEQUENCE {
    cabhSec2FwFilterScheduleStartTime    Unsigned32,
    cabhSec2FwFilterScheduleEndTime      Unsigned32,
    cabhSec2FwFilterScheduleDOW          BITS,
    cabhSec2FwFilterScheduleDescr        SnmpAdminString
    }

cabhSec2FwFilterScheduleStartTime OBJECT-TYPE
    SYNTAX      Unsigned32 (0..2359)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The start time for matching the filter ruleset in the
            specified days indicated in cabhSec2FwFilterScheduleDOW.
            Time is represented in Military Time, e.g., 8:30 AM is
            represented as 830 and 11:45 PM as 2345. An attempt to set
            this object to an invalid military time value, e.g., 1182,
            returns 'wrongValue' error."
    DEFVAL { 0 }
    ::= { cabhSec2FwFilterScheduleEntry 1 }

cabhSec2FwFilterScheduleEndTime OBJECT-TYPE
    SYNTAX      Unsigned32 (0..2359)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The end time for matching the filter rule for the
            days indicated in cabhSec2FwFilterScheduleDOW. The filter
            rule associated with this end time MUST not be disabled
            until the minute following the time indicated by this
            MIB object. If the time period is for two days,
            identified by cabhSec2FwFilterScheduleEndTime being
            less than cabhSec2FwFilterScheduleStartTime, then
            the cabhSec2FwFilterScheduleDOW settings
            do not apply to this MIB object.
            Time is represented in the same manner as in
            cabhSec2FwFilterScheduleStartTime. An attempt to set
            this object to an invalid military time value, e.g., 1182,
            returns 'wrongValue' error."
    DEFVAL { 2359 }
    ::= { cabhSec2FwFilterScheduleEntry 2 }

cabhSec2FwFilterScheduleDOW OBJECT-TYPE
    SYNTAX BITS {
                    sunday(0),
                    monday(1),
                    tuesday(2),
                    wednesday(3),
                    thursday(4),
                    friday(5),
                    saturday(6)
                }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
```

```
            "If the day of week bit associated with the PS given day
            is '1', this object criteria matches."
    DEFVAL { 'fe'h }  -- 11111110 Sun-Sat
    ::= { cabhSec2FwFilterScheduleEntry 3 }

cabhSec2FwFilterScheduleDescr OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "A filter rule description configured by the
            cable operator or subscriber."
    DEFVAL { "" }
    ::= { cabhSec2FwFilterScheduleEntry 4 }

-- ============================================================
--
--  CableHome 1.1 PS Firewall Factory Default Filter Table
--
--  The cabhSec2FwFactoryDefaultFilterTable contains the
--  firewall factory default ruleset in a read only table as
--  defined by the CableLabs CableHome 1.1 Specification.
--
-- ============================================================

cabhSec2FwFactoryDefaultFilterTable OBJECT-TYPE
    SYNTAX SEQUENCE OF CabhSec2FwFactoryDefaultFilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Contains the firewall factory default ruleset as
            defined by the CableLabs CableHome 1.1 Specification."
    ::= { cabhSec2FwFilter 2 }

cabhSec2FwFactoryDefaultFilterEntry OBJECT-TYPE
    SYNTAX      CabhSec2FwFactoryDefaultFilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Contains the firewall factory default ruleset."
    INDEX {cabhSec2FwFactoryDefaultFilterIndex }
    ::= { cabhSec2FwFactoryDefaultFilterTable 1 }

CabhSec2FwFactoryDefaultFilterEntry ::= SEQUENCE {
    cabhSec2FwFactoryDefaultFilterIndex           Unsigned32,
    cabhSec2FwFactoryDefaultFilterControl         INTEGER,
    cabhSec2FwFactoryDefaultFilterIfIndex         InterfaceIndexOrZero,
    cabhSec2FwFactoryDefaultFilterDirection       INTEGER,
    cabhSec2FwFactoryDefaultFilterSaddr           InetAddress,
    cabhSec2FwFactoryDefaultFilterSmask           InetAddress,
    cabhSec2FwFactoryDefaultFilterDaddr           InetAddress,
    cabhSec2FwFactoryDefaultFilterDmask           InetAddress,
    cabhSec2FwFactoryDefaultFilterProtocol        Unsigned32,
    cabhSec2FwFactoryDefaultFilterSourcePortLow   Unsigned32,
    cabhSec2FwFactoryDefaultFilterSourcePortHigh  Unsigned32,
    cabhSec2FwFactoryDefaultFilterDestPortLow     Unsigned32,
    cabhSec2FwFactoryDefaultFilterDestPortHigh    Unsigned32,
    cabhSec2FwFactoryDefaultFilterContinue        TruthValue
}

cabhSec2FwFactoryDefaultFilterIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..2147483647)
    MAX-ACCESS  not-accessible
    STATUS      current
```

```
    DESCRIPTION
            "Index used to order the application of filters.
            The filter with the lowest index is always applied
            first."
    ::= { cabhSec2FwFactoryDefaultFilterEntry 1 }

cabhSec2FwFactoryDefaultFilterControl OBJECT-TYPE
    SYNTAX      INTEGER {
                    deny(1),
                    allow(2)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "If set to deny(1), all packets matching this filter
            will be discarded. If set to allow(2), all
            packets matching this filter will be accepted.
            The cabhSec2FwFactoryDefaultFilterContinue object is
            set to true, and therefore the PS MUST continue to
            scan the table for other matches to apply the match
            with the highest cabhSec2FwFactoryDefaultFilterIndex
            value."
    ::= { cabhSec2FwFactoryDefaultFilterEntry 2 }

cabhSec2FwFactoryDefaultFilterIfIndex OBJECT-TYPE
    SYNTAX      InterfaceIndexOrZero
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The index number assigned to this object MUST
            match the IfIndex numbering assigned in the
            ifTable from the Interfaces Group MIB [RFC 2863],
            and as specified in CH 1.1 Spec, Table 6-17 of
            ITU-T Rec. J.192, Numbering Interfaces in the
            ifTable. If the value is zero, the filter applies
            to all interfaces. This object MUST be specified
            to create a row in this table."
    ::= { cabhSec2FwFactoryDefaultFilterEntry 3 }

cabhSec2FwFactoryDefaultFilterDirection OBJECT-TYPE
    SYNTAX      INTEGER {
                    inbound(1),
                    outbound(2),
                    both(3)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This value represents direction in relationship
            to the assigned
            cabhSec2FwFactoryDefaultFilterIfIndex
            in this particular rule, meaning that the PS
            MUST represent traffic direction as follows:
            inbound(1)traffic, outbound(2) traffic, or
            both(3)inbound and outbound traffic."
    ::= { cabhSec2FwFactoryDefaultFilterEntry 4 }

cabhSec2FwFactoryDefaultFilterSaddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The source IP address, or portion thereof, that is
            to be matched for this filter. The source address
```

```
            is first masked (and'ed) against
            cabhSec2FwFactoryDefaultFilterSmask
            before being compared  to this value. A value of 0
            for this object and 0 for the mask matches all IP
            addresses."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 5 }

cabhSec2FwFactoryDefaultFilterSmask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A bit mask that is to be applied to the source
            address prior to matching. This mask is not
            necessarily the same as a subnet mask, but 1's
            bits must be leftmost and contiguous."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 6 }

cabhSec2FwFactoryDefaultFilterDaddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The destination IP address, or portion thereof, that
            is to be matched for this filter. The destination
            address is first masked (and'ed) against
            cabhSec2FwFactoryDefaultFilterDmask
            before being compared  to this value. A value of 0
            for this object and 0 for the mask matches all
            IP addresses."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 7 }

cabhSec2FwFactoryDefaultFilterDmask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A bit mask that is to be applied to the destination
            address prior to matching. This mask is not necessarily
            the same as a subnet mask, but 1's bits must be leftmost
            and contiguous."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 8 }

cabhSec2FwFactoryDefaultFilterProtocol OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The protocol value that is to be matched. For example:
            icmp is 1, tcp is 6, udp is 17. A value of 65535 matches
            ANY protocol."
    DEFVAL { 65535 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 9 }

cabhSec2FwFactoryDefaultFilterSourcePortLow OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwFactoryDefaultFilterProtocol is udp
```

