Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

J.192

(03/2004)

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

UIT-T

Union internationale des télécommunications

Recommandation UIT-T J.192

Passerelle résidentielle assurant la remise des services de données par câble

Résumé

La présente Recommandation offre un ensemble de caractéristiques fondées sur le protocole IP, normalement associées à une passerelle résidentielle. Cet ensemble, qui peut être intégré dans un câblo-modem ou y être connecté (p. ex. selon les Recommandations UIT-T J.122, J.112), permettra aux câblo-opérateurs d'offrir à leurs clients un ensemble de services de réseau domestique améliorés (par rapport à la Rec. UIT-T J.191). Il comprend la prise en charge de la qualité de service (QS), la découverte de dispositifs et de services, une sécurité améliorée, la gestion du pare-feu, des caractéristiques de gestion et d'approvisionnement orientées vers le réseau domestique, la traduction d'adresse de réseau géré, l'adressage et le traitement de paquet améliorés et les diagnostics de dispositif de réseau LAN.

Source

La Recommandation UIT-T J.192 a été approuvée le 15 mars 2004 par la Commission d'études 9 (2001-2004) 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 la mise en œuvre 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 crée une passerelle résidentielle en offrant un ensemble de caractéristiques fondées sur le protocole IP qui peuvent être ajoutées à un câblo-modem ou être incorporées dans un dispositif autonome. Ces caractéristiques permettront aux câblo-opérateurs d'offrir à leurs clients un ensemble 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 sécurité améliorée, la gestion du pare-feu, des caractéristiques de gestion et d'approvisionnement orientées vers le réseau domestique, la traduction d'adresse de réseau géré, l'adressage et le traitement de paquet améliorés et les diagnostics de dispositif de réseau LAN. La présente Recommandation est fondée sur les cadres architecturaux 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 conserve l'essentiel de la fonctionnalité de la Rec. UIT-T J.191 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 Rec. UIT-T J.192 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 LAN;
- prise en charge par traduction 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 LAN, gérée dans la passerelle résidentielle.

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.

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

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

[Rec. UIT-T J.161] 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*.

[Rec. UIT-T J.162] Recommandation UIT-T J.162 (2004), *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*.

[Rec. UIT-T J.163] Recommandation UIT-T J.163 (2004), *Qualité de service dynamique pour la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems*.

[Rec. UIT-T J.164] Recommandation UIT-T J.164 (2001), *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*.

[Rec. UIT-T J.167] Recommandation UIT-T J.167 (2001), *Prescriptions pour les adaptateurs terminaux de support pour la fourniture de services en temps réel sur les réseaux de télévision par câble au moyen de câblo-modems*.

[Rec. UIT-T J.170] Recommandation UIT-T J.170 (2002), *Spécification de la sécurité sur IPCablecom*.

[Rec. UIT-T J.175] Recommandation UIT-T J.175 (2002), *Protocole de serveur audio*.

[Rec. UIT-T J.178] Recommandation UIT-T J.178 (2003), *Signalisation entre serveurs de gestion d'appel IPCablecom*.

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

[Rec. UIT-T X.25] Recommandation UIT-T X.25 (1996), *Interface entre équipement terminal de traitement de données et équipement de terminaison de circuit de données pour terminaux fonctionnant en mode paquet et raccordés par circuit spécialisé à des réseaux publics pour données*.

[Rec. UIT-T X.509] Recommandation UIT-T X.509 (2000), *Technologies de l'information – Interconnexion de systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

[ANSI/SCTE 22-1] ANSI/SCTE 22-1 2002, *DOCSIS 1.0, Radio Frequency Interface* (Norme d'interface radioélectrique).

[ANSI/SCTE 23-3] ANSI/SCTE 23-3 2003, *DOCSIS 1.1 Partie 3: Operations Support System Interface* (Interface avec le système d'exploitation).

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

[FIPS 180-1] FIPS PUB 180-1 (1995), *Secure Hash Standard* (Algorithme de hachage sécurisé), Department of Commerce, NIST.

[IANAType] IANAifType MIB Definitions (Définitions de la base MIB du type Interface de l'autorité IANA), http://www.iana.org/assignments/ianaiftype-mib.

[ISO/CEI 8825-1] ISO/CEI 8825-1:2002, *Technologies de l'information – Règles de codage ASN.1: Spécification des règles de codage de base (BER), des règles de codage canoniques (CER) et des règles de codage distinctives (DER)*.

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

[RFC 347] IETF RFC 0347 (1972), *Echo Process* (Traitement de l'écho).

[RFC 768] IETF RFC 0768 (1980), *User Datagram Protocol (UDP)* (Protocole des datagrammes d'utilisateur).

[RFC 791] IETF RFC 0791 (1981), *Internet Protocol* (Protocole Internet).

[RFC 792] IETF RFC 0792 (1981), *Internet Control Message Protocol (ICMP)* (Protocole des messages de commande de l'Internet).

[RFC 868] IETF RFC 0868 (1983), *Time Protocol* (Protocole temporel).

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

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

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

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

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

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

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

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

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

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

[RFC 1633] IETF RFC 1633 (1994), *Integrated Services in the Internet Architecture: An Overview* (Services intégrés dans l'architecture Internet).

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

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

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

[RFC 2011] 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).

[RFC 2013] 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).

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

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

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

[RFC 2211] IETF RFC 2211 (1997), *Specification of the Controlled-Load Network Element Service* (Spécification du service d'élément de réseau à charge contrôlée).

[RFC 2212] IETF RFC 2212 (1997), S*pecification of Guaranteed Quality of Service* (Spécification de qualité de service garantie).

[RFC 2233] IETF RFC 2233 (1997), *The Interfaces Group MIB using SMIv2* (La base MIB du groupe d'interfaces utilisant la version SMIv2).

[RFC 2236] IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2* (Protocole de gestion de groupe Internet).

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

[RFC 2315] IETF RFC 2315 (1998), *PKCS #7: Cryptographic Message Syntax Version 1.5* (Système PKCS n°7: Syntaxe de message cryptographique).

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

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

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

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

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

[RFC 2474] 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).

[RFC 2576] IETF RFC 2576 (2000), *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).

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

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

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

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

[RFC 2663] 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)).

[RFC 2665] IETF RFC 2665 (1999), *Definitions of Managed Objects for Ethernet-like Interface Types* (Définitions d'objets gérés pour interfaces de type Ethernet).

[RFC 2669] 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).

[RFC 2670] 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).

[RFC 2786] 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).

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

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

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

[RFC 3280] 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).

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

[RFC 3410] 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).

[RFC 3411] IETF RFC 3411 (2002), *An Architecture for Describing SNMP Management Frameworks* (Architecture de description des cadres de gestion en protocole SNMP).

[RFC 3412] 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).

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

[RFC 3414] 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).

[RFC 3415] 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).

[RFC 3416] 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).

[RFC 3417] 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).

[RFC 3418] 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)).

[SOAP] W3C Recommendation: *SOAP Version 1.2*, 24 juin 2003 (Version 1.2 du protocole simplifié d'accès aux objets), document de travail W3C, World Wide Web Consortium (W3C).
http://www.w3.org/TR/2003/REC-soap12-part0-20030624.

[XML] W3C Working Draft: *XML Protocol (XMLP) Requirements*, 26 juin 2002 (Exigences du protocole XML), document de travail W3C, World Wide Web Consortium (W3C).
http://www.w3.org/TR/2002/WD-xmlp-reqs-20020626.

2.2 Références (informatives)

[ANSI/SCTE 22-3] ANSI/SCTE 22-3 2002, *DOCSIS 1.0 Part 3: Operations Support System Interface* (Interface avec le système d'exploitation).

[draft-ietf-ipcdn-bpiplus-mib-05] IETF Internet Draft, *DOCSIS Baseline Privacy Plus MIB – Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus* (Projet Internet – Base d'informations de gestion pour la confidentialité de base améliorée DOCSIS – Base d'informations de gestion pour les câblo-modems DOCSIS et les systèmes de terminaison de câblo-modems pour la confidentialité de base améliorée).
http://www.watersprings.org/pub/id/draft-ietf-ipcdn-bpiplus-mib-05.txt.

[FIPS 186-2] FIPS PUB 186-2 (2000), *Digital Signature Standard* (Publications normatives fédérales de traitement de l'information) (Norme de signature numérique)
http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf.

[IANA Port] IANA Port Numbers (Numéros de point d'accès attribués par l'autorité IANA) http://www.iana.org/assignments/port-numbers.

[ID-IGMP] IETF Internet Draft, *IGMP-based Multicast Forwarding ("IGMP Proxying")* (Réexpédition multidiffusée en protocole IGMP (réexpédition par mandataire IGMP)), Projet Internet du groupe IETF. http://www.ietf.org/internet-drafts/draft-ietf-magma-igmp-proxy-01.txt.

[PKCS #1] RSA Laboratories, PKCS #1, v2.0: *RSA Cryptography Standard*, 1er octobre 1998 (Norme de cryptographie RSA).

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

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

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

[RFC 3435] IETF RFC 3435 (2003), *Media Gateway Control Protocol (MGCP) Version 1.0* (Protocole de contrôle de passerelle media).

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 gestion de la sécurité et de conversion entre l'hybride HFC et le réseau domestique.

3.2 dispositif PS intégré: élément de services PS 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 LAN: 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 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 PS 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 portail (*bulk portal services configuration*)
CA	autorité de certification (*certification authority*)
CAP	portail d'adresse IPCable2Home (*IPCable2Home address portal*)
CAT	traduction 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 câble (*IPCable2Home DHCP server*)
CH	serveur local IPCable2Home (*IPCable2Home host*)
CM	câblo-modem
CMP	portail de gestion IPCable2Home (*IPCable2Home management portal*)
CMS	serveur (distant) de gestion d'appels (*call management server*)
CMTS	système de terminaison de câblo-modem (*cable modem termination system*)
C-NAT	traduction d'adresse de réseau IPCable2Home (*IPCable2Home network address translation*)
C-NAPT	traduction d'adresse réseau et portail IPCable2Home (*IPCable2Home network address and port translation*)
CNP	portail de nommage IPCable2Home (*IPCable2Home naming 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'essai IPCable2Home (*IPCable2Home test portal*)
CVC	certificat de vérification de code
CVS	signature de vérification de code (*code verification signature*)
CxP	sous-fonction du service 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	service de nom de domaine (*domain name service*)

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 intégré (*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 traverse (*pass-through LAN address*)
LAN-Trans	adresse LAN traduite (*translated LAN 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 (*multi-protocol label switching*)
MSF	fonction de serveur de gestion (*management server function*)
MTA	adaptateur de terminal multimédia (*multimedia terminal adapter*)
NAPT	traduction d'adresse et portail réseau (*network address and portal translation*)
NAT	traduction d'adresse de réseau (*network address translation*)
NCS	signalisation d'appel fondée sur 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 paquet 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 filtering*)
PING	groupeur interréseau de paquets (*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 portail (*portal services*)
PS/WAN-Man	interface de gestion entre un réseau WAN et un élément de service portail CableHome (*CableHome portal services element WAN management interface*)
PS/WAN-Data	interface de données entre un réseau WAN et un élément de service portail CableHome (*CableHome portal services element WAN data interface*)
QBP	point extrême de qualité de service (*quality of service boundary point*)
QCC	client de caractéristiques de qualité de service (*quality of service characteristics client*)
QCS	serveur (distant) de caractéristiques de qualité de service (*quality of service characteristics server*)
QFM	réexpédition et accès au support de la qualité de service (*quality of service forwarding and 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 (*stand-alone multimedia terminal adapter*)
SNMP	protocole simple de gestion de réseau (*simple network management protocol*)
SOA	début d'autorisation (*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 actuelle (*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'adresses de données de réseau régional (*wide area network data address realm*)
WAN-Man	secteur d'adresses 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 d'implémenter 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, *IPCable2Home residential gateway*) interopérable et de serveurs locaux conformes (CH, *IPCable2Home host*). L'objectif est la création d'un environnement orienté vers une passerelle résidentielle configurable par le câblo-opérateur, qui va interagir valablement avec les dispositifs domestiques en protocole IP (dispositifs IP de réseau LAN) qu'ils soient conformes ou non. Cet environnement apporte à la passerelle résidentielle une gestion, un approvisionnement, une qualité de service et une sécurité pilotés par le câblo-opérateur. La messagerie de réseau LAN, la qualité de service priorisée et les télédiagnostics simples pour les dispositifs domestiques sont également spécifiés. La qualité de service pour les applications fonctionnant sur des serveurs locaux de réseau LAN conformes à l'environnement IPCable2Home est également spécifiée. Un résumé des capacités offertes par la présente Recommandation est reproduit ci-dessous:

gestion, découverte et approvisionnement

- gestion et configuration à distance du dispositif de passerelle résidentielle;
- mandataire de diagnostics simples de passerelle résidentielle pour les dispositifs domestiques en protocole IP;
- approvisionnement 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 LAN;

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;

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;

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.

La communication IPCable2Home dans les réseaux WAN et LAN est en protocole IPv4, par déploiement des protocoles spécifiquement définis dans la suite de la présente Recommandation. Les dispositifs conformes au modèle IPCable2Home DOIVENT implémenter la version 4 de la suite de protocoles Internet (IPv4) [RFC 791], [RFC 3280].

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

- point de vue logique (§ 5.1);
- point de vue fonctionnel (§ 5.2);
- point de vue de l'interface de messagerie (§ 5.3);
- point de vue informationnel (§ 5.4);
- point de vue opérationnel (§ 5.5);
- point de 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 logiques du domaine IPCable2Home, les éléments logiques et les dispositifs IPCable2Home.

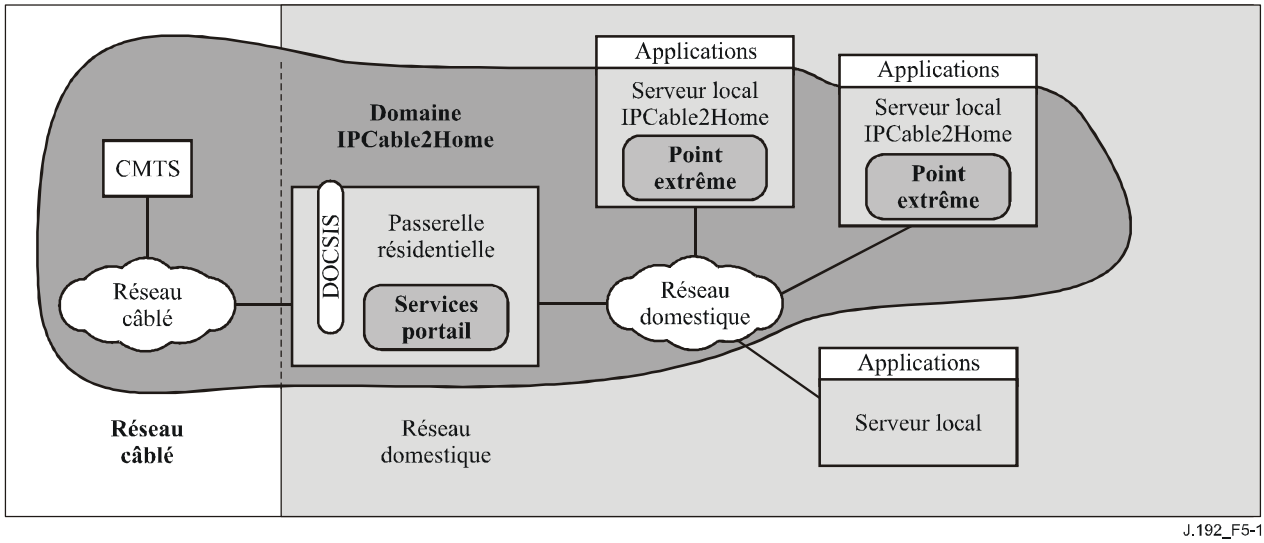


Figure 5-1/J.192 – Principaux concepts logiques IPCable2Home

5.1.1 Domaines IPCable2Home

Le domaine IPCable2Home représente l'ensemble des éléments de réseau qui sont conformes à la présente Recommandation. Ce domaine est représenté sous forme schématique par la zone ombrée

de la Figure 5-1. Cette région sert d'utilitaire visuel, permettant de repérer clairement les éléments du réseau domestique qui sont conformes au modèle IPCable2Home. Les éléments qui résident dans le domaine IPCable2Home (c'est-à-dire les éléments conformes) sont directement ou indirectement gérables par les câblo-opérateurs. Le domaine IPCable2Home existe au niveau de chaque résidence.

5.1.2 Dispositifs IPCable2Home

L'architecture IPCable2Home identifie des dispositifs afin d'offrir un contexte tangible aux éléments logiques décrits dans le § 5.1.3. 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 dans la Rec. UIT-T J.190) représente l'emplacement physique de l'élément logique de services portail (PS) qui est décrit dans le § 5.1.3.1. La passerelle résidentielle a une seule interface avec un réseau WAN, un seul élément logique des services portail et peut avoir une ou plusieurs interfaces avec un réseau LAN.

Le terme de *dispositif IP de réseau LAN* sert à désigner tout dispositif de réseau LAN qui a une interface IP. Un dispositif IP de réseau LAN qui implémente une fonctionnalité IPCable2Home le rendant conforme à la spécification IPCable2Home, est désigné par le terme de *dispositif de serveur local IPCable2Home* (HC dans la Rec. UIT-T J.190). Un dispositif IP de réseau LAN sans fonctionnalité IPCable2Home 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 § 5.1.3.2, 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 LAN dans le domaine IPCable2Home.

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 LAN domestique. L'on part du principe que le CM 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 CM et la passerelle résidentielle IPCable2Home afin que celle-ci puisse offrir la protection spécifiée au réseau domestique. Tous les serveurs locaux de réseau LAN sont connectés au réseau LAN derrière la passerelle résidentielle IPCable2Home.

5.1.3 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 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 § 5.1.2 une description des dispositifs IPCable2Home).

5.1.3.1 Services portail (PS)

Les services portail forment un élément logique qui fournit dans les bâtiments des services composites de sécurité, de gestion, d'approvisionnement, d'adressage et de qualité de service. Le

terme de "portail" sert à indiquer des services qui assurent l'interface du réseau WAN avec le réseau LAN. Le présent paragraphe décrit les caractéristiques de l'élément logique de services portail.

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

Les deux entités fonctionnelles primaires pouvant être intégrées dans une passerelle résidentielle, à savoir le câblo-modem (CM) et l'élément de services portail (PS), peuvent utiliser des ressources matérielles et logicielles partagées ou indépendantes. C'est l'absence de partage de ressources entre les fonctions de câblo-modem et de services 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 portail comme une simple déconnexion de son réseau WAN – c'est-à-dire que le dispositif PS restera entièrement fonctionnel, comme s'il avait été déconnecté du réseau WAN. 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.

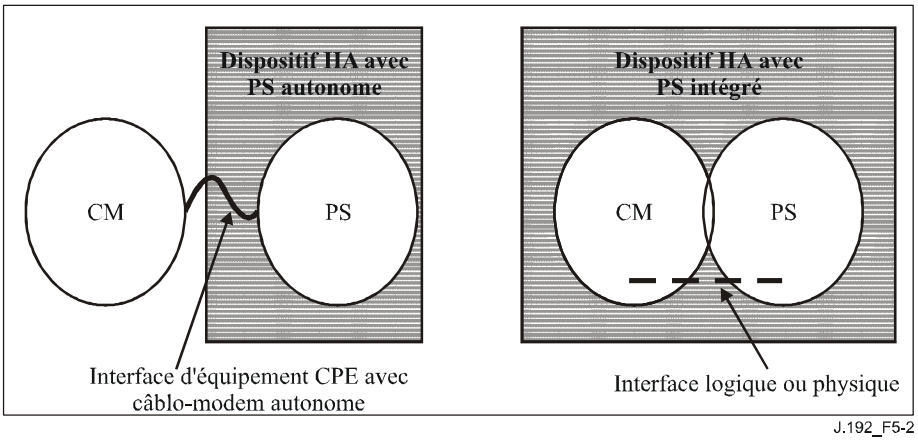


Figure 5-2/J.192 – Dispositif PS autonome et dispositif PS avec câblo-modem intégré

5.1.3.2 Point extrême (point BP)

Un point extrême (point BP) est un élément logique qui encapsule l'ensemble de la fonctionnalité IPCable2Home définie pour un serveur local IPCable2Home. Cette fonctionnalité comprend la messagerie et le comportement requis pour la découverte de dispositifs et d'applications par le câblo-opérateur, ainsi que pour permettre de prioriser la qualité de service dans le réseau domestique. Le point BP interagit avec le dispositif PS afin d'acheminer des informations sur les dispositifs et les applications et de demander les préférences approvisionnées par le câblo-opérateur pour les priorités applicatives.

5.1.4 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 WAN et secteurs d'adresses de réseau LAN (voir Figure 5-3).

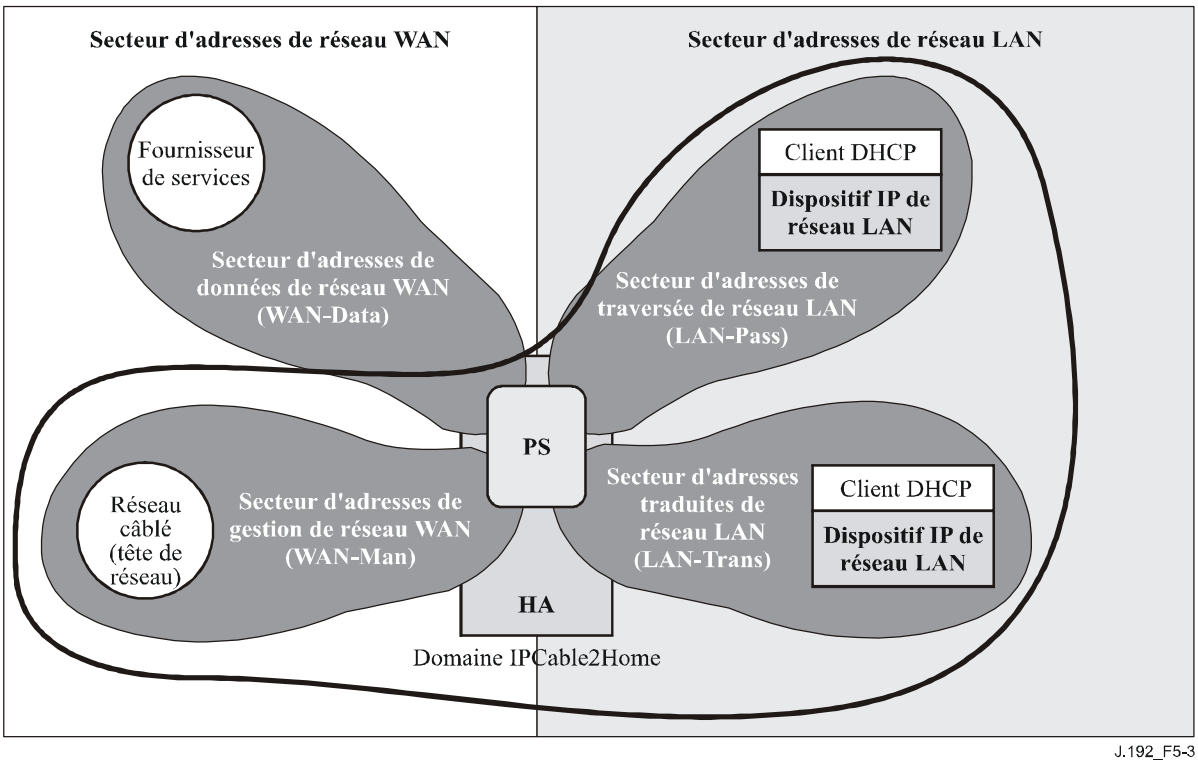


Figure 5-3/J.192 – Secteurs d'adresses IPCable2Home

Les adresses de réseau WAN résident dans un seul des deux secteurs suivants: le secteur d'adresses de gestion de réseau WAN (WAN-Man) ou le secteur d'adresses de données de réseau WAN (WAN-Data). Les adresses de réseau LAN résident également dans un seul des deux secteurs suivants: le secteur d'adresses de traversée de réseau LAN (LAN-Pass) ou le secteur d'adresses traduites de réseau LAN (LAN-Trans). Les propriétés de ces secteurs d'adressage sont les suivantes:

- le secteur d'adresses de gestion de réseau WAN (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 PS. En principe, les adresses de ce secteur résideront dans l'espace privé d'adresses IP;
- le secteur d'adresses de données de réseau WAN (WAN-Data) est destiné à transporter du trafic d'application d'abonné dans le réseau câblé et au-delà, en tant que trafic entre serveurs locaux IPCable2Home et serveurs locaux Internet. En principe, les adresses de ce secteur résideront dans l'espace public d'adresses IP;
- le secteur d'adresses traduites de réseau LAN (LAN-Trans) est destiné à transporter du trafic d'application d'abonné et de gestion dans le réseau domestique entre serveurs locaux IPCable2Home, dispositifs IP de réseau LAN et l'élément de services PS. 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 traversée de réseau LAN (LAN-Pass) est destiné à transporter du trafic d'application d'abonné, comme du trafic entre serveurs locaux IPCable2Home, dispositifs IP de réseau LAN 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 LAN, les adresses contenues dans le secteur d'adresses de traversée de réseau LAN (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 LAN 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 LAN, les dispositifs IP de réseau LAN peuvent se faire attribuer des adresses traduites à partir du secteur d'adresses traduites de réseau LAN (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 LAN, situées dans le dispositif PS, se font attribuer un indice conformément à la base MIB de groupe d'interfaces [RFC 2233] comme décrit dans le § 6.3.3.1.4.8, Base MIB de groupe d'interfaces. Une interface virtuelle avec un réseau LAN intégrant les interfaces physiques avec un réseau LAN est également définie pour le dispositif PS dans le § 6.3.3.1.4.8. L'adresse IP du côté LAN qui a été définie pour le dispositif PS est "reliée" à cette interface virtuelle. Les fonctions de protocole DHCP et de serveur (distant) de noms de domaine, ainsi que la fonction de routeur des services PS, sont des applications implémentées dans le dispositif PS adressé au moyen de l'adresse IP du côté LAN qui est reliée à l'interface virtuelle avec un réseau LAN.

5.2 Modèle de référence fonctionnel IPCable2Home

Les fonctions IPCable2Home sont des services en protocole IP destinés à être implémentés par le dispositif PS, par le point BP, 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: approvisionnement, gestion, sécurité et qualité de service.

Des sous-éléments sont définis pour les deux dispositifs: PS et BP. Ces sous-éléments représentent des groupements de fonctionnalités associées dans le dispositif PS et dans les points extrêmes. Les éléments logiques PS et BP peuvent 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).

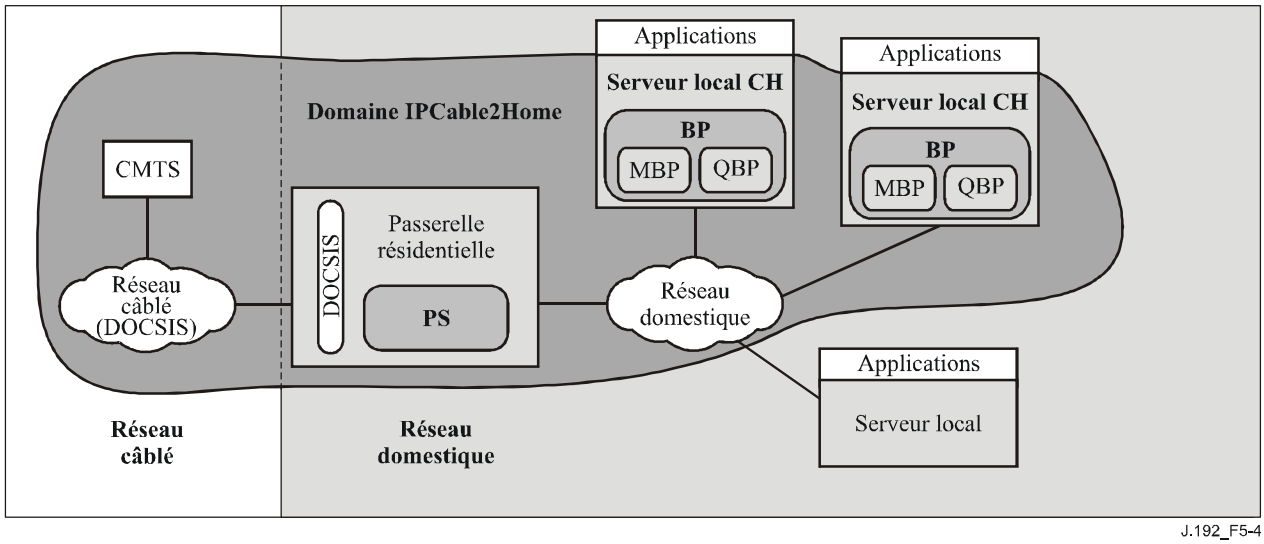


Figure 5-4/J.192 – Sous-éléments IPCable2Home

Le dispositif PS contient un certain nombre de sous-éléments, qui sont présentés ci-dessous. Dans le point extrême, il y a deux sous-éléments primaires: le point extrême de gestion (MBP, *management boundary point*) et le point extrême de qualité de service (QBP, *quality of service boundary point*), qui définissent respectivement la fonctionnalité de découverte et gestion et la fonctionnalité de qualité de service. Le point QBP contient des sous-éléments additionnels particuliers.

5.2.1 Fonctions de gestion et d'approvisionnement IPCable2Home

Afin de prendre en charge les exigences pendant l'approvisionnement et la gestion de serveurs locaux IPCable2Home à domicile, le modèle IPCable2Home fait appel à des fonctions de gestion et d'approvisionnement qui résident dans le réseau de données par câble et définit des fonctions pour le dispositif PS et pour le point extrême. Les fonctions de gestion et d'approvisionnement fondées sur le réseau câblé comprennent un certain nombre de services utilisés par des processus de gestion et d'approvisionnement conformes à IPCable2Home. Les fonctions de gestion et d'approvisionnement des services 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. Les fonctions de point extrême résident dans des serveurs locaux IPCable2Home et comprennent normalement des capacités de client ainsi que d'autres types de fonctionnalité. Des exemples de fonctions de réseau câblé, de services portail et de points extrêmes sont présentés dans les Tableaux 5-1, 5-2 et 5-3. Ils sont également illustrés dans la Figure 5-5.

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 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 actuelle à ses clients.

Tableau 5-2/J.192 – Fonctions de gestion et d'approvisionnement des services 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/Traversée)
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 LAN-Trans.
Traversée	Sous-fonction du portail CAP, la fonction de traversée 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 MSO et la base de données PS.

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

Fonctions de portail de gestion	Description
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 WAN.
Portail de nommage IPCable2Home (CNP)	Le portail CNP offre un service DNS simple pour les dispositifs IP de réseau LAN 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 LAN.
Serveur (distant) HTTP	HTTP est le protocole de transport servant à acheminer la messagerie en protocole SOAP dans le réseau LAN. 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 LAN. Le dispositif PS contient des répartiteurs-vérificateurs syntaxiques pour ces deux langages.

Tableau 5-3/J.192 – Fonctions de point extrême de gestion et d'approvisionnement

Fonctions de client de gestion	Description
Client de serveur local CableHome en protocole DHCP	La fonction de client IPCable2Home en protocole DHCP est un composant domestique qui est utilisé pendant le processus d'approvisionnement d'un dispositif IP de réseau LAN afin de demander dynamiquement des adresses IP et d'autres informations de configuration d'élément logique.
Répondeur de bouclage de serveur local IPCable2Home	Dans un dispositif IP de réseau LAN, le répondeur de bouclage renvoie en boucle à la fonction de bouclage du portail CTP les données envoyées par cette fonction.
Client HTTP	HTTP est le protocole de transport servant à acheminer la messagerie en protocole SOAP dans le réseau LAN. Le point BP contient un client HTTP qui demande des données à partir du serveur HTTP implanté dans le dispositif PS.
Répartiteurs-vérificateurs syntaxiques XML et SOAP	Les langages SOAP et XML sont utilisés pour la messagerie dans le réseau LAN. Le point BP contient des répartiteurs-vérificateurs syntaxiques pour ces deux langages.