```
            or tcp, this is the inclusive lower bound of the
            transport-layer source port range that is to be
            matched, otherwise it is ignored during matching."
    DEFVAL { 0 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 10 }

cabhSec2FwFactoryDefaultFilterSourcePortHigh OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwFactoryDefaultFilterProtocol is
            udp or tcp, this is the inclusive upper bound
            of the transport-layer source port range that
            is to be matched, otherwise it is ignored
            during matching."
    DEFVAL { 65535 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 11 }

cabhSec2FwFactoryDefaultFilterDestPortLow OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwFactoryDefaultFilterProtocol is
            udp or tcp, this is the inclusive lower bound
            of the transport-layer destination port range
            that is to be matched, otherwise it is ignored
            during matching."
    DEFVAL { 0 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 12 }

cabhSec2FwFactoryDefaultFilterDestPortHigh OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwFactoryDefaultFilterProtocol is
            udp or tcp, this is the inclusive upper bound
            of the transport-layer destination port range
            that is to be matched, otherwise it is ignored
            during matching."
    DEFVAL { 65535 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 13 }

cabhSec2FwFactoryDefaultFilterContinue OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This value is always set to true so the PS MUST continue
            scanning and applying rules."
    DEFVAL { true }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 14 }

-- ============================================================
--
--  CableHome 1.1 PS Firewall Local Filter Table
--
--  The cabhSec2FwLocalFilterIpTable can be configured to contain
--  a filtering Ruleset for the PS firewall.  It can be used to
--  support subscriber specific or local filtering rules that
--  are separate from general filtering rules that may be
--  be configured in the docsDevFilterIpTable.
```

```
-- ============================================================

cabhSec2FwLocalFilterIpTable OBJECT-TYPE
    SYNTAX SEQUENCE OF CabhSec2FwLocalFilterIpEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Contains a configured filtering Ruleset for the
            PS firewall."
    ::= { cabhSec2FwFilter 3 }

cabhSec2FwLocalFilterIpEntry OBJECT-TYPE
    SYNTAX      CabhSec2FwLocalFilterIpEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Contains a configured filter rule for the PS
            firewall.

            If the PS has not acquired ToD, entries that do not have
            default time settings are ignored.

            Note that a filter time period may include two days
            (e.g., from 10 PM to 4 AM).  A filter time period that
            includes two days is identified by the absolute value of
            the cabhSec2FwLocalFilterIpEndTime being less than the
            absolute value of the cabhSec2FwLocalFilterIpStartTime.
            The cabhSec2FwLocalFilterIpDOW setting and the
            cabhSec2FwLocalFilterIpStartTime value indicate what day
            and time the filter becomes active.  The
            cabhSec2FwLocalFilterIpEndTime indicates when the filter
            becomes inactive on the second day. The maximum filter time
            period that includes two days is 24 hours.

            If cabhSec2FwLocalFilterIpStartTime is less than or equal
            to the cabhSec2FwLocalFilterIpEndTime, the time period
            of the filter falls in the same day."

    INDEX { cabhSec2FwLocalFilterIpIndex }
    ::= { cabhSec2FwLocalFilterIpTable 1 }

CabhSec2FwLocalFilterIpEntry ::= SEQUENCE {
    cabhSec2FwLocalFilterIpIndex           Unsigned32,
    cabhSec2FwLocalFilterIpStatus          RowStatus,
    cabhSec2FwLocalFilterIpControl         INTEGER,
    cabhSec2FwLocalFilterIpIfIndex         InterfaceIndexOrZero,
    cabhSec2FwLocalFilterIpDirection       INTEGER,
    cabhSec2FwLocalFilterIpSaddr           InetAddress,
    cabhSec2FwLocalFilterIpSmask           InetAddress,
    cabhSec2FwLocalFilterIpDaddr           InetAddress,
    cabhSec2FwLocalFilterIpDmask           InetAddress,
    cabhSec2FwLocalFilterIpProtocol        Unsigned32,
    cabhSec2FwLocalFilterIpSourcePortLow   Unsigned32,
    cabhSec2FwLocalFilterIpSourcePortHigh  Unsigned32,
    cabhSec2FwLocalFilterIpDestPortLow     Unsigned32,
    cabhSec2FwLocalFilterIpDestPortHigh    Unsigned32,
    cabhSec2FwLocalFilterIpMatches         Counter32,
    cabhSec2FwLocalFilterIpContinue        TruthValue,
    cabhSec2FwLocalFilterIpStartTime       Unsigned32,
    cabhSec2FwLocalFilterIpEndTime         Unsigned32,
    cabhSec2FwLocalFilterIpDOW             BITS,
    cabhSec2FwLocalFilterIpDescr           SnmpAdminString
}
```

```
cabhSec2FwLocalFilterIpIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..2147483647)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Index used to order the application of filters.
            The filter with the lowest index is always applied
            first."
    ::= { cabhSec2FwLocalFilterIpEntry 1 }

cabhSec2FwLocalFilterIpStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Controls and reflects the status of rows in this
             table.  Creation of the
             rows may be done via either create-and-wait or
             create-and-go, but the filter is not applied until this
             object is set to (or changes to) active. There is no
             restriction in changing any object in a row while this
             object is set to active."
    ::= { cabhSec2FwLocalFilterIpEntry 2 }

cabhSec2FwLocalFilterIpControl OBJECT-TYPE
    SYNTAX      INTEGER {
                    deny(1),
                    allow(2)
                }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "If set to deny(1), all packets matching this filter
            will be discarded. If set to allow(2), all
            packets matching this filter will be accepted.
            The cabhSec2FwLocalFilterIpContinue object is
            set to true, and therefore the PS MUST continue to
            scan the table for other matches to apply the match
            with the highest cabhSec2FwLocalFilterIpIndex
            value."
    ::= { cabhSec2FwLocalFilterIpEntry 3 }

cabhSec2FwLocalFilterIpIfIndex OBJECT-TYPE
    SYNTAX      InterfaceIndexOrZero
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The index number assigned to this object MUST
            match the IfIndex numbering assigned in the
            ifTable from the Interfaces Group MIB [RFC 2863],
            and as specified in CH 1.1 Spec, Table 6-17 of
            ITU-T Rec. J.192, Numbering Interfaces in the ifTable."
    DEFVAL { 255 }
    ::= { cabhSec2FwLocalFilterIpEntry 4 }

cabhSec2FwLocalFilterIpDirection OBJECT-TYPE
    SYNTAX      INTEGER {
                    inbound(1),
                    outbound(2),
                    both(3)
                }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
```

```
            "This value represents direction in relationship
            to the assigned cabhSec2FwLocalFilterIpIfIndex
            in this particular rule, meaning that the PS
            MUST represent traffic direction as follows:
            inbound(1)traffic, outbound(2) traffic, or
            both(3)inbound and outbound traffic."
    ::= { cabhSec2FwLocalFilterIpEntry 5 }

cabhSec2FwLocalFilterIpSaddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The source IP address, or portion thereof, that is
            to be matched for this filter. The source address
            is first masked (and'ed) against
            cabhSec2FwLocalFilterIpSmask before being compared to this
            value. A value of 0 for this object and 0 for the mask
            matches all IP addresses."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwLocalFilterIpEntry 6 }

cabhSec2FwLocalFilterIpSmask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "A bit mask that is to be applied to the source
            address prior to matching. This mask is not
            necessarily the same as a subnet mask, but 1's
            bits must be leftmost and contiguous."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwLocalFilterIpEntry 7 }

cabhSec2FwLocalFilterIpDaddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The destination IP address, or portion thereof, that
            is to be matched for this filter. The destination
            address is first masked (and'ed) against
            cabhSec2FwLocalFilterIpDmask
            before being compared  to this value. A value of 0
            for this object and 0 for the mask matches all
            IP addresses."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwLocalFilterIpEntry 8 }

cabhSec2FwLocalFilterIpDmask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "A bit mask that is to be applied to the destination
            address prior to matching. This mask is not necessarily
            the same as a subnet mask, but 1's bits must be leftmost
            and contiguous."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwLocalFilterIpEntry 9 }

cabhSec2FwLocalFilterIpProtocol OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-create
```