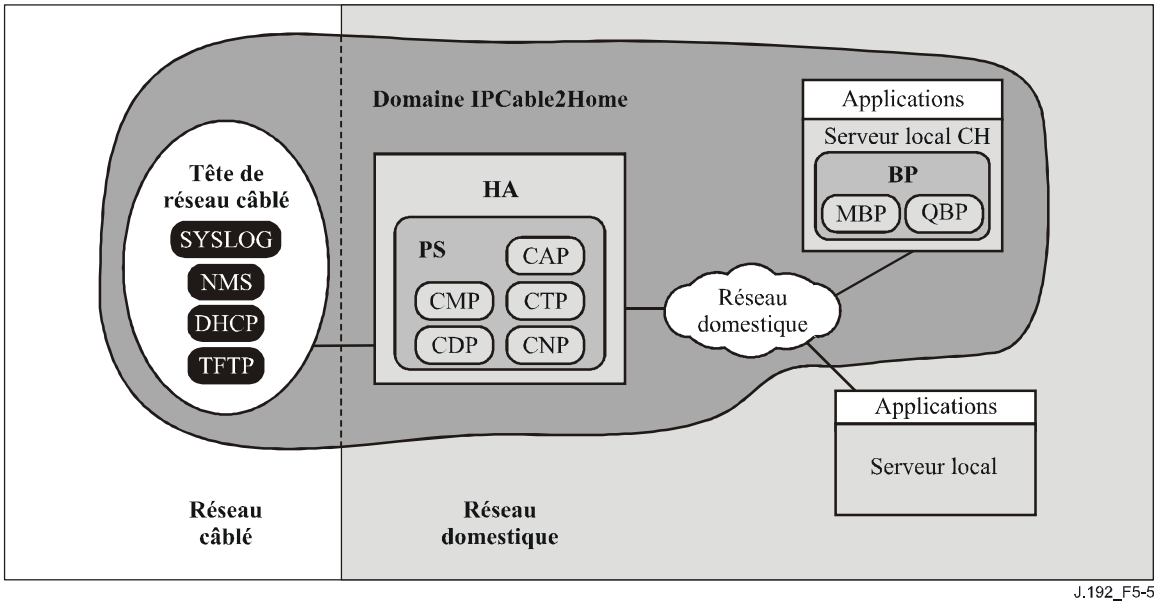


Figure 5-5/J.192 – Eléments de gestion IPCable2Home

5.2.2 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. Ces fonctions résident dans le domaine de sécurité IPCable2Home, qui existe au niveau de chaque domicile. 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 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 5-6.

Tableau 5-4/J.192 – Fonctions de sécurité fournies par le dispositif PS

Fonctions de sécurité fournies par le dispositif PS	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

Fonction de sécurité fournies par le réseau câblé	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.

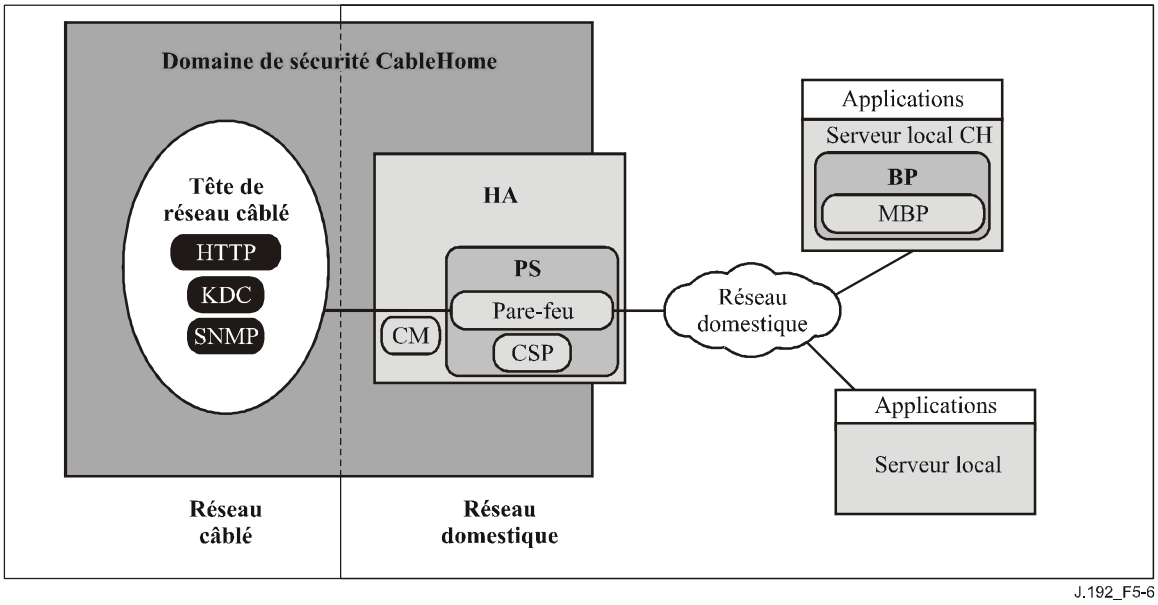


Figure 5-6/J.192 – Eléments de sécurité IPCable2Home

5.2.3 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 et pour le point extrême. Les fonctions de qualité de service pour services portail sont situées dans la passerelle résidentielle et comprennent une fonction de serveur et d'autres types de fonctions. Les fonctions de qualité de service de point extrême sont situées dans des dispositifs de serveur local IPCable2Home et comprennent une fonction de client et d'autres types de fonctions. Des exemples de fonctions de qualité de service pour services portail et point extrême sont présentés dans les Tableaux 5-6 et 5-7. Ils sont également illustrés dans la Figure 5-7.

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

Fonctions de qualité de service pour services portail	Description
Serveur (distant) de caractéristiques de qualité de service (QCS, *QoS characteristics server*)	Ce serveur acquiert, à partir du système de gestion de réseau câblé, des informations sur la priorité des applications en termes de qualité de service. Ce serveur acquiert une liste d'applications de point extrême à partir du point extrême. Il offre des informations sur les priorités applicatives au point extrême, telles qu'elles ont été établies par le câblo-opérateur.

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

Fonctions de qualité de service pour services portail	Description
Réexpédition et accès au support de la qualité de service (QFM)	Cette fonction ordonne les paquets arrivant de multiples interfaces avec un réseau LAN et allant au dispositif PS, puis les réexpédie vers une interface avec un réseau LAN de destination conformément à leur priorité. Cette fonction offre également un accès rendu prioritaire (priorisé) aux supports partagés, pendant la transmission de paquets selon leur priorité.

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

Fonctions de qualité de service pour point extrême	Description
Client des caractéristiques de qualité de service (QCC)	Cette fonction offre aux services portail des informations sur les applications résidant dans le serveur local IPCable2Home; elle demande également des informations sur les priorités applicatives établies par l'opérateur MSO. Elle offre également un accès priorisé aux supports partagés pendant la transmission de paquets selon leur priorité.

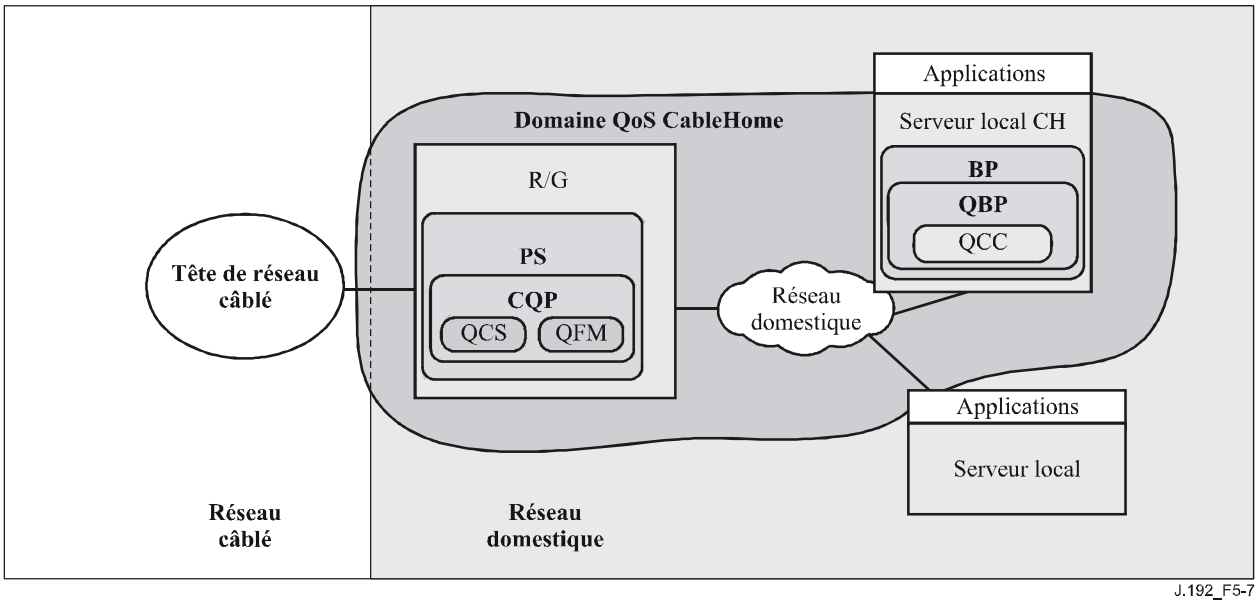


Figure 5-7/J.192 – Eléments de qualité de service IPCable2Home

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 LAN passe par les interfaces de messagerie identifiées et étiquetées dans la Figure 5-8. Les types d'interfaces de messagerie sont différenciés par les éléments qui sont impliqués dans la communication.

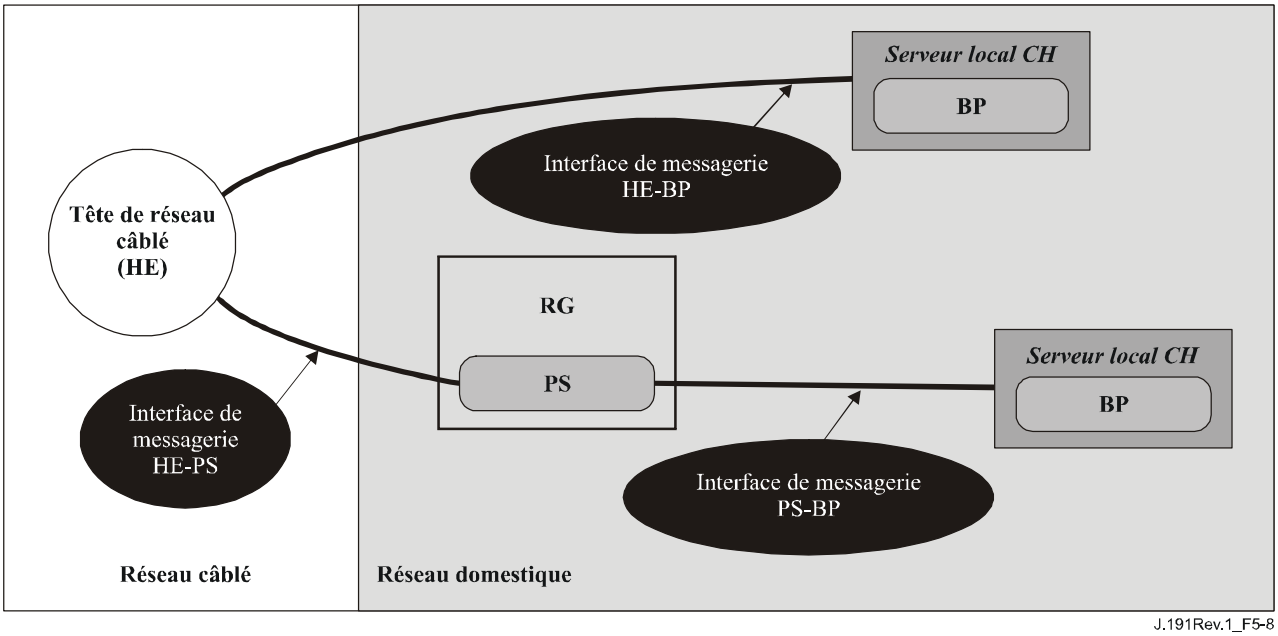


Figure 5-8/J.192 – Interfaces de référence IPCable2Home

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-PS	HE-BP	RG-BP
Service de nommage	DNS	Non spécifiée	Non spécifiée	J.192
Téléchargement de logiciel	TFTP	J.192	Non spécifiée	Non spécifiée
Acquisition d'adresse	DHCP	J.192	Non spécifiée	J.192
Gestion (simple) (en masse)	 SNMP TFTP ou HTTP	 J.192 J.192	 Non spécifiée Non spécifiée	 Non spécifiée Non spécifiée
Notification d'événement	SNMP SYSLOG	J.192 J.192	Non spécifiée	Non spécifiée
Qualité de service	Protocoles de QS IPCablecom, priorités IPCable2Home SOAP/XML	Non spécifiée	IPCablecom	J.192
Sécurité (distribution de clés)	Kerberos	J.192	Non spécifiée	Non spécifiée
Nom de service	DNS	Non spécifié	Non spécifiée	J.192

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

Fonctionnalité	Protocole	Interface		
		HE-PS	HE-BP	RG-BP
Sécurité (authentification)	Kerberos ou TLS	J.192	Non spécifiée	Non spécifiée
Sondage par écho	ICMP	J.192	Non spécifiée	J.192
Bouclage/Echo	UDP/TCP	Non spécifiée	Non spécifiée	J.192
Découverte d'application	SNMP SOAP/XML	J.192	Non spécifiée	J.192

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 5-9 montre la relation entre la base de données et les fonctions de services portail. Le Tableau 5-9 décrit les informations typiquement associées à chacune de ces fonctions. La Figure 5-10 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.

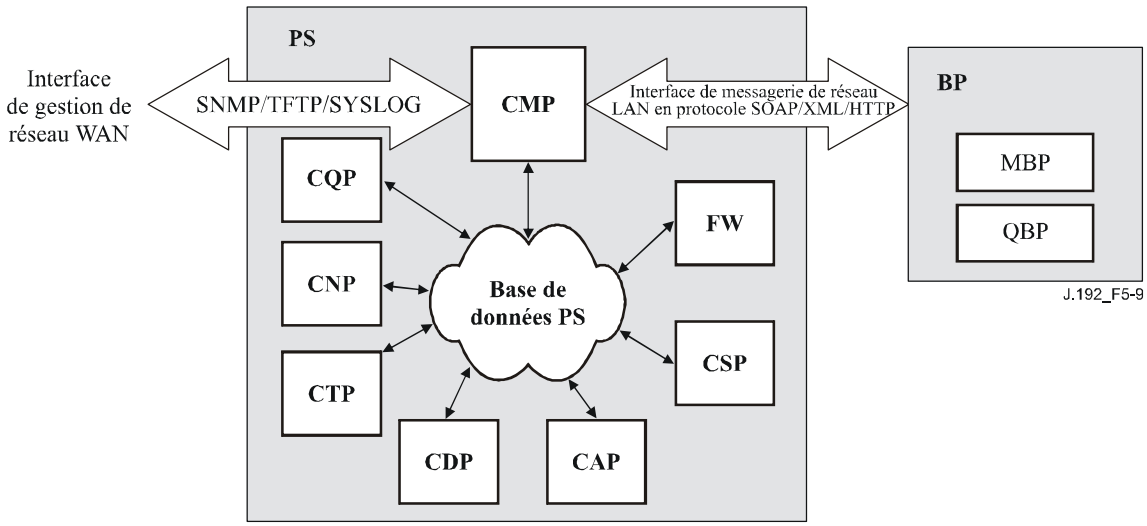


Figure 5-9/J.192 – Relation entre fonction PS et base de données PS

La base de données PS mémorise une multitude de relations entre données. Le portail CMP fournit l'interface de gestion d'un réseau WAN (SNMP) à la base de données PS. Les fonctions remplies au sein des services portail introduisent et révisent les relations entre données dans la base de données PS. De plus, les fonctions remplies au sein des services 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 portail. Informations sur les dispositifs de serveur local IPCable2Home
Informations CTP	Informations associées aux résultats des essais de réseau LAN effectués par le portail CMP
Informations CNP	Informations associées à la résolution du nom d'un dispositif IP de réseau LAN
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 transferts automatiques, etc.
Informations de serveur local IPCable2Home	Informations sur le profil du dispositif de point extrême, collectées par la messagerie BP_Init à partir de serveurs locaux IPCable2Home
Informations de serveur local IPCable2Home – caractéristiques de qualité de service	Caractéristiques de qualité de service reçues du câblo-opérateur et informations sur le profil de qualité de service reçues des serveurs locaux IPCable2Home par messagerie BP_Init