```
    STATUS      current
    DESCRIPTION
            "The protocol value that is to be matched. For example:
            icmp is 1, tcp is 6, udp is 17. A value of 65535 matches
            ANY protocol."
    DEFVAL { 65535 }
    ::= { cabhSec2FwLocalFilterIpEntry 10 }

cabhSec2FwLocalFilterIpSourcePortLow OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwLocalFilterIpProtocol is udp
            or tcp, this is the inclusive lower bound of the
            transport-layer source port range that is to be
            matched, otherwise it is ignored during matching."
    DEFVAL { 0 }
    ::= { cabhSec2FwLocalFilterIpEntry 11 }

cabhSec2FwLocalFilterIpSourcePortHigh OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwLocalFilterIpProtocol is
            udp or tcp, this is the inclusive upper bound
            of the transport-layer source port range that
            is to be matched, otherwise it is ignored
            during matching."
    DEFVAL { 65535 }
    ::= { cabhSec2FwLocalFilterIpEntry 12 }

cabhSec2FwLocalFilterIpDestPortLow OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwLocalFilterIpProtocol is
            udp or tcp, this is the inclusive lower bound
            of the transport-layer destination port range
            that is to be matched, otherwise it is ignored
            during matching."
    DEFVAL { 0 }
    ::= { cabhSec2FwLocalFilterIpEntry 13 }

cabhSec2FwLocalFilterIpDestPortHigh OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwLocalFilterIpProtocol is
            udp or tcp, this is the inclusive upper bound
            of the transport-layer destination port range
            that is to be matched, otherwise it is ignored
            during matching."
    DEFVAL { 65535 }
    ::= { cabhSec2FwLocalFilterIpEntry 14 }

cabhSec2FwLocalFilterIpMatches OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
```

```
            "Counts the number of times this filter was matched.
             This object is initialized to 0 at boot, or at row
             creation, and is reset only upon reboot."
    ::= { cabhSec2FwLocalFilterIpEntry 15 }

cabhSec2FwLocalFilterIpContinue OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This value is always set to true so the PS MUST continue
            scanning and applying rules."
    DEFVAL { true }
    ::= { cabhSec2FwLocalFilterIpEntry 16 }

cabhSec2FwLocalFilterIpStartTime OBJECT-TYPE
    SYNTAX      Unsigned32 (0..2359)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The start time for matching the filter ruleset in the
            specified days indicated in cabhSec2FwLocalFilterIpDOW.
            Time is represented in Military Time, e.g., 8:30 AM is
            represented as 830 and 11:45 PM as 2345. An attempt to set
            this object to an invalid military time value, e.g., 1182,
            returns 'wrongValue' error."
    DEFVAL { 0 }
    ::= { cabhSec2FwLocalFilterIpEntry 17 }

cabhSec2FwLocalFilterIpEndTime OBJECT-TYPE
    SYNTAX      Unsigned32 (0..2359)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The end time for matching the filter ruleset for the
            days indicated in cabhSec2FwLocalFilterIpDOW.  The filter
            rule associated with this end time MUST not be disabled
            until the minute following the time indicated by this
            MIB object.  If the time period is for two days, identified
            by cabhSec2FwLocalFilterIpEndTime being less than
            cabhSec2FwLocalFilterIpStartTime, then the
            cabhSec2FwLocalFilterIpDOW settings do not apply to this
            MIB object. Time is represented in the same manner as in
            cabhSec2FwLocalFilterIpStartTime. An attempt to set
            this object to an invalid military time value, e.g., 1182,
            returns 'wrongValue' error."
    DEFVAL { 2359 }
    ::= { cabhSec2FwLocalFilterIpEntry 18 }

cabhSec2FwLocalFilterIpDOW OBJECT-TYPE
    SYNTAX BITS {
                    sunday(0),
                    monday(1),
                    tuesday(2),
                    wednesday(3),
                    thursday(4),
                    friday(5),
                    saturday(6)
                }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "If the day of week bit associated with the PS given day
            is '1', this object criteria matches."
```

```
    DEFVAL { 'fe'h }  -- 11111110 Sun-Sat
    ::= { cabhSec2FwLocalFilterIpEntry 19 }

cabhSec2FwLocalFilterIpDescr OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "A filter rule description configured by the
            cable operator or subscriber."
    DEFVAL { "" }
    ::= { cabhSec2FwLocalFilterIpEntry 20 }

--
-- Kerberos MIBs
--

cabhSecKerbPKINITGracePeriod OBJECT-TYPE
    SYNTAX      Unsigned32 (15..600)
    UNITS       "minutes"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PKINIT Grace Period is needed by the PS
            to know when it should start retrying to get
            a new ticket. The PS MUST obtain a new Kerberos
            ticket (with a PKINIT exchange),this, many minutes
            before the old ticket expires."
    DEFVAL { 30 }
    ::= { cabhSecKerbBase 1}

cabhSecKerbTGSGracePeriod OBJECT-TYPE
    SYNTAX      Unsigned32 (1..600)
    UNITS       "minutes"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The TGS Grace Period is needed by the PS to
            know when it should start retrying to get a new
            ticket. The PS MUST obtain a new Kerberos ticket
            (with a TGS Request), this, many minutes before the
            old ticket expires."
    DEFVAL { 10 }
    ::= { cabhSecKerbBase 2 }

cabhSecKerbUnsolicitedKeyMaxTimeout OBJECT-TYPE
    SYNTAX      Unsigned32 (15..600)
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This timeout applies to PS initiated AP-REQ/REP
            key management exchange with NMS. The maximum
            timeout is the value which may not be exceeded in
            the exponential backoff algorithm."
    DEFVAL { 600 }
    ::= { cabhSecKerbBase 3 }

cabhSecKerbUnsolicitedKeyMaxRetries OBJECT-TYPE
    SYNTAX      Unsigned32 (1..32)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The number of retries the PS is allowed for
```

```
            AP-REQ/REP key management exchange initiation
            with the NMS. This is the maximum number of
            retries before the PS gives up attempting to
            establish an SNMPv3 security association
            with NMS."
    DEFVAL { 8 }
    ::= { cabhSecKerbBase 4 }

cabhSecNotification OBJECT IDENTIFIER ::= { cabhSecMib 3 }
cabhSecConformance  OBJECT IDENTIFIER ::= { cabhSecMib 4 }
cabhSecCompliances  OBJECT IDENTIFIER ::= { cabhSecConformance 1 }
cabhSecGroups       OBJECT IDENTIFIER ::= { cabhSecConformance 2 }

--
--    Notification Group for future extension
--

-- compliance statements

cabhSecCompliance MODULE-COMPLIANCE
    STATUS      deprecated
    DESCRIPTION
            "The compliance statement for CableHome Security."
    MODULE   --cabhSecMib

-- unconditionally mandatory groups

    MANDATORY-GROUPS {
        cabhSecCertGroup,
        cabhSecKerbGroup
        }

-- conditional mandatory groups

    GROUP cabhSecGroup
    DESCRIPTION
            "This group is implemented only for CH 1.0 gateways."
    ::= { cabhSecCompliances 1 }

    cabhSec2Compliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for CableHome 1.1 Security."
    MODULE   --cabhSecMib

-- unconditionally mandatory groups

    MANDATORY-GROUPS {
        cabhSecCertGroup,
        cabhSecKerbGroup,
        cabhSec2Group
        }
    ::= { cabhSecCompliances 2 }

cabhSecGroup OBJECT-GROUP
    OBJECTS {
        cabhSecFwPolicyFileEnable,
        cabhSecFwPolicyFileURL,
        cabhSecFwPolicyFileHash,
        cabhSecFwPolicyFileOperStatus,
        cabhSecFwPolicyFileCurrentVersion,
        cabhSecFwPolicySuccessfulFileURL,
        cabhSecFwEventType1Enable,
        cabhSecFwEventType2Enable,
```

```
        cabhSecFwEventType3Enable,
        cabhSecFwEventAttackAlertThreshold,
        cabhSecFwEventAttackAlertPeriod
        }
    STATUS      deprecated
    DESCRIPTION
            "Group of objects in CableHome 1.0 Firewall MIB."
    ::= { cabhSecGroups 1 }

cabhSecCertGroup OBJECT-GROUP
    OBJECTS {
        cabhSecCertPsCert
        }
    STATUS      current
    DESCRIPTION
            "Group of objects in CableHome gateway for PS
            Certificate."
    ::= { cabhSecGroups 2 }

cabhSecKerbGroup OBJECT-GROUP
    OBJECTS {
        cabhSecKerbPKINITGracePeriod,
        cabhSecKerbTGSGracePeriod,
        cabhSecKerbUnsolicitedKeyMaxTimeout,
        cabhSecKerbUnsolicitedKeyMaxRetries
        }
    STATUS      current
    DESCRIPTION
            "Group of objects in CableHome gateway for Kerberos."
    ::= { cabhSecGroups 3 }

cabhSec2Group OBJECT-GROUP
    OBJECTS {
        cabhSec2FwEnable,
        cabhSec2FwPolicyFileURL,
        cabhSec2FwPolicyFileHash,
        cabhSec2FwPolicyFileOperStatus,
        cabhSec2FwPolicyFileCurrentVersion,
        cabhSec2FwClearPreviousRuleset,
        cabhSec2FwPolicySelection,
        cabhSec2FwEventSetToFactory,
        cabhSec2FwEventLastSetToFactory,
        cabhSec2FwPolicySuccessfulFileURL,
        cabhSec2FwEventEnable,
        cabhSec2FwEventThreshold,
        cabhSec2FwEventInterval,
        cabhSec2FwEventCount,
        cabhSec2FwEventLogReset,
        cabhSec2FwEventLogLastReset,
        cabhSec2FwLogEventType,
        cabhSec2FwLogEventPriority,
        cabhSec2FwLogEventId,
        cabhSec2FwLogTime,
        cabhSec2FwLogIpProtocol,
        cabhSec2FwLogIpSourceAddr,
        cabhSec2FwLogIpDestAddr,
        cabhSec2FwLogIpSourcePort,
        cabhSec2FwLogIpDestPort,
        cabhSec2FwLogMessageType,
        cabhSec2FwLogReplayCount,
        cabhSec2FwLogMIBPointer,
        cabhSec2FwFilterScheduleStartTime,
        cabhSec2FwFilterScheduleEndTime,
        cabhSec2FwFilterScheduleDOW,
```

```
        cabhSec2FwFactoryDefaultFilterControl,
        cabhSec2FwFactoryDefaultFilterIfIndex,
        cabhSec2FwFactoryDefaultFilterDirection,
        cabhSec2FwFactoryDefaultFilterSaddr,
        cabhSec2FwFactoryDefaultFilterSmask,
        cabhSec2FwFactoryDefaultFilterDaddr,
        cabhSec2FwFactoryDefaultFilterDmask,
        cabhSec2FwFactoryDefaultFilterProtocol,
        cabhSec2FwFactoryDefaultFilterSourcePortLow,
        cabhSec2FwFactoryDefaultFilterSourcePortHigh,
        cabhSec2FwFactoryDefaultFilterDestPortLow,
        cabhSec2FwFactoryDefaultFilterDestPortHigh,
        cabhSec2FwFactoryDefaultFilterContinue
        }
    STATUS      current
    DESCRIPTION
            "Group of objects in CableHome 1.1 Firewall MIB."
    ::= { cabhSecGroups 4 }

END
```

E.6 Cablelabs definition MIB

The CableLabs Definition MIB MUST be implemented as defined below.

```
CLAB-DEF-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    enterprises
                    FROM SNMPv2-SMI
    DocsX509ASN1DEREncodedCertificate
                    FROM DOCS-IETF-BPI2-MIB;

cableLabs MODULE-IDENTITY
    LAST-UPDATED "200504081700Z" -- April 8, 2005
    ORGANIZATION "Cable Television Laboratories, Inc."
    CONTACT-INFO
           "Editor: Jean-Francois Mule
            Postal: Cable Television Laboratories, Inc.
                    858 Coal Creek Circle
                    Louisville, Colorado 80027-9750
                    U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: jfm@cablelabs.com
                    mibs@cablelabs.com"
    DESCRIPTION
            "This MIB module defines the namespace organization for the
            CableLabs enterprise OID registry.

            Copyright 1999-2005 Cable Television Laboratories, Inc.
            All rights reserved."

    REVISION "200504081700Z" -- April 8, 2005
    DESCRIPTION
            "This revision, published as CL-SP-MIB-CLABDEF-I05."
    ::= { enterprises 4491 }

-- Sub-tree for Registrations
clabFunction            OBJECT IDENTIFIER ::= { cableLabs 1 }
clabFuncMib2            OBJECT IDENTIFIER ::= { clabFunction 1 }
clabFuncProprietary     OBJECT IDENTIFIER ::= { clabFunction 2 }
```

```
-- Sub-tree for Project Definitions
clabProject             OBJECT IDENTIFIER ::= { cableLabs 2 }
clabProjDocsis          OBJECT IDENTIFIER ::= { clabProject 1 }
clabProjPacketCable     OBJECT IDENTIFIER ::= { clabProject 2 }
clabProjOpenCable       OBJECT IDENTIFIER ::= { clabProject 3 }
clabProjCableHome       OBJECT IDENTIFIER ::= { clabProject 4 }

-- Sub-tree for Global Security Definitions
clabSecurity            OBJECT IDENTIFIER ::= { cableLabs 3 }
clabSecCertObject       OBJECT IDENTIFIER ::= { clabSecurity 1 }

-- Sub tree for CableLabs cross project common MIB definitions
clabCommonMibs          OBJECT IDENTIFIER ::= { cableLabs 4 }

--
-- CableLabs DOCSIS Project Sub-tree Definitions
--
dsgMIB OBJECT IDENTIFIER
    -- DOCSIS Set-top Gateway (DSG) MIB module
    -- This object identifier points to the MIB module
    -- DOCSIS-SETTOP-GATEWAY-MIB, which is being deprecated by
    -- DSG-IF-MIB MIB module (dsgIfMib).
    -- Reference:
    -- CableLabs DOCSIS Set-top Gateway (DSG) Interface Specification
    ::= { clabProjDocsis 1 }

docsLoadBalMib OBJECT IDENTIFIER
    -- DOCSIS MIB module defining the CMTS configuration parameters to
    -- support Load Balancing requirements."
    ::= { clabProjDocsis 2 }

dsgIfMIB OBJECT IDENTIFIER
    -- DOCSIS Set-top Gateway (DSG) MIB module
    -- Obsoletes DOCSIS-SETTOP-GATEWAY-MIB Module (dsgMib)
    -- defined initially in DOCSIS Set-top Gateway (DSG) Interface
    -- Specification SP-DSG-I01-020228.
    -- Reference:
    -- CableLabs DOCSIS Set-top Gateway (DSG) Interface Specification
    ::= { clabProjDocsis 3 }

dsgIfStdMib OBJECT IDENTIFIER
    -- DOCSIS Set-top Device (DSG) MIB module.
    -- Reference:
    -- CableLabs DOCSIS Set-top Gateway (DSG) Interface Specification
    ::= { clabProjDocsis 4 }

docsIfExt2Mib OBJECT IDENTIFIER
    -- This MIB module contains the management objects that enhance
    -- DOCSIS RFI Interface Extensions. Contains Enhancements to
    -- DOCSIS RFI interface MIB module.
    -- Reference:
    -- CableLabs DOCSIS RFI Interface Specification.
    ::= { clabProjDocsis 5 }

docsTestMIB OBJECT IDENTIFIER
    -- DOCSIS Test MIB module supporting programmable test features
    -- for DOCSIS 2.0 compliant Cable Modems (CM) and Cable Modems
    -- Termination Systems (CMTS).
    -- Reference:
    -- CableLabs DOCSIS 2.0 Testing MIB Specification
    ::= { clabProjDocsis 12 }

sledMib OBJECT IDENTIFIER
    -- eDOCSIS MIB module supporting the Software Loopback Application
```

```
    -- for eDOCSIS (SLED).
    -- Reference:
    -- CableLabs eDOCSIS Specification
    ::= { clabProjDocsis 13 }

--
-- CableLabs CableHome Project Sub-tree Definitions
-- Reference
-- CableLabs CableHome Specification
--
cabhPsDevMib OBJECT IDENTIFIER
    -- CableHome MIB module defining the basic management objects for
    -- the Portal Services logical element of a CableHome compliant
    -- Residential Gateway device. The PS device parameters describe
    -- general PS Device attributes and behaviour characteristics
    ::= { clabProjCableHome 1 }

cabhSecMib OBJECT IDENTIFIER
    -- CableHome MIB module defining the basic management objects for
    -- the firewall and other security features of the Portal Services
    -- element.
    ::= { clabProjCableHome 2 }

cabhCapMib OBJECT IDENTIFIER
    -- CableHome MIB module defining the basic management objects for
    -- the CableHome Address Portal (CAP) function of the Portal
    -- Services element.
    ::= { clabProjCableHome 3 }

cabhCdpMib OBJECT IDENTIFIER
    -- This MIB module supplies the basic management objects for the
    -- CableHome DHCP Portal (CDP) function of the Portal Services
    -- element.
    ::= { clabProjCableHome 4 }

cabhCtpMib OBJECT IDENTIFIER
    -- CableHome MIB module supporting the remote LAN diagnostic
    -- features provided by the CableHome Test Portal (CTP) function
    -- of the Portal Services element.
    ::= { clabProjCableHome 5 }

cabhQosMib OBJECT IDENTIFIER
    -- CABLEHOME QOS MIB Module (cabhQosMib).
    -- This object identifier points to the MIB module
    -- CABH-QOS-MIB, which is being deprecated by
    -- CABH-QOS2-MIB module (cabhQos2Mib).
    -- Reference:
    -- CableLabs CableHome 1.1 Specification
    ::= { clabProjCableHome 6 }

cabhCsaMib OBJECT IDENTIFIER
    -- CableHome MIB module defining management objects for the
    -- configuration and monitoring of CableHome Commercial Services
    -- Annex.
    -- Reference:
    -- CableLabs CableOffice Commercial Services Annex MIB
    -- Specification
    ::= { clabProjCableHome 7 }

cabhQos2Mib OBJECT IDENTIFIER
    -- Obsoletes CABH-QOS-MIB module (cabhQosMib)
    -- defined initially in CABLEHOME 1.1 Interface Specification.
    -- This MIB module defines the Quality of Service Management
    -- Information Base (MIUB) for CableHome UPnP QOS-compliant
```