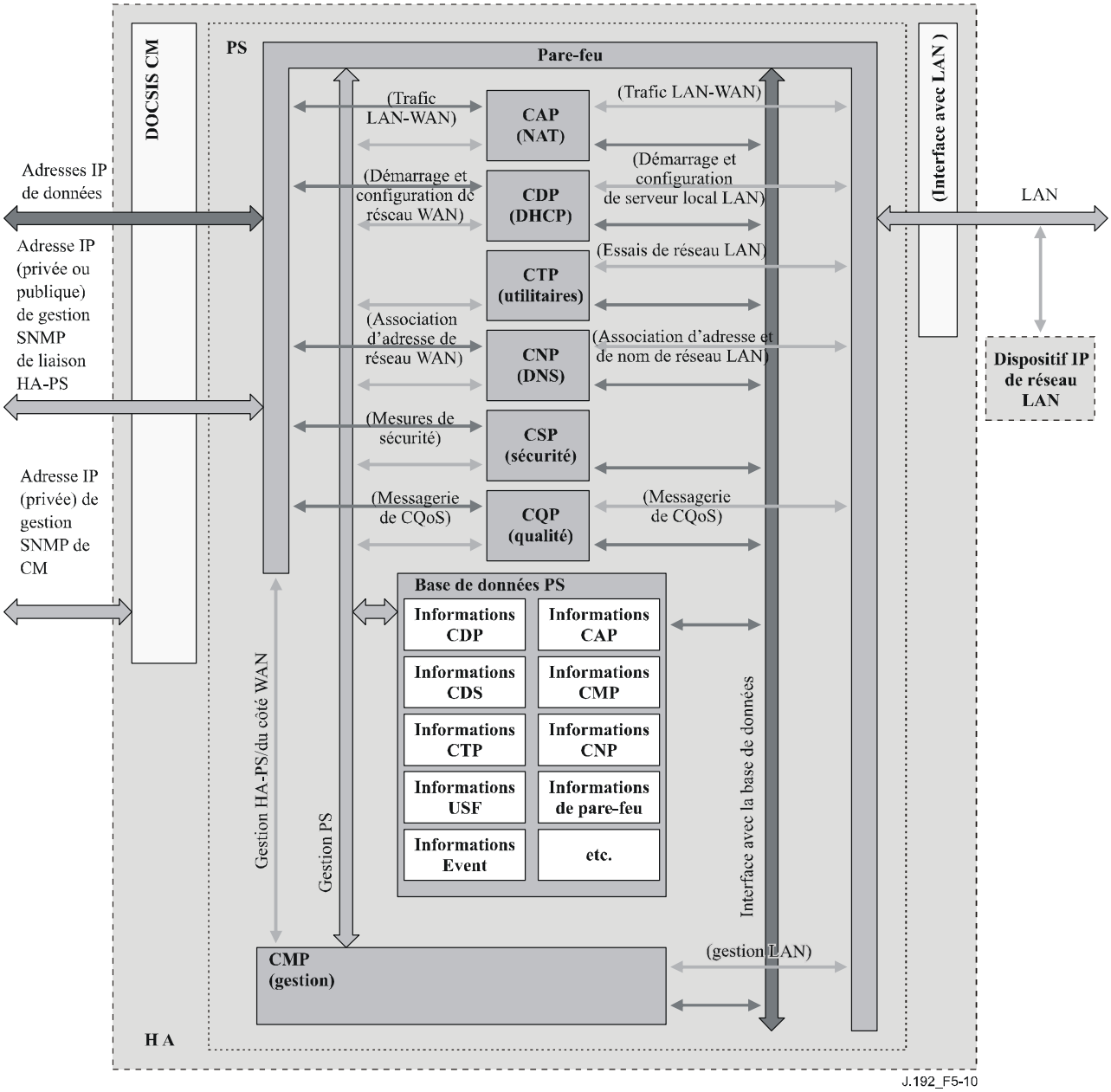


Figure 5-10/J.192 – Base de données PS: exemple détaillé d'implémentation

Le dispositif PS est principalement géré à partir du réseau WAN 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 l'approvisionnement des fonctions de services portail, ainsi qu'aux télédiagnostics ou aux états du réseau LAN. Les diagnostics peuvent s'appuyer sur le portail CTP afin d'obtenir une meilleure visibilité de l'état actuel du réseau LAN. La connexité et les performances rudimentaires du réseau peuvent être mesurées.

Le portail CNP est le serveur (distant) de noms de domaine (DNS) du réseau LAN. Tous les dispositifs IP de réseau LAN 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 LAN, retourne leurs adresses IP correspondantes et, en outre, renvoie les dispositifs IP de réseau LAN 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 pour implémenter un client du protocole DHCP dans les secteurs de réseau WAN.

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 WAN) du seul trafic local de réseau LAN. Enfin, le portail CAP contient la fonction de traversée, qui dérive le trafic entre les secteurs d'adresses du réseau LAN et du réseau WAN.

Le portail CSP fournit les capacités d'authentification des services 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 Modes de fonctionnement IPCable2Home

La fonctionnalité de l'élément de services PS est compatible avec diverses infrastructures de réseau câblé prises en charge par un certain nombre de différents modes de fonctionnement des services portail, qui permettent au dispositif PS de fonctionner correctement à l'intérieur d'une infrastructure d'approvisionnement de type CableModem (Rec. UIT-T J.112 ou Rec. UIT-T J.122) seulement, ainsi qu'à l'intérieur d'une infrastructure d'approvisionnement CableModem plus IPCablecom. L'infrastructure d'approvisionnement 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 d'approvisionnement IPCablecom.

Aux fins de la configuration, le dispositif PS peut fonctionner dans un des deux modes d'approvisionnement suivants:

- le mode d'approvisionnement DHCP;
- le mode d'approvisionnement SNMP.

Si le dispositif PS n'est pas configuré de façon à fonctionner soit en mode d'approvisionnement DHCP ou en mode d'approvisionnement SNMP, cela implique que la logistique administrative n'est pas actuellement disponible et va se replier par défaut de façon à fonctionner 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.

Quand le dispositif PS est configuré de façon à fonctionner en mode d'approvisionnement 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 doit fonctionner en mode d'approvisionnement DHCP, il peut opérer dans un seule 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 d'approvisionnement SNMP, il ne fonctionne qu'en mode de gestion de réseau par coexistence SNMPv3.

La Figure 5-11 décrit les divers modes de fonctionnement des services 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 d'approvisionnement.

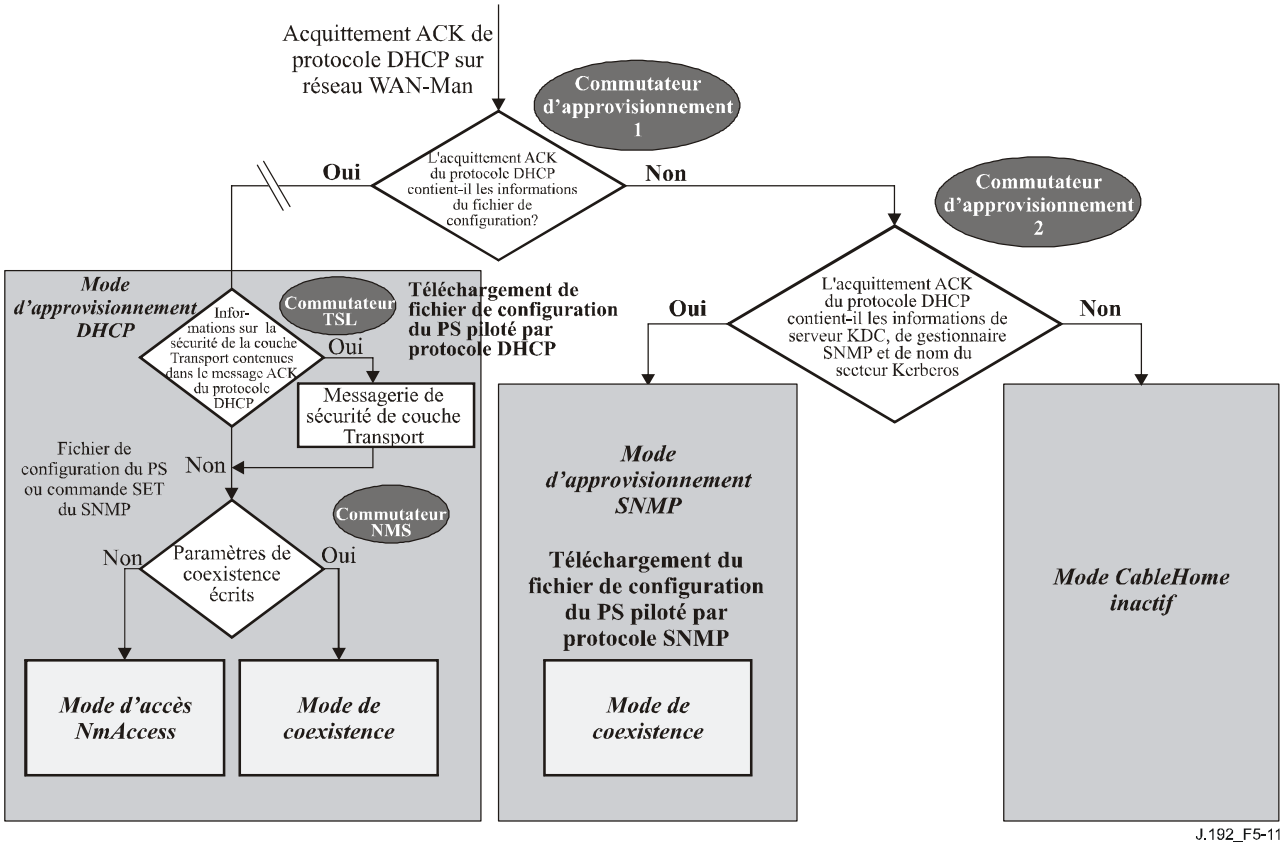


Figure 5-11/J.192 – Modes de fonctionnement des services portail

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

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

Mode	Fonctionnalité directement affectée	Infrastructure prévue
Mode d'approvisionnement SNMP	Téléchargement du fichier de configuration.	Infrastructure d'approvisionnement CableModem plus IPCablecom
Mode d'approvisionnement DHCP	Téléchargement du fichier de configuration.	Infrastructures CableModem avec prise en charge du modèle IPCable2Home
Mode d'approvisionnement 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 d'approvisionnement 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 d'approvisionnement DHCP: mode de gestion de réseau par coexistence SNMP	Version SNMP utilisée entre NMS et PS	Infrastructures d'approvisionnement 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

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 portail. Plusieurs de ces types sont décrits dans la liste ci-dessous:

- interfaces de mise en réseau 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 WAN destinées à la connexion avec un réseau WAN, dans le cas d'un dispositif PS autonome;
- interfaces de mise en réseau LAN pour connexion à des dispositifs IP de réseau LAN 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 commande 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 PS 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. 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 portail PEUT offrir la possibilité de configurer des fonctions autres que de type IPCable2Home. L'accès à des fonctions PS par une interface de gestion (lecture/écriture) utilisant le mécanisme servant à configurer des fonctions autres que de type IPCable2Home NE DOIT PAS être autorisé.

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 PS, de découvrir des dispositifs IP de réseau LAN et les applications qu'ils offrent, de vérifier à distance la connexité entre le dispositif PS et les dispositifs IP de réseau LAN afin d'offrir la politique de qualité de service aux points extrêmes à l'appui de la qualité de service priorisée entre dispositifs de serveur local IPCable2Home, et de

signaler les événements d'état et d'exception dans le dispositif PS. Le présent paragraphe décrit et spécifie les exigences relatives à ces capacités.

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

- la présente Recommandation ajoute l'exigence que les services portail assurent la gestion SNMP à partir de toute interface avec un réseau LAN;
- la présente Recommandation ajoute l'exigence que le dispositif PS et le point BP assurent tous les deux la messagerie PS-BP pour l'échange de priorités de qualité de service;
- la présente Recommandation ajoute l'exigence que le point BP implémente un profil de dispositif en format XML;
- la présente Recommandation ajoute les objets de base MIB suivants aux services portail:
  - objets requis afin de prendre en charge la qualité de service priorisée dans le réseau LAN;
  - objets prenant en charge la fonctionnalité améliorée de pare-feu;
  - objets permettant au câblo-opérateur de découvrir les attributs de dispositifs de serveur local IPCable2Home.

6.1.1 Objectifs

Les objectifs des utilitaires de gestion IPCable2Home sont les suivants:

- permettre au câblo-opérateur de découvrir des dispositifs IP de réseau LAN;
- offrir aux câblo-opérateurs une visibilité sur des dispositifs IP de réseau LAN;
- offrir aux câblo-opérateurs une visibilité sur les applications des dispositifs de serveur local IPCable2Home;
- définir une méthode pour communiquer les priorités de qualité de service aux applications fonctionnant sur des dispositifs de serveur local IPCable2Home;
- définir un ensemble minimal d'utilitaires de télédiagnostics qui permettront au câblo-opérateur de vérifier la connexité entre l'élément de services PS et tout dispositif IP de réseau LAN;
- offrir aux câblo-opérateurs, par les bases MIB, l'accès à des données internes de l'élément de services PS 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 transferts automatiques 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);
- les dispositifs de serveur local IPCable2Home implémentent un profil de dispositif et un profil de qualité de service en format XML;
- 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 PS 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 PS du modèle IPCable2Home;
- les dispositifs IP de réseau LAN implémentent un client du protocole DHCP;
- la passerelle résidentielle IPCable2Home et les dispositifs IP de réseau LAN 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 PS et les dispositifs IP de réseau LAN.

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 portail.
Mgmt 2	Le dispositif PS sera capable d'envoyer une commande ICMP (de sondage par écho) à tout dispositif IP de réseau LAN 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 LAN 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 PS sera capable de signaler les événements.
Mgmt 5	L'élément de services PS sera capable de communiquer avec les dispositifs de serveur local IPCable2Home 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 d'application de serveur local IPCable2Home.
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'essai IPCable2Home (CTP);
3) une base d'informations de gestion (MIB);
4) un système de gestion de réseau (NMS) en protocole SNMP qui fait partie du réseau câblé;
5) un profil de dispositif en format XML implémenté par chaque dispositif de serveur local IPCable2Home (élément logique de point extrême).

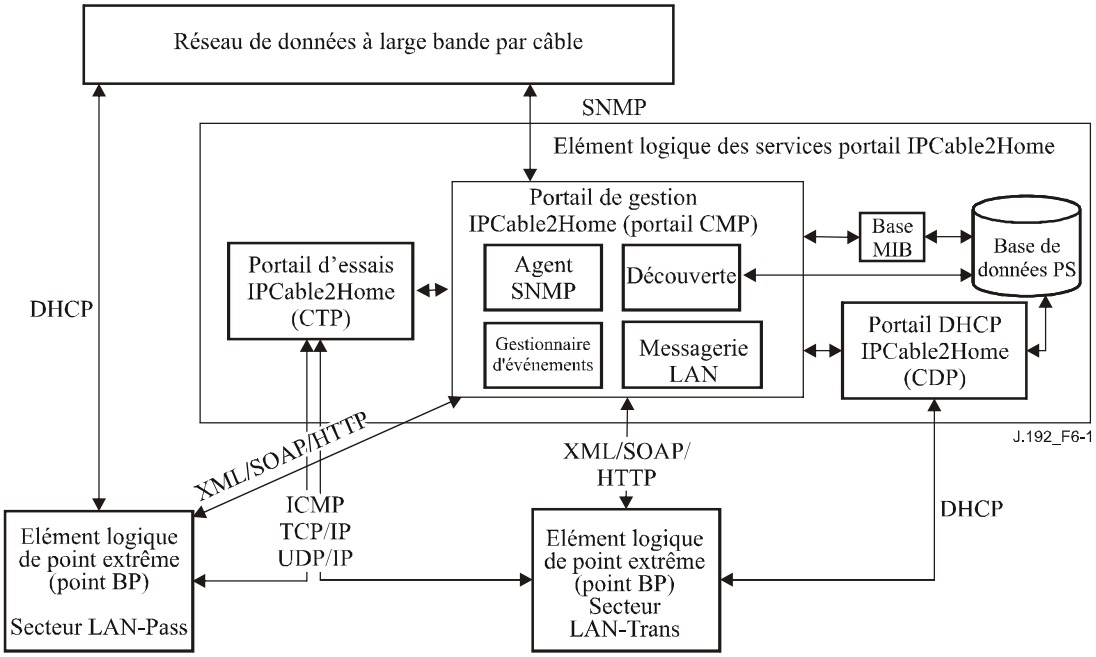


Figure 6-1/J.192 – Architecture de gestion IPCable2Home

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. Le câblo-opérateur accède aux attributs de dispositif de serveur local IPCable2Home et de passerelle résidentielle IPCable2Home par la base MIB d'objets PsDev [voir § E.4] et par la base MIB de qualité de service [voir § 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.

Dès réception du message DHCP ACKNOWLEDGE (message ACK du protocole DHCP) [RFC 2131] issu de son serveur DHCP, l'élément logique de point extrême situé dans chaque dispositif de serveur local IPCable2Home commence la communication avec le dispositif PS par une interface de messagerie sur réseau LAN. Cette messagerie, sous la forme d'un transport du protocole simple d'accès aux objets (SOAP, *simple object access protocol*) sur le protocole de transfert d'hypertextes (HTTP, *hypertext transfer protocol*), est effectuée de façon à informer le dispositif PS au sujet des attributs du dispositif (profil du dispositif) et à lui communiquer une liste d'applications (profil de qualité de service) implémentées dans le serveur local IPCable2Home. Quand le dispositif PS reçoit le profil du dispositif et le profil de qualité de service, il fait ce qui suit:

- il mémorise les informations relatives au profil du dispositif de point BP contenues dans une table de base MIB de profils de dispositif BP (objet cabhPsDevBpProfileTable).

  Le profil du dispositif de point extrême permet au câblo-opérateur de découvrir des informations sur des dispositifs de serveur local IPCable2Home dans le secteur LAN-Pass et offre au câblo-opérateur des informations sur des dispositifs de serveur local IPCable2Home dans le secteur LAN-Trans en plus des informations obtenues par messagerie en protocole DHCP entre le dispositif PS et le point BP de réseau LAN-Trans;
- il mémorise les informations de point BP sur le profil de qualité de service dans une table MIB de priorités d'application de point BP (objet cabhPriorityQosBpTable).

  Le profil de qualité de service d'un point BP permet au câblo-opérateur de découvrir des applications implémentées sur des dispositifs de serveur local IPCable2Home. Ces

applications sont identifiées par le "notoire" numéro de point d'accès de l'autorité IANA sous lequel elles ont été enregistrées.

Si le câblo-opérateur a approvisionné le dispositif PS avec la politique de qualité de service en remplissant la table de référence des priorités d'application (objet cabhPriorityQosMasterTable), le dispositif PS va également offrir au point extrême des priorités de qualité de service à partir de cette table, par la même interface de messagerie de réseau LAN. Cette procédure est décrite dans le § 10.3.2.4.2, Echange d'informations du côté LAN.

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

Le portail DHCP IPCable2Home, décrit dans le paragraphe relatif aux utilitaires d'approvisionnement (§ 7), joue un rôle dans la découverte de base des dispositifs IP de réseau LAN. Par communication en protocole DHCP entre dispositifs IP de réseau LAN et portail CDP, le dispositif IP de réseau LAN 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 LAN 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 portail peut être corésident avec un câblo-modem intégré ou être autonome, sans fonctionnalité de câblo-modem intégré, comme décrit dans le § 5.1.3.1.1.

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 CM 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 portail (et vice versa). Les droits d'accès SNMP aux services 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 PS accepte les protocoles SNMPv1, SNMPv2c et SNMPv3. Le paragraphe 5.5 a présenté les modes d'approvisionnement acceptés par un élément de services PS et le § 7 donne des détails supplémentaires sur ces modes. Le mode d'approvisionnement 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 portail – Portail de gestion IPCable2Home (portail CMP)

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

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 CableHome et les dispositifs IP de réseau LAN dans le secteur LAN-Trans, par le portail d'essai IPCable2Home (CTP);
- permettre la configuration à distance des paramètres d'adressage d'un dispositif IP de réseau LAN;
- permettre de voir les informations de dispositif IP de réseau LAN obtenues par le portail DHCP IPCable2Home (CDP);
- offrir au câblo-opérateur l'accès aux attributs des dispositifs de serveur local IPCable2Home et des applications implémentées par ces dispositifs, acquis par le processus de découverte IPCable2Home;
- prendre en charge l'échange, entre la passerelle résidentielle IPCable2Home et les dispositifs de serveur local IPCable2Home, des attributs de dispositif, de la liste des applications et des priorités de qualité de service pour les applications;
- permettre de voir les résultats de la surveillance de la performance d'un dispositif IP de réseau LAN, assurée par le portail d'essai IPCable2Home (CTP);
- permettre au système NMS d'accéder à d'autres paramètres de configuration des services 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 LAN.

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 approvisionnés 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	Les serveurs locaux IPCable2Home se trouvant dans le réseau domestique devraient se rétablir après une coupure de courant et revenir à un état opérationnel normal dès que l'alimentation sera rétablie.
CMP 4	Les dispositifs du réseau domestique seront faciles à installer et à configurer pour le fonctionnement, exactement comme un appareil d'utilisation domestique.

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

Référence	Directives de conception du système de portail CMP
CMP 5	Le dispositif PS et les dispositifs IP de réseau LAN prendront en charge un protocole permettant de découvrir les dispositifs IP de réseau LAN connectés au réseau LAN domestique.
CMP 6	Le dispositif PS offrira au câblo-opérateur, sur demande, des informations sur les dispositifs ajoutés au réseau LAN domestique.
CMP 7	Le dispositif PS et le point extrême prendront en charge un protocole permettant d'échanger les attributs des dispositifs de serveur local IPCable2Home, les attributs des applications implémentées par ces dispositifs, ainsi que les priorités de qualité de service pour ces applications.
CMP 8	Le dispositif PS offrira au câblo-opérateur, sur demande, des informations sur les attributs des dispositifs de serveur local IPCable2Home et sur les attributs des applications implémentées par ces dispositifs.
CMP 9	L'échange des messages du protocole de découverte dans le réseau LAN domestique ne dégradera pas perceptiblement la performance du réseau LAN domestique.
CMP 10	La messagerie de découverte ne se propagera pas dans le réseau WAN.

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 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;
- permettre l'échange des priorités de qualité de service entre dispositifs PS et BP;
- permettre au gestionnaire de découvrir à distance les dispositifs connectés au réseau LAN domestique et les applications fonctionnant sur ces dispositifs;
- traiter et journaliser les messages événementiels.

Le portail CMP se compose des quatre 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 WAN au moyen de l'adresse IP du réseau WAN-Man, et les messages SNMP issus d'interface avec le réseau LAN 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 LAN.

2) *Fonction de traitement des événements*

   Le portail CMP signale les événements conformément aux réglages de la table docsDevEvent. La liste des événements pris en charge figure dans l'Annexe B.

3) *Fonction de découverte*

   Le portail CMP, par sa fonctionnalité de découverte, acquiert des informations sur chaque dispositif de serveur local IPCable2Home et sur les applications qu'il fait fonctionner. Le portail CMP mémorise ces informations dans la base de données PS et les rend disponibles

à une entité de gestion SNMP, au moyen de la base MIB d'objets PSDev [voir § E.4] et de la base MIB d'objets QS [voir § E.7].

4) *Fonction de messagerie LAN*

Le portail CMP échange en format XML les paramètres de qualité de service et les attributs du profil de dispositif, avec les serveurs locaux IPCable2Home contenus dans le réseau LAN, au moyen du protocole simple d'accès aux objets (SOAP).

Ces fonctions sont décrites dans les § 6.3.3.1 à 6.3.3.4.

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 Accès en protocole SNMP 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	Fonction d'agent SNMP: directives de conception du système
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 LAN, et en interconnecte la gestion. Elle prend également en charge la messagerie de gestion par protocole SNMP à toute interface avec un réseau LAN.

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

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

Mode d'approvisionnement SNMP/mode de gestion par coexistence avec le protocole SNMP

Comme décrit dans le § 5.5, lorsque le dispositif PS se trouve en mode d'approvisionnement 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 d'approvisionnement DHCP/mode de gestion par table NmAccess

Comme décrit dans le § 5.5, lorsque le dispositif PS se trouve en mode d'approvisionnement 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.

Mode d'approvisionnement DHCP/mode de gestion par coexistence de la version SNMPv3

Quand le dispositif PS fonctionne en mode d'approvisionnement DHCP, le câblo-opérateur peut remplir la table de coexistence au moyen de messages SNMP de demande de mise à jour ou par fichier de configuration du 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 2576], 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 PS.

Le Tableau 6-4 contient les définitions des termes qui sont propres au portail CMP.

Tableau 6-4/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 PS	Ensemble de paramètres qui contrôle ou surveille le comportement de l'élément de services PS, lisible par le système de gestion du réseau WAN. Il peut être conçu comme un répertoire d'informations décrivant l'état actuel du service 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 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 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 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 LAN. 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 HTTP. 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 LAN: échange de messages de gestion entre le système NMS du réseau câblé et les dispositifs IP de réseau LAN dans le secteur LAN-Pass. Cette messagerie de gestion est hors du domaine d'application de la présente Recommandation.

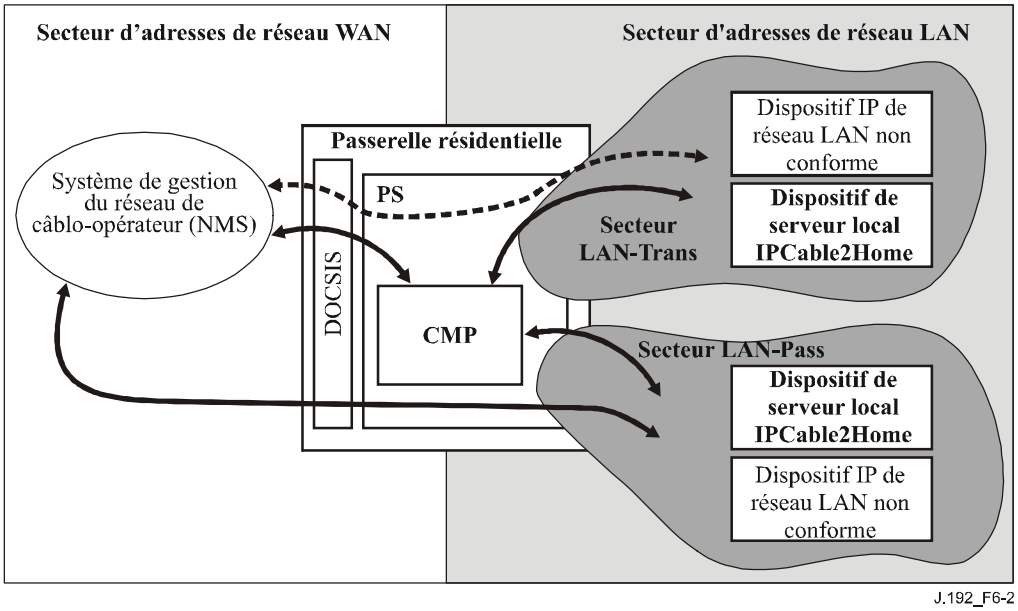


Figure 6-2/J.192 – Interfaces avec les messages de gestion CableHome

Le portail CMP est essentiellement une entité à laquelle on accède (au moyen du système NMS) par un réseau WAN 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 LAN 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.

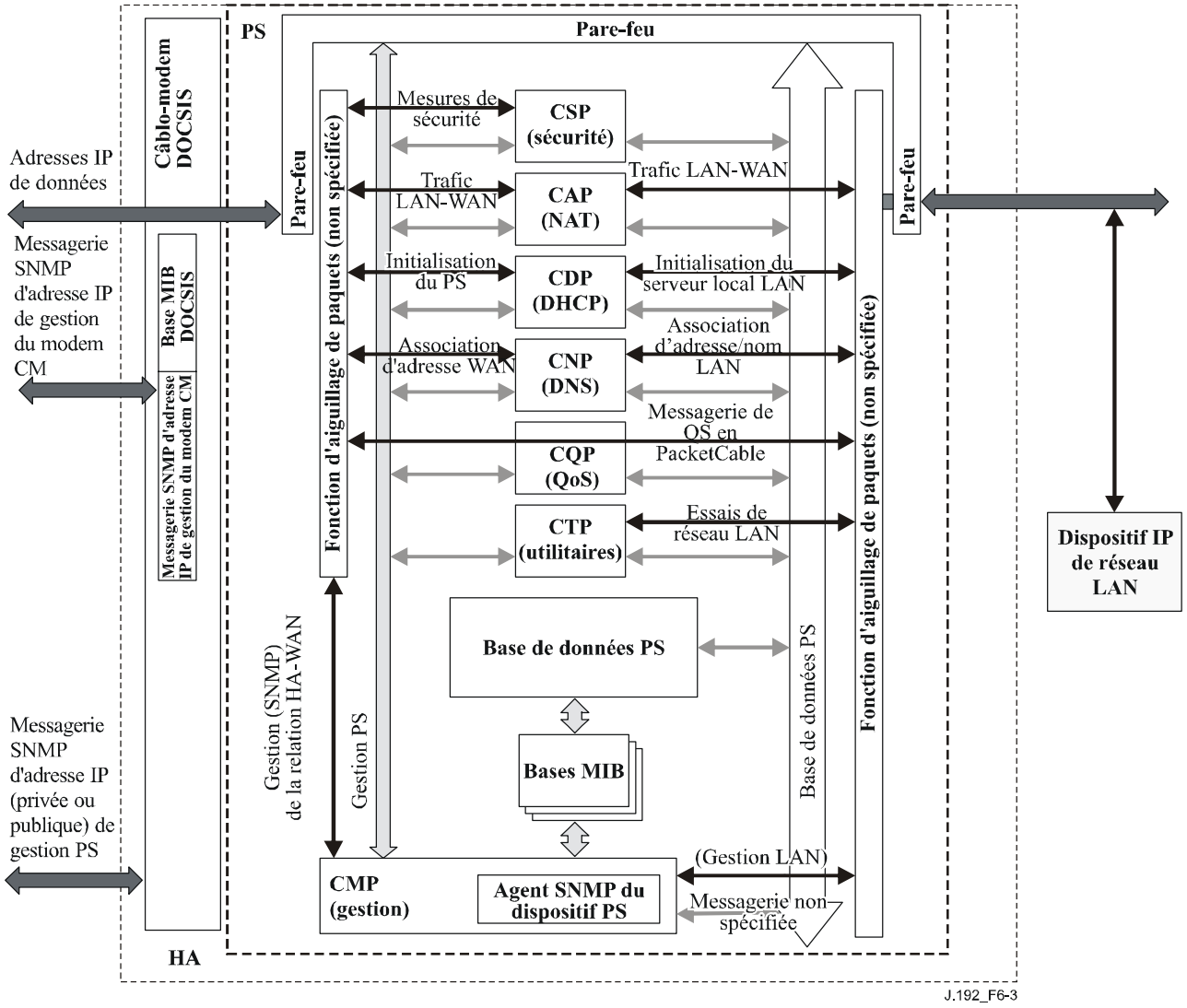


Figure 6-3/J.192 – Organigramme des services portail

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 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 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 CableHome – ou les gérer – d'une des deux façons suivantes. Le câblo-opérateur peut accéder directement aux serveurs locaux CableHome au moyen d'un adressage de traversée entre le réseau câblé et l'élément de dispositif de réseau LAN (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 demande SNMP de mise à jour (SET) ou par des messages de demande SNMP de requête 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 CableHome.

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".

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 ou envoyés à l'adresse du routeur-serveur de son réseau LAN (objet cabhCdpServerRouter), lorsqu'il fonctionne en mode d'approvisionnement DHCP ou en mode d'approvisionnement SNMP (objet cabhPsDevProvMode = dhcpmode(1) ou snmpmode(2)).

L'agent SNMP contenu dans le dispositif PS DOIT recevoir et traiter tous les messages SNMP envoyés à l'adresse du routeur-serveur du réseau LAN des services portail (objet cabhCdpServerRouter) si le dispositif PS n'a jamais été approvisionné.

Le dispositif PS DOIT ignorer les messages SNMP reçus par l'intermédiaire d'une quelconque interface avec un réseau LAN 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) ainsi que les types de messages ICMP de marqueur temporel et de réponse au marqueur temporel (de types 13 et 14) 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 d'approvisionnement 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 d'approvisionnement DHCP".

Si le dispositif PS doit fonctionner en mode d'approvisionnement 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 d'approvisionnement SNMP".

Quand le dispositif PS doit fonctionner en mode de coexistence SNMP, le réglage par défaut d'autorité ultime DOIT être "administrateur de réseau WAN" (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 6-5:

Tableau 6-5/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 "docsDevSwCurrentVers" 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 LAN à réseau WAN et de réseau WAN à réseau LAN 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 PS sont réglés à leur valeur par défaut à la construction au moyen des objets de base MIB cabhCapSetToFactory, cabhCdpSetToFactory, cabhCtpSetToFactory, ou cabhPsDevSetToFactory, la fonctionnalité correspondante de services portail DOIT utiliser en exploitation ces réglages par défaut à la construction sans devoir ré-approvisionner l'élément de services PS.