```
    -- devices.
    -- Reference:
    -- CableLabs CableHome 1.1 Specification
    ::= { clabProjCableHome 8 }

--
-- CableLabs PacketCable Project Sub-tree Definitions
--
pktcMtaMib OBJECT IDENTIFIER
    -- PacketCable MIB module defining the basic management object for
    -- the Multimedia Terminal Adapter (MTA) devices compliant with
    -- PacketCable requirements.
    -- Reference
    -- CableLabs PacketCable MTA Device Provisioning Specification
    ::= { clabProjPacketCable 1 }

pktcSigMib OBJECT IDENTIFIER
    -- PacketCable MIB module defining the basic management object for
    -- the PacketCable MTA Signalling protocols. This version of the MIB
    -- includes common signalling and Network Call Signalling (NCS)
    -- related signalling objects.
    -- Reference
    -- CableLabs PacketCable MTA Device Provisioning Specification
    ::= { clabProjPacketCable 2 }

pktcEventMib OBJECT IDENTIFIER
    -- PacketCable MIB module defining the basic management objects for
    -- event reporting.
    -- Reference
    -- CableLabs PacketCable Management Event Specification
    ::= { clabProjPacketCable 3 }

pktcSecurity OBJECT IDENTIFIER
    -- CableLabs OID reserved for security and used to specify errors
    -- that can be returned for the Kerberos KDC - Provisioning
    -- Server interface, or the MTA-CMS Kerberized IPSec interface, or
    -- the MTA-Provisioning Server Kerberized SNMPv3 interface.
    -- CableLabs PacketCable Security Specification
    ::= { clabProjPacketCable 4 }

pktcLawfulIntercept OBJECT IDENTIFIER
    -- CableLabs OID reserved for the PacketCable Electronic
    -- Surveillance Protocol (PCESP) between the Delivery Function
    -- and Collection Function. This OID is used to define the ASN.1
    -- PCESP messages.
    -- CableLabs PacketCable Electronic Surveillance Protocol
    -- Specification
    ::= { clabProjPacketCable 5 }

--
-- Sub-tree for PacketCable MIB Enhancements
--

pktcEnhancements OBJECT IDENTIFIER ::= { clabProjPacketCable 6 }


-- The following MIB OBJECTS are being introduced for
-- incorporation of new MIB objects (MIB enhancements)
-- proposed to the PacketCable MIB group.
-- This includes new MIB objects being introduced
-- as part of the PacketCable MIB Enhancement efforts
-- and as a place holder for future revisions.
-- This sub-division would facilitate easier incorporation
-- of proposed IETF Drafts/RFCs by keeping enhancements
```

```
-- independent of RFC/Draft changes.
-- For new MIB tables that use previously used indices, it is
-- recommended that the AUGMENT CLAUSE be used to aid SNMP Operations,
-- as deemed necessary.


pktcEnMtaMib OBJECT IDENTIFIER
    -- PacketCable MIB module enhancements to the basic management
    -- objects defined by the MIB group pktcMtaMib for the Multimedia
    -- Terminal Adapter (MTA) devices compliant with PacketCable
    -- requirements.
    -- Reference:
    -- CableLabs PacketCable MTA Device Provisioning Specification.
    ::= { pktcEnhancements 1 }

pktcEnSigMib OBJECT IDENTIFIER
    -- PacketCable MIB module enhancements to the basic management
    -- objects defined by the MIB group pktcSigMib for the
    -- PacketCable MTA Signalling protocols.
    -- Reference:
    -- CableLabs PacketCable MTA Device Provisioning Specification.
    ::= { pktcEnhancements 2 }

pktcEnEventMib OBJECT IDENTIFIER
    -- PacketCable MIB module enhancements to the basic management
    -- objects defined by the MIB group pktcEventMib for event reporting.
    -- Reference:
    -- CableLabs PacketCable Management Event Specification.
    ::= { pktcEnhancements 3 }

pktcEnSecurityMib OBJECT IDENTIFIER
    -- PacketCable MIB module enhancements to the basic management
    -- objects defined by the reserved MIB group pktcSecurity.
    -- Reference:
    -- CableLabs PacketCable Security Specification.
    ::= { pktcEnhancements 4 }

--
--
-- Definition of CableLabs Security Certificate Objects
--
clabSrvcPrvdrRootCACert OBJECT-TYPE
    SYNTAX      DocsX509ASN1DEREncodedCertificate
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The X509 DER-encoded CableLabs Service Provider Root CA
            Certificate."
    REFERENCE
            "CableLabs CableHome Specification;
            CableLabs PacketCable Security Specification."
    ::= { clabSecCertObject 1 }

clabCVCRootCACert OBJECT-TYPE
    SYNTAX      DocsX509ASN1DEREncodedCertificate
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The X509 DER-encoded CableLabs CVC Root CA Certificate."
    REFERENCE
            "CableLabs CableHome Specification;
            CableLabs PacketCable Security Specification."
    ::= { clabSecCertObject 2 }
```

```
clabCVCCACert OBJECT-TYPE
    SYNTAX      DocsX509ASN1DEREncodedCertificate
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The X509 DER-encoded CableLabs CVC CA Certificate."
    REFERENCE
            "CableLabs CableHome Specification;
            CableLabs PacketCable Security Specification."
    ::= { clabSecCertObject 3 }

clabMfgCVCCert OBJECT-TYPE
    SYNTAX      DocsX509ASN1DEREncodedCertificate
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The X509 DER-encoded Manufacturer CVC Certificate."
    REFERENCE
            "CableLabs CableHome Specification;
            CableLabs PacketCable Security Specification."
    ::= { clabSecCertObject 4 }

clabMfgCACert OBJECT-TYPE
    SYNTAX      DocsX509ASN1DEREncodedCertificate
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The X509 DER-encoded Manufacturer CA Certificate."
    REFERENCE
            "CableLabs CableHome Specification;
            CableLabs PacketCable Security Specification."
    ::= { clabSecCertObject 5 }

--
-- CableLabs cross project common MIB sub-tree definitions
--

clabUpsMib OBJECT IDENTIFIER
    -- CableLabs cross project MIB module defining the basic management
    -- objects for the configuration and monitoring of the battery
    -- backup and UPS functionality for CableLabs compliant devices.
    ::= { clabCommonMibs 1 }

END
```

E.7 IPCable2Home QoS Portal (CQP) MIB requirements

The IPCable2Home CQP MIB MUST be implemented as defined below.

```
CABH-QOS2-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Unsigned32,
    Gauge32                  FROM SNMPv2-SMI

    TruthValue,
    TimeStamp,
    RowStatus                FROM SNMPv2-TC

    SnmpAdminString          FROM SNMP-FRAMEWORK-MIB
```

```
    OBJECT-GROUP,
    MODULE-COMPLIANCE        FROM SNMPv2-CONF

    InetPortNumber,
    InetAddressType,
    InetAddress              FROM INET-ADDRESS-MIB

    ifIndex                  FROM IF-MIB

    clabProjCableHome        FROM CLAB-DEF-MIB;

cabhQos2Mib MODULE-IDENTITY
    LAST-UPDATED    "200504080000Z" -- April 8, 2005
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
            858 Coal Creek Circle
            Louisville, Colorado 80027
            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com; mibs@cablelabs.com"
    DESCRIPTION
            "This MIB module supplies parameters for the
            configuration and monitoring of CableHome
            QoS capabilities."
    ::= { clabProjCableHome 8 }

   -- Textual conventions

-- Notifications
cabhQos2Mib2Notifications   OBJECT IDENTIFIER ::= { cabhQos2Mib 0 }

-- Objects definitions

cabhQos2MibObjects          OBJECT IDENTIFIER ::= { cabhQos2Mib 1 }
cabhQos2Base                OBJECT IDENTIFIER ::= {
                                                    cabhQos2MibObjects 1 }
cabhQos2PsIfAttributes      OBJECT IDENTIFIER ::= {
                                                    cabhQos2MibObjects 2 }
cabhQos2PolicyHolderObjects OBJECT IDENTIFIER ::= {
                                                    cabhQos2MibObjects 3 }
cabhQos2DeviceObjects       OBJECT IDENTIFIER ::= {
                                                    cabhQos2MibObjects 4 }

   --================================================================
   --
   -- PS QoS basic control and configuration
   --
   --================================================================

cabhQos2SetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "When this object is set to true(1), the PS MUST clear
            all the entries in cabhQos2PolicyTable and
            cabhQos2TrafficClassTable. Reading this object always
            returns false(2)."
    ::= { cabhQos2Base 1 }
```

```
cabhQos2LastSetToFactory OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when cabhQos2SetToFactory
            was last set to true. Zero if never reset."
    ::= { cabhQos2Base 2 }

   --================================================================
   --
   --  PS Interface Attributes Table
   --
   --  The cabhQos2PsIfAttribTable replaces the deprecated
   --  cabhPriorityQosPsIfAttribTable and contains the number of
   --  media access priorities and number of queues associated with
   --  each PS interface.
   --
   --================================================================

cabhQos2PsIfAttribTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhQos2PsIfAttribEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains interface attributes. It includes
            the number of media access priorities and number of
            queues associated with each PS interface in the
            Residential Gateway."
    ::= { cabhQos2PsIfAttributes 1 }

cabhQos2PsIfAttribEntry OBJECT-TYPE
    SYNTAX      CabhQos2PsIfAttribEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Number of media access priorities and number
            of queues for each PS interface in the Residential
            Gateway. PS does not need to provide support for entries
            associated with Aggregated LAN interfaces (ifIndex 255 and
            254). The PS WAN interfaces are assigned as ifIndex 1 for
            Wan Management and ifIndex 2 for Wan Data; both interfaces
            are indicated in this table as 'WAN interface' with
            ifIndex 1 as the entry identifier."
    INDEX { ifIndex }
    ::= { cabhQos2PsIfAttribTable 1 }

CabhQos2PsIfAttribEntry::= SEQUENCE {
    cabhQos2PsIfAttribNumPriorities   Unsigned32,
    cabhQos2PsIfAttribNumQueues       Unsigned32
    }

cabhQos2PsIfAttribNumPriorities OBJECT-TYPE
    SYNTAX      Unsigned32 (1..8)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of media access priorities supported
            by this interface."
    ::= { cabhQos2PsIfAttribEntry 1 }

cabhQos2PsIfAttribNumQueues OBJECT-TYPE
    SYNTAX      Unsigned32 (1..8)
    MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
            "The number of queues associated with this interface."
    ::= { cabhQos2PsIfAttribEntry 2 }

   --================================================================
   --
   --  PS UPnP Policy Holder Information
   --
   --  Provides the UPnP Qos admission control and Upnp Policy Holder
   -- control and information to be used by the policy manager.
   --
   --================================================================

cabhQos2PolicyHolderEnabled OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The value true indicates that the Policy Holder entity is
            active and advertised in PS UPnP standard discovery
            mechanisms; false indicates it is disabled."
    DEFVAL { true }
    ::= { cabhQos2PolicyHolderObjects 1 }

cabhQos2PolicyAdmissionControl OBJECT-TYPE
    SYNTAX      INTEGER {
                enabled(1),
                disabled(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Indicates if the QoS Policy Admission Control
            is enabled or disabled for all the traffic requests."
    DEFVAL { disabled }
    ::= { cabhQos2PolicyHolderObjects 2 }

cabhQos2NumActivePolicyHolder OBJECT-TYPE
    SYNTAX      Gauge32 (0..4294967295)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Indicates the number of active policy holders the PS
            have discovered in the LAN. This object includes the PS
            Policy Holder if active."
    ::= { cabhQos2PolicyHolderObjects 3 }

cabhQos2PolicyTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhQos2PolicyEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains the operator and user created
            policies for the management of QoS for applications.
            PS creates non-persistent entries (of type 'upnp') for
            the QoS-aware applications and services discovered
            through UPnP actions in the user part of this table which
            could be converted to persistent entries by user (of type
            'user' or by cable operator of type
            'operatorForHomeUserOnly)."
    ::= { cabhQos2PolicyHolderObjects 4 }

cabhQos2PolicyEntry OBJECT-TYPE
```

```
    SYNTAX      CabhQos2PolicyEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The indices for these entries."
    INDEX { cabhQos2PolicyOwner, cabhQos2PolicyOwnerRuleId }
    ::= { cabhQos2PolicyTable 1 }

CabhQos2PolicyEntry ::= SEQUENCE {
    cabhQos2PolicyOwner             INTEGER,
    cabhQos2PolicyOwnerRuleId       Unsigned32,
    cabhQos2PolicyRuleOrder         Unsigned32,
    cabhQos2PolicyAppDomain         SnmpAdminString,
    cabhQos2PolicyAppName           SnmpAdminString,
    cabhQos2PolicyServiceProvDomain SnmpAdminString,
    cabhQos2PolicyServiceName       SnmpAdminString,
    cabhQos2PolicyPortDomain        SnmpAdminString,
    cabhQos2PolicyPortNumber        InetPortNumber,
    cabhQos2PolicyIpType            InetAddressType,
    cabhQos2PolicyIpProtocol        Unsigned32,
    cabhQos2PolicySrcIp             InetAddress,
    cabhQos2PolicyDestIp            InetAddress,
    cabhQos2PolicySrcPort           InetPortNumber,
    cabhQos2PolicyDestPort          InetPortNumber,
    cabhQos2PolicyTraffImpNum       Unsigned32,
    cabhQos2PolicyUserImportance    Unsigned32,
    cabhQos2PolicyRowStatus         RowStatus
    }

cabhQos2PolicyOwner OBJECT-TYPE
    SYNTAX      INTEGER {
                operatorOnly(1),
                homeUser(2),
                operatorForHomeUser(3),
                upnp(4)
                }
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This Index defines the policy creation owner. The entries
            of type 'upnp' are dynamically created by the PS for
            the applications, services and devices that it discovers
            on the LAN with UPnP QoS actions."
    ::= { cabhQos2PolicyEntry 1 }

cabhQos2PolicyOwnerRuleId OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Index for the set of rules related to an
            owner index."
    ::= { cabhQos2PolicyEntry 2 }

cabhQos2PolicyRuleOrder OBJECT-TYPE
    SYNTAX      Unsigned32 (0..4294967295)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The order in which the policy rules are processed within
             An owner."
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 3 }
```

```
cabhQos2PolicyAppDomain OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Vendor domain name from the Vendor
            application name URN."
    DEFVAL { "" }
    ::= { cabhQos2PolicyEntry 4 }

cabhQos2PolicyAppName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Text description of the application."
    DEFVAL { "" }
    ::= { cabhQos2PolicyEntry 5 }

cabhQos2PolicyServiceProvDomain OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The service Provider Service Domain Name from the
            service Provider URN."
    DEFVAL { "" }
    ::= { cabhQos2PolicyEntry 6 }

cabhQos2PolicyServiceName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Text description of the Service."
    DEFVAL { "" }
    ::= { cabhQos2PolicyEntry 7 }

cabhQos2PolicyPortDomain OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Domain name from the Port URN."
    DEFVAL { "" }
    ::= { cabhQos2PolicyEntry 8 }

cabhQos2PolicyPortNumber OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Well known IP transport port of the application."
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 9 }

cabhQos2PolicyIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The type of InetAddress for cabhQos2PolicySrcIp,
            and cabhQos2PolicyDestIp."
    DEFVAL { ipv4 }
```