6.3.3.1.4.1 Exigences relatives au protocole SNMP

Le dispositif PS DOIT observer ou implémenter, 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 the Simple Network Management Protocol" (Modèle de sécurité fondé sur l'utilisateur (USM) pour le 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 le 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 2576]

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 d'approvisionnement (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 portail dans chacun des deux modes d'approvisionnement, 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 paragraphes décrivent les modes de gestion de réseau pour un dispositif PS fonctionnant en mode d'approvisionnement DHCP. Le paragraphe 6.3.3.1.4.3 et ses paragraphes décrivent les modes de gestion de réseau pour un dispositif PS fonctionnant en mode d'approvisionnement 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 d'approvisionnement DHCP ou en mode d'approvisionnement SNMP. Il fonctionne par défaut en mode de coexistence de la version SNMPv3 lorsqu'il est en mode d'approvisionnement SNMP. Lorsqu'il fonctionne en mode d'approvisionnement 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 implémentées 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 par 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 2576], [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 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 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 d'approvisionnement 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 2576]. 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 d'approvisionnement 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 d'approvisionnement DHCP

Le fonctionnement initial du dispositif PS configuré en mode d'approvisionnement DHCP peut être considéré comme comportant trois étapes:

1) le comportement du dispositif PS après qu'il a été configuré en mode d'approvisionnement DHCP mais avant que son mode de gestion de réseau ait été configuré par le fichier de configuration du 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:

a) Une fois que le dispositif PS a été configuré de façon à fonctionner en mode d'approvisionnement 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 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 PS DOIT être achevé avant le début du calcul des valeurs publiques dans la table USMDHKickstart.

b) Si un dispositif PS doit fonctionner en mode d'approvisionnement DHCP, le contenu du fichier de configuration du 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 PS contient SEULEMENT le réglage de table docsDevTable NmAccess pour le contrôle d'accès par protocole SNMP;
- si le fichier de configuration du 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 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.

c) Après achèvement du processus d'approvisionnement décrit dans le paragraphe 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 PS comme décrit ci-dessus. Les règles de fonctionnement des services 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 transfert comme décrit dans le document [RFC 2669]. Le dispositif PS 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 CableHome, sans tenir compte de l'interface 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 transferts automatiques 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

  "Spécifie la version du message-transfert qui est envoyé au système NMS considéré. Le réglage de cet objet à la valeur "disableSNMPv2trap(1)" provoque l'envoi du message-transfert en format SNMPv1 à un système NMS particulier. Le réglage de cet objet à la valeur "EnableSNMPv2trap(2)" provoque l'envoi du message-transfert en format SNMPv2 à un système NMS particulier".

  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 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 WAN;
- le dispositif PS PEUT continuer afin de permettre l'accès à partir du réseau LAN 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-transfert 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 2576];

- la table docsDevNmAccessTable n'est pas accessible;
- les destinations des messages de contrôle d'accès et de transfert 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 CableHome, 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-transferts 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 d'approvisionnement SNMP

Si le dispositif PS doit fonctionner en mode d'approvisionnement 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 d'approvisionnement DHCP et a été configuré en mode de gestion de réseau par coexistence SNMPv3, quand le dispositif PS doit fonctionner en mode d'approvisionnement 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 CableHome 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 CableHome, 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 2576]. 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 WAN (vue CHAdministrator) et un utilisateur-administrateur de réseau WAN (utilisateur CHAdministrator) sont définis par la présente Recommandation. D'autres vues et utilisateurs, comme la vue de maintenance de réseau WAN, la vue d'administrateur de réseau WAN, ou la vue d'utilisateur de réseau LAN peuvent être établis par l'autorité ultime (CHAdministrator), conformément aux règles définies dans les documents [RFC 3414] et [RFC 3415].

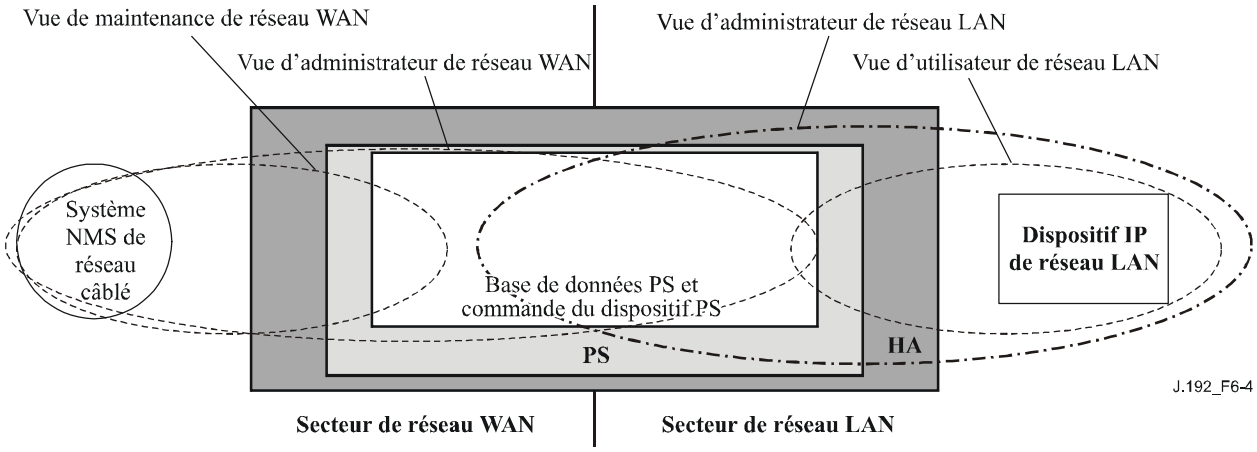


Figure 6-4/J.192 – Vues de gestion

Les paramètres gérés et définis par CableHome 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 LAN et WAN en définissant des vues de gestion dans la base de données PS et dans la fonction de commande des services PS. 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 LAN qu'à l'interface de gestion de réseau WAN;
- 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 PS;
- établissement de la politique d'accès du côté LAN comme du côté WAN.

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 par CableHome.

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 WAN

Le contrôle d'accès SNMP, selon [RFC 3415], va servir à commander l'accès aux objets de base MIB spécifiés par le modèle CableHome, sans tenir compte de l'interface par laquelle la requête arrive. Le modèle de commande d'accès fondé sur la vue (VACM) [RFC 3415] 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] section 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 CableHome afin d'assurer la gestion par réseau WAN 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 WAN 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 § 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 WAN DOIT être implémentée dans un élément de services PS conforme. Les vues par défaut autres que la vue d'administrateur de réseau WAN 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 WAN 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	'CHAdministrator'
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-arbre 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 § 7.4.4.1.9, 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 6-6 (snmpNotifyTable) à 6-15 (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 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 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<Addresse IP> TLV 38.1

<Point d'accès> TLV 38.2

<Type de transfert> TLV 38.3

<Temporisation> TLV 38.4

<Réessais> TLV 38.5

<OID de filtre> TLV 38.6

<nom de sécurité> 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 6-6/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 PS.

Tableau 6-7/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 PS
snmpTargetAddrTDomain	snmpUDPDomain – snmpDomains
snmpTargetAddrTAddress (Adresse IP et point d'accès UDP du récepteur de notification)	Chaîne d'octets (6) Octets 1 – 4: <Adresse IP> Octets 5 – 6: <Point d'accès>
snmpTargetAddrTimeout	<Temporisation> d'après l'élément TLV
snmpTargetAddrRetryCount	<Réessais> d'après l'élément TLV
snmpTargetAddrTagList	Si <Type de transfert> == 1,2, ou 4 "@PSconfig_trap" Sinon si <Type de transfert> = 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 PS.

Tableau 6-8/J.192 – snmpTargetAddrExtTable

[RFC 2576] 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 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 <Type de transfert> est 1, 2, ou 3, ou si le champ <nom de sécurité> a une longueur égale à zéro, créer le tableau comme suit:

Tableau 6-9/J.192 – snmpTargetParamsTable pour <Type de transfert> 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 PS
snmpTargetParamsMPModel SYNTAX: SnmpMessageProcessingModel	Si <Type de transfert> = 1 SNMPv1(0) Sinon si <Type de transfert> = 2 ou 3 SNMPv2c(1) Sinon si <Type de transfert> = 4 ou 5 SNMPv3(3)
snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	Si <Type de transfert> = 1 SNMPv1(1) Sinon si <Type de transfert> = 2 ou 3 SNMPv2c(2) Sinon si <Type de transfert> = 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 <Type de transfert> est 4 ou 5 et si le champ <nom de sécurité> a une longueur différente de zéro, créer le tableau comme suit:

Tableau 6-10/J.192 – Tableau snmpTargetParamsTable pour <Type de transfert> 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 PS
snmpTargetParamsMPModel SYNTAX: SnmpMessageProcessingModel	Si <Type de transfert> = 1 SNMPv1(0) Sinon si <Type de transfert> = 2 ou 3 SNMPv2c(1) Sinon si <Type de transfert> = 4 ou 5 SNMPv3(3)
snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	Si <Type de transfert> = 1 SNMPv1(1) Sinon si <Type de transfert> = 2 ou 3 SNMPv2c(2) Sinon si <Type de transfert> = 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 <nom de sécurité>
snmpTargetParamsStorageType	"volatile"
snmpTargetParamsRowStatus	active(1)

snmpNotifyFilterProfileTable

Créer une seule rangée pour chaque TLV qui a une <Longueur de filtre> différente de zéro.

Tableau 6-11/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 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 PS.
snmpNotifyFilterProfileStorType	"volatile"
snmpNotifyFilterProfileRowStatus	active(1)

snmpNotifyFilterTable

Créer une seule rangée pour chaque TLV qui a une <Longueur de filtre> différente de zéro.

Tableau 6-12/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 PS.
* snmpNotifyFilterSubtree	<OID de filtre> d'après l'élément TLV
snmpNotifyFilterMask	<Chaîne d'octets de longueur égale à zéro>
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 6-13/J.192 – snmpCommunityTable

snmpCommunityTable [RFC 2576] SNMP-COMMUNITY-MIB	Première rangée
Nom de colonne (* = partie de l'indice)	Valeur de colonne
* snmpCommunityIndex	"@PSconfig"
snmpCommunityName	"public"
snmpCommunitySecurityName	"@PSconfig"
snmpCommunityContextEngineID"	<Identificateur d'automate PS>
snmpCommunityContextName	<Chaîne d'octets de longueur égale à zéro>
snmpCommunityTransportTag	<Chaîne d'octets de longueur égale à zéro>
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-transferts 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 6-14/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 <nom de sécurité> d'après l'élément TLV.
usmUserSecurityName	"@PSconfig" Quand d'autres rangées sont créées, celle-ci est remplacée par le champ <nom de sécurité> d'après l'élément TLV.
usmUserCloneFrom	<valeur indifférente> – 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	<valeur indifférente> – écriture seulement
usmUserOwnAuthKeyChange	<valeur indifférente> – 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	<valeur indifférente> – écriture seulement
usmUserOwnPrivKeyChange	<valeur indifférente> – écriture seulement
usmUserPublic	<chaîne de longueur égale à zéro>
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 <Type de transfert> est réglé à 1, 2, ou 3 ou dont le champ <nom de sécurité> a une longueur égale à zéro.

Tableau 6-15/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 implémenter 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 un approvisionnement (objet cabhPsDevProvState à la valeur = 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 CableHome [voir § E.4]
- base MIB de portail CAP CableHome [voir § E.1]
- base MIB de portail CDP CableHome [voir § E.2]
- base MIB de portail CTP CableHome [voir § E.3]
- base MIB de sécurité CableHome [voir § E.5]
- base MIB d'objets de qualité de service CableHome [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]

Dans une passerelle résidentielle IPCable2Home ou dans tout autre dispositif comportant un dispositif PS intégré et un câblo-modem intégré, l'entité de gestion du câblo-modem et l'entité de gestion des services 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 PS, 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 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 PS, 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 portail (adresse IP de l'interface PS/WAN-Man) ou par l'adresse IP de l'interface PS/routeur-serveur du réseau LAN 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.

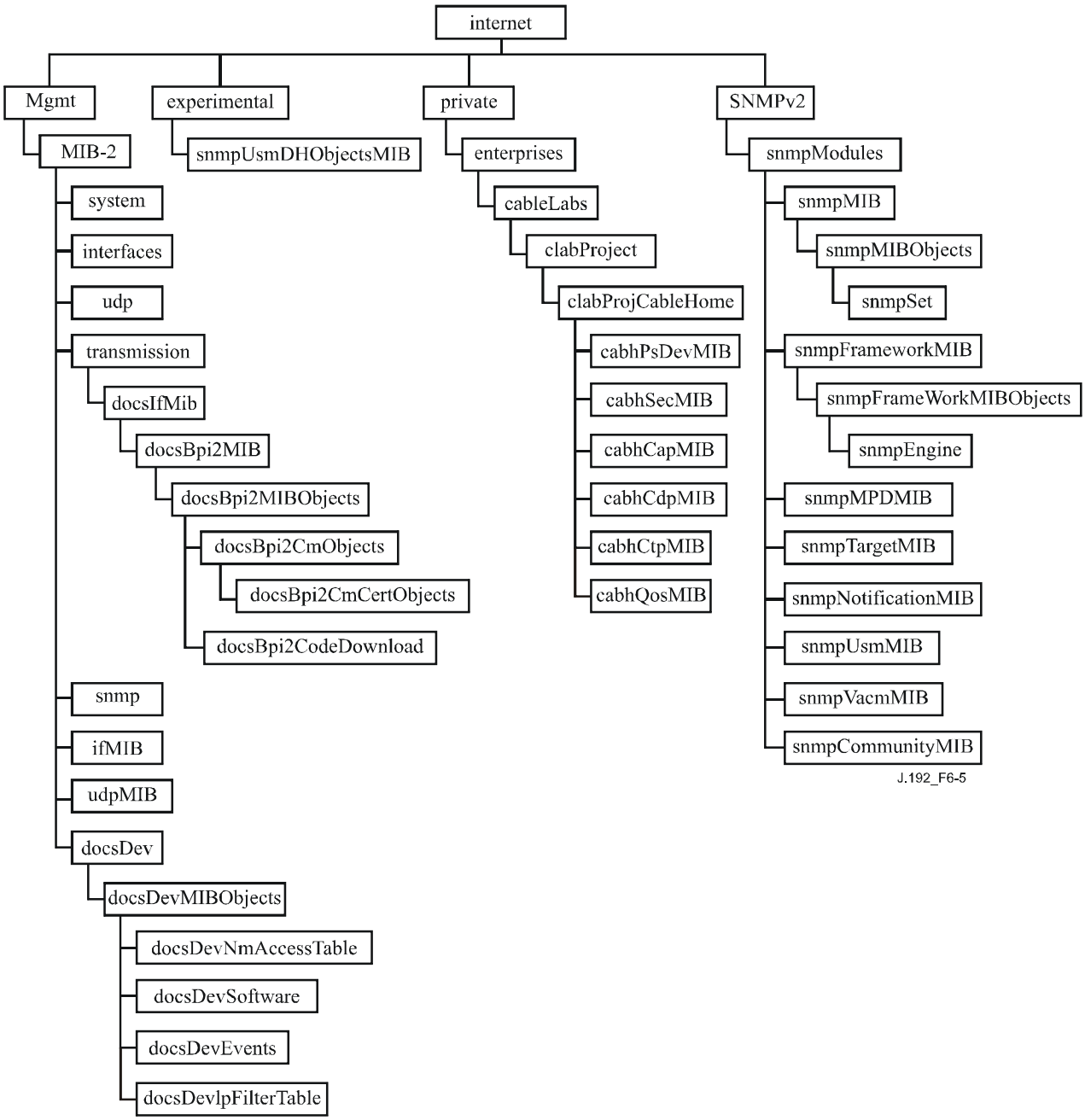


Figure 6-5/J.192 – Hiérarchie des bases MIB dans le modèle IPCable2Home

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 PS. 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 PS soient conformes aux exigences suivantes:

une instance de l'objet ifEntry DOIT exister pour l'interface entre l'élément PS et le réseau 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.

Une instance de l'objet ifEntry DOIT exister pour chaque interface physique avec un réseau LAN de l'élément de services PS.

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

Les interfaces de la table ifTable des services PS DOIVENT être numérotées comme représenté dans le Tableau 6-16.

Tableau 6-16/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 LAN
255	Interface avec côté résultant de réseau LAN

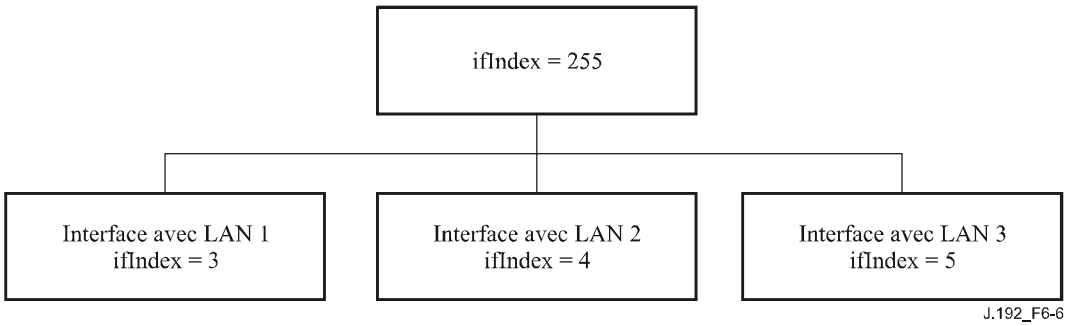
Si le statut ifAdminStatus d'une interface donnée a la valeur "down", cette interface NE DOIT PAS accepter ou réexpédier un quelconque trafic. L'objet ifAdminStatus correspondant à la valeur 255 de l'indice ifIndex DOIT assurer la commande administrative de toutes les interfaces avec un réseau LAN et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

Le dispositif PS DOIT attribuer la valeur other(1) aux entrées ifType de l'objet ifTable [RFC 2233] correspondant à l'indice ifIndex 255. 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.

Les compteurs d'interfaces avec un réseau WAN ayant les valeurs 1 et 2 d'indice ifIndex dans la table ifTable DOIVENT être partagés entre les deux interfaces. Les compteurs contenus dans la table ifTable pour la valeur d'indice ifIndex 255 PEUVENT être implémentés.

Le groupe-pile d'interfaces (ifStack) selon [RFC 2233] 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 LAN" et les sous-interfaces de couche inférieure avec un réseau LAN. La Figure 6-6 décrit l'utilisation du groupe ifStack dans un dispositif PS possédant trois interfaces avec un réseau LAN.



Implémentation du groupe ifStack dans cet exemple :

Groupe ifStack de couche supérieure	Groupe ifStack de couche inférieure
255	3
255	4
255	5

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

6.3.3.1.4.9 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 WAN à deux adresses de matériel. 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 6-17 ci-après.

Tableau 6-17/J.192 – PS ipNetToMediaTable

Adresse ipNetToMediaAddress	Adresse ipNetToMediaPhysAddress	Indice ipNetToMediaIfIndex
Adresse IP de réseau WAN-Man	Adresse matérielle de réseau WAN-Man	1
Adresse IP de réseau WAN-Data	Adresse matérielle de réseau WAN-Data	2
Adresse IP de serveur DHCP	Chaîne d'octets de longueur égale à zéro	255
Adresse IP de serveur DNS	Chaîne d'octets de longueur égale à zéro	255
Adresse IP du routeur-serveur	Chaîne d'octets de longueur égale à zéro	255

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 WAN. Les messages événementiels définis par IPCable2Home pour l'élément de services PS 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 LAN.

Signalisation des événements pour le domaine de réseau WAN

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 WAN 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 6-18 ont guidé la spécification de la fonction de signalisation d'événement de portail CMP.

Tableau 6-18/J.192 – Fonction de signalisation d'événement de portail CMP: directives de conception du système

Référence	Directives
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 transfert 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 transferts automatiques (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 6-19). 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 PS 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 implémenter 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 demande 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 = transfert seulement;
- 0x60 = (transfert + 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 6-19 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 bits 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 demande 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" en 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 transfert exigeant du serveur de réception qu'il accuse réception de l'arrivée d'une unité PDU de demande "InformRequest" par une unité PDU "InformResponse".

Quand un transfert normalisé du protocole SNMP est activé dans le dispositif PS, celui-ci DOIT envoyer des notifications pour chaque événement de cette catégorie dont la priorité est soit "erreur" ou "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 transfert SNMP DOIVENT être décrits dans une base MIB privée qui est distribuée avec le dispositif PS. Lors de la définition d'un transfert SNMP propre au vendeur, la déclaration "OBJECTS" de la définition du transfert privé DEVRAIT contenir au moins les objets décrits ci-dessous:

- EvLevel;
- EvIdText;
- EventThreshold (s'il y a un seuil pour le transfert);
- 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:

<niveau>PortalServicesElement[vendeur]: <eventId> texte

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 (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 actuelle reçue en format non valide":

<132>Elément des services portail[CABLEHOME]: <68000402> heure actuelle 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 PS 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 PS 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 de ce paragraphe qui concerne les exigences.

6.3.3.2.4.6 Priorités d'événement

Le document [RFC 2669] définit huit 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 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 6-19 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 6-19: Types de notification par défaut pour priorités événementielles des services PS, 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 6-19/J.192 – Types de notification par défaut pour priorités événementielles des services PS

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	CableHome
3) Critique	Oui	Non	Non	Non	CableHome
4) Erreur	Oui	Oui	Oui	Non	CableHome
5) Avertissement	Oui	Oui	Oui	Non	CableHome
6) Remarque	Non	Oui	Oui	Oui	CableHome
7) Information	Non	Non	Non	Non	CableHome 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 6-19.

6.3.3.2.4.7 Evénements normalisés

Le dispositif PS DOIT envoyer les transferts génériques suivants 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 transferts automatiques ne dépasse pas le seuil;
- l'état "stopAtThreshold(3)" (maintien au niveau du seuil) provoque la cessation de la transmission des transferts 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 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 PS. Le dispositif PS intégré, tel que défini dans le § 5.1.3.1, 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.

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 IPCable2Home et des dispositifs de passerelle résidentielle IPCable2Home;
- offrir aux câblo-opérateurs une visibilité sur les applications implémentées dans des dispositifs de serveur local IPCable2Home;
- assurer la coexistence et l'interopérabilité entre dispositifs PS, dispositifs de serveur local IPCable2Home et dispositifs IP de réseau LAN non conformes à la présente Recommandation.

NOTE – Les objectifs de découverte n'excluent pas l'utilisation d'autres méthodes, protocoles, etc. de découverte dans le réseau LAN mais ne visent qu'à spécifier les exigences relatives aux dispositifs conformes. Cependant, les dispositifs de serveur local IPCable2Home NE DOIVENT PAS interférer avec les dispositifs IP de réseau LAN non conformes au modèle IPCable2Home mais fonctionnant correctement.

Hypothèses

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

- les dispositifs de serveur local IPCable2Home, les dispositifs IP de réseau LAN et les dispositifs de passerelle résidentielle IPCable2Home implémentent la suite protocolaire du protocole Internet (IPv4);
- les serveurs locaux IPCable2Home implémentent un profil de dispositif en format XML comme décrit dans le § 6.5.3.1.3 et un profil de qualité de service en format XML comme décrit dans le § 10.3.2.4.2.1.

6.3.3.3.2 Fonction de découverte: directives de conception du système

Les directives de conception du système énumérées dans le Tableau 6-20 offrent des indications pour la mise au point de la spécification de la fonction de découverte du portail CMP.

Tableau 6-20/J.192 – Directives de conception du système de découverte PS

Référence	Directives de conception du système de découverte
Découverte 1	Les dispositifs PS et BP prendront en charge un protocole permettant de découvrir les dispositifs de serveur local IPCable2Home connectés au réseau LAN domestique.
Découverte 2	Le dispositif PS offrira au câblo-opérateur, sur demande, des informations sur les dispositifs ajoutés au réseau LAN domestique.
Découverte 3	Le dispositif PS offrira au câblo-opérateur, sur demande, des informations sur les applications implémentées dans des dispositifs de serveur local IPCable2Home.
Découverte 4	L'échange de messages du protocole de découverte à l'intérieur du réseau LAN domestique ne dégradera pas de façon appréciable la performance de ce réseau.
Découverte 5	La messagerie du protocole de découverte par le réseau LAN domestique ne se propagera pas dans le réseau WAN.

6.3.3.3.3 Fonction de découverte: description du système

L'objet de la fonction de découverte du portail CMP est d'offrir au câblo-opérateur des informations sur les dispositifs et applications disponibles sur un réseau LAN d'abonné.

La découverte spécifie le dispositif PS qui doit jouer le rôle de répertoire central des informations relatives aux dispositifs et applications disponibles dans le réseau LAN d'abonné. Les éléments

logiques de point BP spécifiés fournissent des informations spécifiques sur le dispositif dans lequel ces éléments résident et une liste des applications implémentées dans le dispositif dans lequel ces éléments résident.

La fonction de découverte comporte les deux étapes suivantes:

1) le dispositif PS apprend chaque adresse IP et chaque adresse MAC du serveur local IPCable2Home. Le dispositif PS apprend ces informations directement pour les dispositifs de réseau LAN-Trans quand il reçoit et répond à leurs demandes de découverte DHCP. Voir § 7.3.3.1.4: Exigences relatives au serveur CDS. Le dispositif PS est tenu d'apprendre ces informations à partir des dispositifs de réseau LAN-Pass afin d'assurer la fonctionnalité de commutation USFS (voir le § 8.3.3.4 concernant l'aperçu général et les exigences de la commutation de réexpédition sélective en amont), mais la présente Recommandation ne prescrit pas comment cette commutation doit être effectuée;
2) le dispositif PS acquiert les informations relatives aux attributs et aux applications du dispositif à partir de chaque point BP. Chaque point BP est tenu d'envoyer aux services portail son profil de dispositif et son profil de qualité de service. Cet envoi est effectué par un modèle "lancé par point BP", dans lequel le point BP envoie ces informations au portail CMP. Le point BP est autorisé à lancer ce transfert d'informations à tout instant mais est tenu de faire ainsi chaque fois qu'il acquiert ou renouvelle sa location d'adresse IP. Le dispositif PS reçoit ces informations et les mémorise, ce qui les rend accessibles au câblo-opérateur par la base MIB d'objets PsDev (voir § E.4).

Le dispositif PS conserve des informations sur le dispositif de passerelle résidentielle IPCable2Home, analogues au profil de dispositif BP, dans la base de données PS. Ces informations, permettant au câblo-opérateur de découvrir les attributs de la passerelle résidentielle IPCable2Home, sont disponibles en protocole SNMP par les objets sysDescr, sysName et sysLocation des bases MIB-2 [RFC 1213] et par le groupe de profils de dispositif PS de la base MIB d'objets PsDev (voir § E.4).

6.3.3.3.4 Exigences relatives à la fonction de découverte

Le dispositif PS DOIT stocker, dans la base de données PS, les informations relatives au profil de dispositif BP (voir § 6.5.3.1: Profil du dispositif de point extrême) reçues dans le message BP_Init à partir de chaque point BP, et DOIT les rendre accessibles au moyen de la table de profil de dispositif de serveur local IPCable2Home ou de profil de dispositif BP (objet cabhPsDevBpProfileTable) contenue dans la base MIB d'objets PsDev (voir § E.4). Le dispositif PS est également tenu de stocker les informations relatives aux applications reçues du profil de qualité de service provenant de la découverte de ces informations d'application. Voir § 10.3.2.4.2.

Le dispositif PS DOIT stocker ses attributs de profil de dispositif, énumérés ci-dessous, dans la base de données PS et DOIT les rendre accessibles à l'entité SNMP par le groupe de profils de dispositif PS contenu dans la base MIB d'objets PsDev (voir § E.4):

- type de dispositif (objet cabhPsDevPsDeviceType);
- adresse universelle du constructeur (objet cabhPsDevPsManufacturerUrl);
- adresse universelle du modèle de dispositif (objet cabhPsDevPsModelUrl);
- code de produit universel du dispositif (objet cabhPsDevPsModelUpc).

6.3.3.4 Fonction de messagerie LAN du portail CMP

La messagerie LAN se rapporte à l'échange de messages entre le dispositif PS et un dispositif de point BP. Bien que les systèmes SNMP soient prévalents dans les réseaux de transmission de données des câblo-opérateurs afin de surveiller et de configurer les systèmes de terminaison de câblo-modem (CMTS) et les câblo-modems (CM), le protocole SNMP n'est pas prévalent dans les dispositifs que les abonnés au service de transmission de données par câble ont connectés à leur

réseau LAN domestique. Par conséquent, le modèle IPCable2Home définit un protocole de messagerie domestique afin de répondre aux besoins des câblo-opérateurs concernant la prise en charge de leurs abonnés au service de transmission de données tout en conservant la compatibilité avec les protocoles de messagerie normalement implémentés dans les dispositifs de communication de données fondés sur un réseau LAN. Le présent paragraphe décrit la solution de messagerie par réseau local (LAN).

Il est critique de noter qu'un point BP pourrait résider dans le domaine du réseau LAN-Trans ou dans celui du réseau LAN-Pass. Un point BP situé dans le domaine du réseau LAN-Trans peut facilement adresser des paquets au dispositif PS, car l'adresse de l'interface PS/routeur-serveur (objet cabhCdpServerRouter) est celle de la passerelle par défaut du point BP situé dans le domaine du réseau LAN-Trans, transmise au point extrême dans le code 3 d'option DHCP. Cependant, un point BP situé dans le domaine du réseau LAN-Pass n'a aucune connaissance légitime de l'adresse IP de l'interface PS/routeur-serveur. Les messages de réseau LAN émis vers le dispositif PS à partir d'un point BP situé dans le domaine du réseau LAN-Trans peuvent utiliser l'adresse IP de l'interface PS/routeur-serveur comme adresse IP de destination. Une autre méthode doit être définie pour le point BP situé dans le domaine du réseau LAN-Pass.

Une méthode permettant d'assurer la messagerie de dispositif BP à dispositif PS dans le domaine du réseau LAN-Pass (qui est la méthode adoptée à cette fin) consiste à définir une adresse IP fixe et "notoire" dans le dispositif PS, que le point BP situé dans le domaine du réseau LAN-Pass utilisera comme destination. Etant donné que le dispositif PS est une dérivation de couche 2 pour les dispositifs situés dans le domaine du réseau LAN-Pass, la fonction de commutation USFS sera invoquée afin de capturer les messages envoyés par un point BP situé dans le domaine du réseau LAN-Pass à l'adresse IP de destination notoire. Le ou les paquets envoyés à l'adresse IP notoire du dispositif PS et capturés par la fonction de commutation USFS sont alors traités par le dispositif PS. L'adresse 192.168.0.1 est définie comme étant l'adresse IP "notoire" du dispositif PS que les points BP du domaine LAN-Pass sont tenus d'utiliser comme adresse IP de destination pour la messagerie BP-PS dans le réseau LAN. L'attribution par le serveur CDS de cette adresse IP notoire et fixe du dispositif PS aux dispositifs du domaine LAN-Trans n'est pas autorisée. L'adresse IP notoire du dispositif PS définie ci-dessus est égale à la valeur par défaut de l'objet cabhCdpServerRouter, mais l'adresse IP notoire du dispositif PS, définie pour la messagerie dans le réseau local, est fixe. Elle ne peut pas être changée, alors que la valeur de l'objet cabhCdpServerRouter peut être modifiée par fichier de configuration du PS ou par demande SET (mise à jour) du protocole SNMP. Le dispositif PS est tenu de répondre aux deux adresses si celles-ci sont différentes.

Etant donné qu'il pourrait résider dans l'un ou l'autre domaine d'adressage, un dispositif de point BP a besoin de prendre en charge la méthode d'adressage définie pour les points BP du domaine LAN-Trans ainsi que la méthode d'adressage définie pour les points BP du domaine LAN-Pass. En d'autres termes, les points BP sont tenus de prendre en charge les deux adressages: de domaine LAN-Trans à dispositif PS et de domaine LAN-Pass à dispositif PS. D'autre part, le dispositif PS est tenu d'accepter les messages destinés soit à l'adresse IP fixe et "notoire" du dispositif PS ou à l'adresse de l'interface PS/routeur-serveur (adresses qui pourraient être identiques ou différentes). Le point BP utilisera la présence ou l'absence de la valeur "CableHome1.1LAN-Trans" dans la sous-option 101 de l'option DHCP de code 43 contenue dans le message ACK du protocole DHCP reçu de son serveur DHCP afin de déterminer quelle méthode d'adressage il est tenu d'utiliser. Si cette valeur est présente dans la sous-option 101 de l'option DHCP de code 43, le point BP est tenu d'envoyer ses messages BP_Init à sa passerelle par défaut (celle de ce point BP), c'est-à-dire à l'adresse de l'interface PS/routeur-serveur. Si la valeur n'est pas présente dans le message ACK du protocole DHCP, le point BP est tenu d'envoyer ses messages BP_Init à l'adresse 192.168.0.1.

Le dispositif PS va répondre à un dispositif de point BP en utilisant, comme adresse de destination, l'adresse de point BP que le dispositif PS a reçue comme adresse IP d'origine, c'est-à-dire que le dispositif PS répond par un envoi à l'adresse à partir de laquelle il a reçu le message lancé par le

point extrême. A un certain point BP du domaine LAN-Pass, ce message paraît provenir d'un dispositif situé dans le domaine du réseau LAN-Trans.

La Figure 6-7 résume les exigences d'adressage du dispositif BP à PS pour un élément logique de point extrême conforme.