```
    ::= { cabhQos2PolicyEntry 10 }

cabhQos2PolicyIpProtocol OBJECT-TYPE
    SYNTAX         Unsigned32 (0..255)
    MAX-ACCESS     read-create
    STATUS         current
    DESCRIPTION
            "The IANA-defined IP protocol number representing
            the IP protocol to match against the IPv4 protocol
            number or the IPv6 Next-Header number in the packet.
            '0' means no protocol is specified as matching criteria
            for policy determination, i.e., QoS policy is
            irrespective of IP protocol."
    REFERENCE
            "http://www.iana.org/assignments/protocol-numbers"
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 11 }

cabhQos2PolicySrcIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address to match against the packet's source IP
            address. This may not be a DNS name, but may be an IPv4 or
            IPv6 prefix."
    DEFVAL { '00000000'h }
    ::= { cabhQos2PolicyEntry 12 }

cabhQos2PolicyDestIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address to match against the packet's source IP
            address. This may not be a DNS name, but may be an IPv4 or
            IPv6 prefix."
    DEFVAL { '00000000'h }
    ::= { cabhQos2PolicyEntry 13 }

cabhQos2PolicySrcPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The value that the layer-4 source port number in the
            packet must have in order to match this policy entry."
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 14 }

cabhQos2PolicyDestPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The value that the layer-4 destination port number in the
             packet must have in order to match this policy entry."
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 15 }

cabhQos2PolicyTraffImpNum OBJECT-TYPE
    SYNTAX      Unsigned32 (0..7)
    MAX-ACCESS  read-create
    STATUS      current
```

```
    DESCRIPTION
            "The Traffic priority being assigned to this policy. The
            final packet tagging is determined by 802.1D rules with
            the priority hierarchy order (highest to lowest priority)
            as defined in 802.1D-2004 table G-2:
            7, 6, 5, 4, 3, 0, 2, 1.
            Note that traffic type '1' and '2' has lower priority than
            '0' (best effort)."
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 16 }

cabhQos2PolicyUserImportance OBJECT-TYPE
    SYNTAX      Unsigned32 (0..255)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The UPnP relative value to determine the allocation or
            reallocation of resources to multiple streams."
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 17 }

cabhQos2PolicyRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The status of this conceptual row. All writable objects
            in this row may be modified at any time. The PS MUST
            NOT allow creation of new entry or modification to an
            existing active entry such that the resulting entry is a
            duplicate entry with respect to the following MIBs
            in an entry:
            cabhQos2PolicyAppDomain,
            cabhQos2PolicyAppNameSnmpAdminString,
            cabhQos2PolicyServiceProvDomainSnmpAdminString,
            cabhQos2PolicyServiceName SnmpAdminString,
            cabhQos2PolicyPortDomain SnmpAdminString,
            cabhQos2PolicyPortNumber InetPortNumber,
            cabhQos2PolicyIpType InetAddressType,
            cabhQos2PolicyIpProtocol Unsigned32,
            cabhQos2PolicySrcIp InetAddress,
            cabhQos2PolicyDestIp InetAddress,
            cabhQos2PolicySrcPort InetPortNumber,
            cabhQos2PolicyDestPort InetPortNumber,

            The entries of type 'upnp' are not persistent while others
            are persistent. The user or the operator can change the
            'upnp' entries and in that case the PS MUST change the
            entry to either 'homeUser' or 'operatorForHomeUser',
            respectively. The PS MUST NOT change the entries of type
            'upnp' to 'operatorOnly'."
    ::= { cabhQos2PolicyEntry 18 }

   --================================================================
   --
   --  PS UPnP QoS Device Information
   --
   --  Contains PS QoS device traffic descriptors as classifiers when
   --  acting as an intermediate device for traffic flows
   --  Qos Device information retrieval from the SNMP WAN interface is
   --  defined in PSDEV-MIB module
   --
   --================================================================
```

```
cabhQos2TrafficClassTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhQos2TrafficClassEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains the Classifiers being configured
            in the PS as an intermediate QoS device.
            For matching classifiers the PS processes entries
            in a sorted manner, first entries with
            cabhQos2TrafficClassMethod 'static' and then
            'dynamic' entries."
    ::= { cabhQos2DeviceObjects 1 }

cabhQos2TrafficClassEntry OBJECT-TYPE
    SYNTAX      CabhQos2TrafficClassEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The conceptual row definition of this table.
            Only entries with cabhQos2TrafficClassMethod
            'static' do persist after PS reboot."
    INDEX { cabhQos2TrafficClassMethod, cabhQos2TrafficClassIdx }
    ::= { cabhQos2TrafficClassTable 1 }

CabhQos2TrafficClassEntry::= SEQUENCE {
    cabhQos2TrafficClassMethod         INTEGER,
    cabhQos2TrafficClassIdx            Unsigned32,
    cabhQos2TrafficClassProtocol       Unsigned32,
    cabhQos2TrafficClassIpType         InetAddressType,
    cabhQos2TrafficClassSrcIp          InetAddress,
    cabhQos2TrafficClassDestIp         InetAddress,
    cabhQos2TrafficClassSrcPort        InetPortNumber,
    cabhQos2TrafficClassDestPort       InetPortNumber,
    cabhQos2TrafficClassImpNum         Unsigned32,
    cabhQos2TrafficClassRowStatus      RowStatus
    }

cabhQos2TrafficClassMethod OBJECT-TYPE
    SYNTAX      INTEGER {
                static(1),
                upnp(2)
                }
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Indicates how this entry has been created.
            'static' indicates that the entry has been
             provisioned via SNMP or related mechanisms
             like a config file.
            'upnp' indicates that the entry was created via UPnP
            Qos actions."
    ::= { cabhQos2TrafficClassEntry 1 }

cabhQos2TrafficClassIdx OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index of this conceptual row entry."
    ::= { cabhQos2TrafficClassEntry 2 }

cabhQos2TrafficClassProtocol OBJECT-TYPE
    SYNTAX      Unsigned32 (0..256)
    MAX-ACCESS  read-create
```

```
    STATUS      current
    DESCRIPTION
            "The IANA IP transport protocol designated for this
            classifier. '0' means no protocol is specified as
            matching criteria."
    DEFVAL { 0 }
    ::= { cabhQos2TrafficClassEntry 3 }

cabhQos2TrafficClassIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The type of InetAddress for cabhQos2TrafficClassSrcIp,
            and cabhQos2TrafficClassDestIp."
    DEFVAL { ipv4 }
    ::= { cabhQos2TrafficClassEntry 4 }

cabhQos2TrafficClassSrcIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address to match against the packet's source IP
            address for this classifier. This may not be a DNS name,
            but may be an IPv4 or IPv6 prefix."
    DEFVAL { '00000000'h }
    ::= { cabhQos2TrafficClassEntry 5 }

cabhQos2TrafficClassDestIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address to match against the packet's source IP
            address for this classifier. This may not be a DNS name,
            but may be an IPv4 or IPv6 prefix."
    DEFVAL { '00000000'h }
    ::= { cabhQos2TrafficClassEntry 6 }

cabhQos2TrafficClassSrcPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The value that the layer-4 source port number in the
            packet must have in order to match this classifier entry."
    DEFVAL { 0 }
    ::= { cabhQos2TrafficClassEntry 7 }

cabhQos2TrafficClassDestPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The value that the layer-4 destination port number in the
            packet must have in order to match this classifier entry."
    DEFVAL { 0 }
    ::= { cabhQos2TrafficClassEntry 8 }

cabhQos2TrafficClassImpNum OBJECT-TYPE
    SYNTAX      Unsigned32 (0..7)
    MAX-ACCESS  read-create
    STATUS      current
```

```
    DESCRIPTION
            "The traffic priority assigned to this classifier and used
            for the tagging of the packet streams."
    DEFVAL { 0 }
    ::= { cabhQos2TrafficClassEntry 9 }

cabhQos2TrafficClassRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The status of this conceptual row. All writable objects
            in rows with cabhQosTrafficMethod 'static' may be
            modified at any time. An SNMP Set to Entries with
            cabhQosTrafficMethod 'upnp' returns an error
            'wrongValue'with the exception of the RowStatus
            object when set to 'destroy'.
            An attempt to create an entry via SNMP with
            cabhQosTrafficMethod UPnP returns error 'wrongValue'."
    ::= { cabhQos2TrafficClassEntry 10 }

   -- Placeholder for notifications.
   --
   --
   -- Conformance definitions
   --
cabhQos2Conformance    OBJECT IDENTIFIER  ::= { cabhQos2Mib 2 }
cabhQos2Compliances    OBJECT IDENTIFIER  ::= { cabhQos2Conformance 1 }
cabhQos2Groups         OBJECT IDENTIFIER  ::= { cabhQos2Conformance 2 }

   -- ==================

   -- compliance statements

cabhQos2Compliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for devices that implement
            CableHome QoS UPnP capabilities."
    MODULE   --cabhQos2Mib

   -- unconditionally mandatory groups

    MANDATORY-GROUPS {
          cabhQos2Group
          }

 -- conditionally groups

GROUP cabhQos2ClassifierGroup
    DESCRIPTION
            "This group is optional and implemented only for
             traffic between LAN and WAN."

OBJECT cabhQos2PolicyIpType
    SYNTAX InetAddressType { ipv4(1) }
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

OBJECT cabhQos2PolicySrcIp
    SYNTAX InetAddress (SIZE(4))
```

```
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

OBJECT cabhQos2PolicyDestIp
    SYNTAX InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

OBJECT cabhQos2TrafficClassIpType
    SYNTAX InetAddressType { ipv4(1) }
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses. "

OBJECT cabhQos2TrafficClassSrcIp
    SYNTAX InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

OBJECT cabhQos2TrafficClassDestIp
    SYNTAX InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."
    ::= { cabhQos2Compliances 1 }

cabhQos2Group OBJECT-GROUP
    OBJECTS {
    cabhQos2SetToFactory,
    cabhQos2LastSetToFactory,
    cabhQos2PsIfAttribNumPriorities,
    cabhQos2PsIfAttribNumQueues,
    cabhQos2PolicyHolderEnabled,
    cabhQos2PolicyAdmissionControl,
    cabhQos2NumActivePolicyHolder,
    cabhQos2PolicyRuleOrder,
    cabhQos2PolicyAppDomain,
    cabhQos2PolicyAppName,
    cabhQos2PolicyServiceProvDomain,
    cabhQos2PolicyServiceName,
    cabhQos2PolicyPortDomain,
    cabhQos2PolicyPortNumber,
    cabhQos2PolicyIpProtocol,
    cabhQos2PolicyIpType,
    cabhQos2PolicySrcIp,
    cabhQos2PolicyDestIp,
    cabhQos2PolicySrcPort,
    cabhQos2PolicyDestPort,
    cabhQos2PolicyTraffImpNum,
    cabhQos2PolicyUserImportance,
    cabhQos2PolicyRowStatus,
    cabhQos2TrafficClassProtocol,
    cabhQos2TrafficClassIpType,
    cabhQos2PolicySrcIp,
    cabhQos2PolicyDestIp,
    cabhQos2PolicySrcPort,
    cabhQos2PolicyDestPort,
    cabhQos2PolicyTraffImpNum,
    cabhQos2PolicyUserImportance,
    cabhQos2PolicyRowStatus
    }
```

```
    STATUS      current
    DESCRIPTION
            "Group of objects for CableHome QoS management."
    ::= { cabhQos2Groups 1 }

cabhQos2ClassifierGroup OBJECT-GROUP
    OBJECTS {
    cabhQos2TrafficClassProtocol,
    cabhQos2TrafficClassIpType,
    cabhQos2TrafficClassSrcIp,
    cabhQos2TrafficClassDestIp,
    cabhQos2TrafficClassSrcPort,
    cabhQos2TrafficClassDestPort,
    cabhQos2TrafficClassImpNum,
    cabhQos2TrafficClassRowStatus
    }
    STATUS      current
    DESCRIPTION
            "Group of objects for cableHome QoS Packet
            classification."
    ::= { cabhQos2Groups 2 }
END
```

Appendice I

Exemple de description de dispositif radical UPnP pour le dispositif PS IPCable2Home

The following XML document provides an example of UPnP Root Device description of IPCable2Home PS.

```
<?xml version="1.0" encoding="utf-8" ?>
- <root xmlns="urn:schemas-upnp-org:device-1-0">
  - <specVersion>
      <major>1</major>
      <minor>0</minor>
    </specVersion>
    <URLBase>URLBase</URLBase>
  - <device>
      <deviceType>urn:schemas-cablelabs-com:device:CableHomePSDevice:1</deviceType>
      <friendlyName>friendlyName</friendlyName>
      <manufacturer>manufacturer</manufacturer>
      <manufacturerURL>manufacturerURL</manufacturerURL>
      <modelDescription>modelDescription</modelDescription>
      <modelName>modelName</modelName>
      <modelNumber>modelNumber</modelNumber>
      <modelURL>modelURL</modelURL>
      <serialNumber>serialNumber</serialNumber>
      <UDN>uuid:CableHomePSDevice-1_0-00AABBCCDDEE</UDN>
      <UPC>upc</UPC>
    - <serviceList>
      - <service>
          <serviceType>urn:schemas-upnp-org:service:QosManager:1</serviceType>
          <serviceId>urn:upnp-org:serviceId:QosManager</serviceId>
          <SCPDURL>/QosManager.xml</SCPDURL>
          <controlURL>/QosManager</controlURL>
          <eventSubURL>/QosManager</eventSubURL>
        </service>
      - <service>
          <serviceType>urn:schemas-upnp-org:service:QosPolicyHolder:1</serviceType>
          <serviceId>urn:upnp-org:serviceId:QosPolicyHolder</serviceId>
          <SCPDURL>/QosPolicyHolder.xml</SCPDURL>
          <controlURL>/QosPolicyHolder</controlURL>
          <eventSubURL>/QosPolicyHolder</eventSubURL>
        </service>
      - <service>
          <serviceType>urn:schemas-upnp-org:service:QosDevice:1</serviceType>
          <serviceId>urn:upnp-org:serviceId:QosDevice</serviceId>
          <SCPDURL>/QosDevice.xml</SCPDURL>
          <controlURL>/QosDevice</controlURL>
          <eventSubURL>/QosDevice</eventSubURL>
        </service>
      </serviceList>
    - <deviceList>
      - <device>
          <deviceType>urn:schemas-upnp-org:device:InternetGatewayDevice:1</deviceType>
          <friendlyName>friendlyName</friendlyName>
          <manufacturer>manufacturer</manufacturer>
          <manufacturerURL>manufacturerURL</manufacturerURL>
          <modelDescription>modelDescription</modelDescription>
          <modelName>modelName</modelName>
          <modelNumber>modelNumber</modelNumber>
          <modelURL>modelURL</modelURL>
          <serialNumber>serialNumber</serialNumber>
          <UDN>uuid:InternetGatewayDevice-1_0-00AABBCCDDEE</UDN>
          <UPC>upc</UPC>
        - <deviceList>
          - <device>
              <deviceType>urn:schemas-upnp-org:device:WANDevice:1</deviceType>
              <friendlyName>friendlyName</friendlyName>
```

```
                    <manufacturer>manufacturer</manufacturer>
                   <manufacturerURL>manufacturerURL</manufacturerURL>
                   <modelDescription>modelDescription</modelDescription>
                    <modelName>modelName</modelName>
                    <modelNumber>modelNumber</modelNumber>
                    <modelURL>modelURL</modelURL>
                    <serialNumber>serialNumber</serialNumber>
                    <UDN>uuid:upnp-WANDevice-1_0-XXXX</UDN>
                    <UPC>upc</UPC>
                  - <serviceList>
                     - <service>
                        <serviceType>urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1</serviceType>
                        <serviceId>urn:upnp-org:serviceId:WANCommonInterfaceConfig</serviceId>
                         <SCPDURL>/WANCommonInterfaceConfig.xml</SCPDURL>
                         <controlURL>/WANCommonInterfaceConfig</controlURL>
                        <eventSubURL>/WANCommonInterfaceConfig</eventSubURL>
                      </service>
                    </serviceList>
                  - <deviceList>
                     - <device>
                        <deviceType>urn:schemas-upnp-org:device:WANConnectionDevice:1</deviceType>
                         <friendlyName>friendlyName</friendlyName>
                         <manufacturer>manufacturer</manufacturer>
                         <manufacturerURL>manufacturerURL</manufacturerURL>
                         <modelDescription>modelDescription</modelDescription>
                         <modelName>modelName</modelName>
                         <modelNumber>modelNumber</modelNumber>
                         <modelURL>modelURL</modelURL>
                         <serialNumber>serialNumber</serialNumber>
                         <UDN>uuid:upnp-WANConnectionDevice-1_0-XXXX</UDN>
                         <UPC>upc</UPC>
                        - <serviceList>
                           - <service>
                              <serviceType>urn:schemas-upnp-org:service:WANIPConnection:1</serviceType>
                              <serviceId>urn:upnp-org:serviceId:WANIPConnection</serviceId>
                               <SCPDURL>/WANIPConnection.xml</SCPDURL>
                               <controlURL>/WANIPConnection</controlURL>
                               <eventSubURL>/WANIPConnection</eventSubURL>
                            </service>
                          </serviceList>
                       </device>
                     </deviceList>
                  </device>
                </deviceList>
                <presentationURL>/index.htm</presentationURL>
              </device>
            </deviceList>
            <presentationURL>/index.htm</presentationURL>
          </device>
        </root>
```

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	**Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias**
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2007