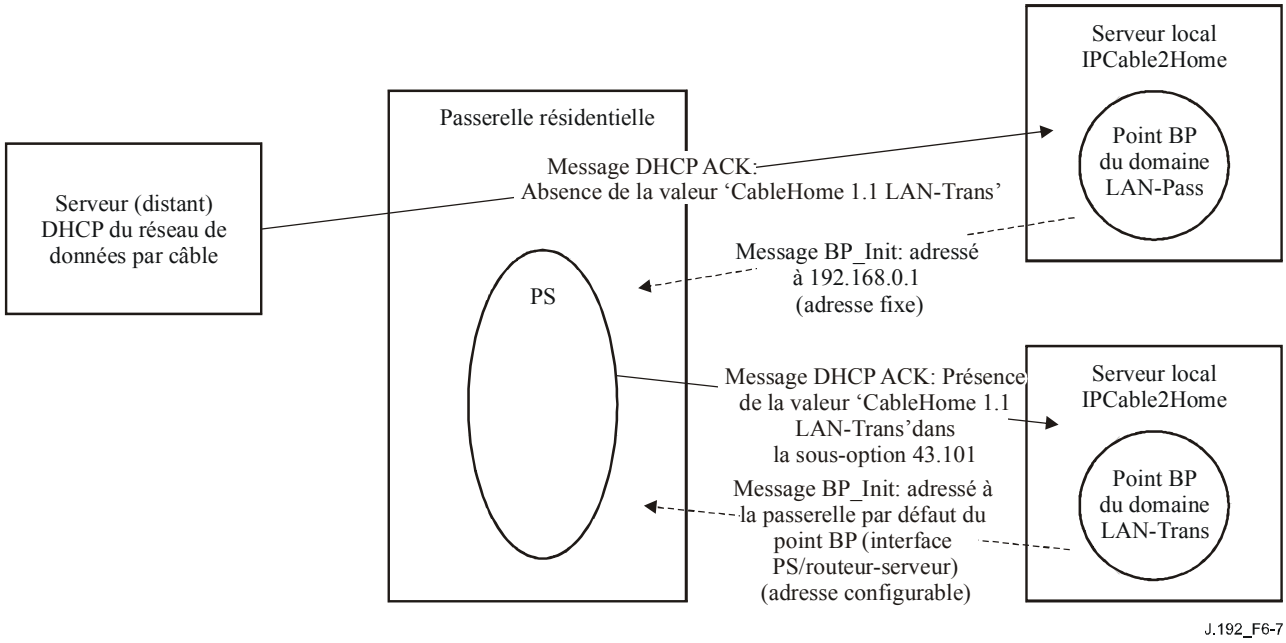


Figure 6-7/J.192 – Adressage du message BP_Init

6.3.3.4.1 Fonction de messagerie LAN: objectifs

Les objectifs de la fonction de messagerie LAN sont énumérés ci-dessous:

- prendre en charge les exigences relatives à la découverte de dispositifs et d'applications en permettant le transfert d'informations relatives au profil de dispositif, à partir d'éléments logiques de point BP contenus dans des dispositifs de serveur local IPCable2Home, vers l'élément de services PS contenu dans des dispositifs de passerelle résidentielle conformes;
- spécifier une méthode de normalisation des systèmes industriels ouverts pour l'échange de profil de dispositif et de profil de qualité de service priorisée entre l'élément logique de point extrême contenu dans chaque dispositif de serveur local IPCable2Home et l'élément logique des services portail contenu dans un dispositif de passerelle résidentielle conforme.

6.3.3.4.2 Fonction de messagerie LAN: directives de conception du système

Les directives de conception énumérées dans le Tableau 6-21 ont guidé la spécification de la fonction de messagerie LAN.

Référence	Directives
LAN Msg 1	Les dispositifs PS et BP prendront en charge un protocole permettant d'échanger des informations mises en format XML.
LAN Msg 2	Le protocole de messagerie LAN sera une norme ouverte.
LAN Msg 3	Le protocole de messagerie LAN sera aussi compatible que possible avec les dispositifs IP de réseau LAN et les dispositifs de passerelle résidentielle existants.

6.3.3.4.3 Fonction de messagerie LAN: description du système

En raison de sa flexibilité, de son acceptation par l'industrie et de ses capacités à communiquer des informations relatives à la configuration et aux états, c'est le langage XML [XML] qui a été choisi comme format des informations pour la messagerie de réseau LAN (BP-PS). Le langage XML a obtenu l'acceptation comme protocole de communication pour l'Internet car c'est un format ouvert, non soumis à des droits de propriété intellectuelle, et populaire pour son adaptation à des systèmes disparates. Les avantages du langage XML sont sa capacité de permettre la création, la modification, l'organisation et le stockage des informations dans toute forme adaptée aux besoins des messages de gestion. Par ses règles documentaires et sa prise en charge des caractères, le langage XML offre un avantage supplémentaire. Les capacités du langage XML en font un bonne solution pour les messages échangés entre dispositif PS et éléments logiques de point BP.

Le protocole simple d'accès aux objets (SOAP) [SOAP] appartient à la famille des protocoles associés au langage XML. C'est un protocole léger pour l'échange des informations contenues dans un environnement réparti et décentralisé. Le protocole SOAP est un protocole qui comporte trois parties:

- une enveloppe qui le définit comme un cadre permettant de décrire le contenu d'un message et quelle est la façon de le traiter;
- un ensemble de règles de codage pour exprimer des instances de types de données définis par l'application; et
- une convention pour représenter les appels et réponses de procédure distante.

Le protocole SOAP est spécifié pour l'échange de profils de dispositif et de profils de qualité de service entre le dispositif PS et des éléments logiques de point BP.

6.3.3.4.3.1 Protocole simple d'accès aux objets (SOAP)

Le codage d'un profil en langage XML n'est que la première étape de l'échange de messages entre passerelle résidentielle IPCable2Home et dispositifs de serveur local IPCable2Home. La présente Recommandation doit également offrir des conventions pour ce qui suit:

- type des informations à échanger;
- façon dont ces informations doivent être exprimées en langage XML;
- façon dont ces informations sont envoyées d'un élément logique à un autre.

Sans ces conventions, le dispositif PS et le point BP ne peuvent pas décoder les informations qu'ils reçoivent, même si elles sont codées en langage XML. Ces conventions préalables sont présentées par le protocole SOAP [SOAP]. Etant donné que la présente Recommandation ne spécifie le protocole SOAP que pour la messagerie dans un réseau LAN domestique d'abonné, tous les formats de la messagerie en protocole SOAP ne sont pas requis.

Couche de transport du protocole SOAP

Le protocole HTTP est le mécanisme de transport le plus couramment utilisé pour la messagerie du protocole SOAP. Le dispositif PS et le point BP sont tenus d'utiliser HTTP comme mécanisme de transport pour la messagerie du protocole SOAP afin d'assurer l'interopérabilité entre diverses implémentations de dispositifs PS et BP. Afin de prendre en charge ce procédé, le dispositif PS implémente un serveur HTTP commuté sur le point d'accès 80 et le point BP implémente un client du protocole HTTP. Le dispositif PS et le point BP sont également tenus d'avoir chacun une application de traitement SOAP en cours de fonctionnement.

Quand l'application de traitement SOAP fonctionnant sur un dispositif de point BP ou sur un dispositif PS reçoit un message du protocole SOAP, cette application traite ce message en exécutant les actions suivantes, dans l'ordre indiqué ci-dessous. Le point BP est empêché d'apporter des

modifications au profil de dispositif ou au profil de qualité de service à la suite de tout message SOAP autre que le message "BP_Init_Response" reçu du dispositif PS:

1) identifier toutes les parties du message SOAP destinées à cette application;

2) vérifier que toutes les parties obligatoires identifiées au cours de l'étape 1 sont prises en charge par l'application pour ce message et les traiter en conséquence. Si ce n'est pas le cas, il y a lieu d'ignorer le message. Le processeur a l'option d'ignorer les parties facultatives identifiées au cours de l'étape 1 sans affecter le résultat du traitement;

3) si applicable, envoyer un message de réponse comme défini dans les paragraphes suivants.

6.3.3.4.3.1.1 Formatage de message SOAP

Le présent paragraphe présente le format des messages SOAP nécessaires afin de respecter les exigences de messagerie dans le réseau local.

La messagerie en protocole SOAP qui intervient entre le dispositif PS et le point BP (afin d'échanger les profils de dispositif et de qualité de service) est lancée par le point extrême. Cette messagerie est désignée par le terme "*Opération BP_Init*".

La présente Recommandation définit deux balises de *code de confirmation* utilisées dans la messagerie par protocole SOAP. Les codes de confirmation associés à ces balises sont décrits ci-dessous:

Codes de confirmation

Un code de confirmation inséré dans un message indique les détails de succès ou d'échec concernant le message précédent dans la transaction. Une valeur négative indique une condition d'erreur. Les valeurs non négatives indiquent un succès. Une valeur positive différente de zéro indique un message informatif. Les codes de confirmation définis par le modèle IPCable2Home sont énumérés dans le Tableau 6-22.

Tableau 6-22/J.192 – Codes de confirmation pour la messagerie dans le réseau local CableHome

Code de confirmation	Signification
10	Présence d'un attribut non reconnu
0	Succès
–10	Absence d'un attribut requis
–20	Valeur inacceptable pour un attribut
–30	Détection d'erreurs multiples
–40	Erreur non classifiée ou définie par ailleurs

CableHome définit deux balises de code de confirmation: le code de confirmation de dispositif et le code de confirmation de qualité de service. Le code de confirmation de dispositif est celui qui est propre au profil de dispositif; le code de confirmation de qualité de service est celui qui est propre au profil de qualité de service. Le dispositif PS est autorisé à envoyer ces codes dans un ordre quelconque. Les valeurs de code de confirmation énumérées ci-dessus s'appliquent aussi bien comme codes de confirmation de dispositif que comme codes de confirmation de qualité de service.

6.3.3.4.3.2 Messagerie SOAP lancée par un point extrême (opération BP_Init)

La Figure 6-8 présente le diagramme de fluence pour les messages échangés entre un point BP et un dispositif PS pendant la messagerie SOAP lancée par un point extrême. Le message émis par le point BP vers le dispositif PS est un message *BP_Init*. Le message envoyé par un dispositif PS en réponse au message BP_Init est une réponse *BP_Init_Response*. La messagerie représentée dans la

Figure 6-8 montre un message BP_Init envoyé par le point BP à partir de ses informations de profil vers le dispositif PS (message *BP_Init*), ainsi que la réponse du dispositif PS à ce message BP_Init (message *BP_Init_Response*).

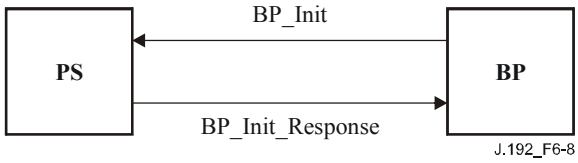


Figure 6-8/J.192 – Messagerie SOAP lancée par un point extrême: opération BP_Init

6.3.3.4.3.2.1 Format du message BP_Init

Le format du message BP_Init est décrit ci-dessous, par exemple au moyen du transfert du profil de dispositif BP et du profil de qualité de service vers le dispositif PS:

```
POST /DevQoSProfileService HTTP/1.1
HOST Adresse IP du dispositif PS
Content-Type: text/xml; charset="utf-8"
Content-Length: nnnn
SOAPAction: "/DevQoSProfileService"
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <ch:BP_Init xmlns:m= Adresse IP du dispositif PS >
      <ch:BP_IP>
        Adresse IP du dispositif BP
      </ch:BP_IP>
      <ch:DeviceProfile>
        Profil de dispositif à partir du dispositif BP
      </ch:DeviceProfile>
      <ch:QoSProfile>
        Profil de qualité de service à partir du dispositif BP
      </ch:QoSProfile>
    </ch:BP_Init>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

6.3.3.4.3.2.2 Format du message BP_Init_Response

Le format du message de réponse au message BP_Init, qui est le message "BP_Init_Response", est représenté ci-dessous, par exemple au moyen de la réponse au message BP_Init de profil de dispositif et de profil de qualité de service décrit ci-dessus.

HTTP/1.1 200 OK

Content-Type: text/xml; charset="utf-8"

Content-Length: nnnn

<SOAP-ENV:Envelope

xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"

SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>

<SOAP-ENV:Body>

<ch:BP_Init_Response xmlns:m= *Adresse IP du dispositif PS* >

<ch:DeviceConfirmationCode>*0*</ch:DeviceConfirmationCode >

<ch:QoSConfirmation Code>*0*</ch:QoSConfirmationCode>

<ch:QoSProfile> *Profil de qualité de service à partir du dispositif PS*
</ch:QoSProfile>

</ch: BP_Init_Response>

</SOAP-ENV:Body>

</SOAP-ENV:Envelope>

6.3.3.4.4 Exigences relatives à la fonction de messagerie de gestion de réseau local

Le dispositif PS DOIT implémenter un serveur HTTP conformément aux exigences relatives aux serveurs du document [RFC 2616], ce serveur étant commuté sur le point d'accès 80.

Le dispositif PS DOIT implémenter un analyseur de syntaxe XML conformément à [XML].

Le dispositif PS DOIT implémenter un analyseur de syntaxe SOAP conforme aux spécifications décrites dans [SOAP].

Le dispositif PS DOIT utiliser le protocole HTTP comme mécanisme de transport pour la messagerie en protocole SOAP afin d'assurer l'interopérabilité entre diverses implémentations de dispositifs PS et BP.

Le dispositif PS DOIT exploiter un service IP de transport du protocole SOAP sur protocole HTTP nommé DevQoSProfileService.

Le dispositif PS DOIT exécuter les actions énumérées dans l'ordre ci-dessous, quand il reçoit un message BP_Init SOAP:

1) identifier toutes les parties du message destinées aux services portail;
2) vérifier que le message reçu est formaté comme spécifié dans le § 6.3.3.4.3.2.1 et traiter le message. Si celui-ci ne contient pas tous les composants obligatoires, les ignorer. Le processeur a l'option d'ignorer les parties facultatives identifiées au cours de l'étape 1 sans affecter le résultat du traitement;
3) si le message BP_Init contenait un profil de dispositif et/ou un profil de qualité de service, envoyer un message BP_Init_Response comme défini dans le § 6.3.3.4.3.1.1: formatage de message SOAP;
4) si le message ne peut pas être traité parce qu'il est incorrectement formaté, qu'il contient une valeur non valide, ou n'est pas conforme à la spécification CableHome ou [SOAP] d'une autre façon, renvoyer un message de description d'état à l'expéditeur avec la valeur

appropriée du code de confirmation comme décrit dans le § 6.3.3.4.3.1.1: formatage de message SOAP.

Le dispositif PS DOIT observer les règles syntaxiques de protocole SOAP suivantes:

- un message SOAP DOIT être codé en langage XML;
- un message SOAP DOIT avoir une enveloppe SOAP;
- un message SOAP PEUT avoir un en-tête SOAP;
- un message SOAP DOIT avoir un corps SOAP;
- un message SOAP DOIT utiliser les espaces nominatifs d'enveloppe SOAP;
- un message SOAP DOIT utiliser l'espace nominatif de codage SOAP;
- un message SOAP NE DOIT PAS contenir de déclaration du type de document (DTD, *document type declaration*);
- un message SOAP NE DOIT PAS contenir d'instructions de traitement XML;
- le dispositif PS DOIT utiliser les espaces nominatifs par défaut ci-après:
  - pour la syntaxe d'enveloppe SOAP: http://schemas.xmlsoap.org/soap/envelope/
  - pour les types de codage et de données SOAP: http://schemas.xmlsoap.org/soap/encoding/
  - pour le message 'BP_Init_Response': adresse IP du dispositif PS.

Le dispositif PS DOIT accepter et traiter chaque message BP_Init qu'il reçoit avec une adresse IP de destination égale à 192.168.0.1 ou avec une adresse IP de destination égale à la valeur de l'objet cabhCdpServerRouter.

Le dispositif PS DOIT ignorer tout message BP_Init reçu par une quelconque interface PS/WAN ou avec une adresse IP de destination *non* égale à l'adresse 192.168.0.1 ou à la valeur de l'objet cabhCdpServerRouter.

Le dispositif PS DOIT répondre avec un message BP_Init_Response à chaque message BP_Init reçu par son interface avec un réseau LAN et transportant un profil de dispositif, un profil de qualité de service, ou à la fois un profil de dispositif et un profil de qualité de service. Le dispositif PS DOIT envoyer le message "BP_Init_Response" à l'adresse IP qui a été l'adresse IP d'origine du message BP_Init. Le dispositif PS n'est pas tenu de répondre aux messages BP_Init qui ne transportent ni un profil de dispositif ni un profil de qualité de service.

Si le message BP_Init reçu par le dispositif PS contient un profil de dispositif, le message "BP_Init_Response" envoyé par le dispositif PS DOIT contenir un code valide de confirmation de dispositif.

Si le message BP_Init reçu par le dispositif PS contient un profil de qualité de service, le message "BP_Init_Response" envoyé par le dispositif PS DOIT contenir un code valide de confirmation de qualité de service et peut contenir un profil de qualité de service.

Le dispositif PS NE DOIT PAS transmettre de message BP_Init_Response à la sortie d'une quelconque interface PS/WAN.

6.4 Elément logique des services portail – Portail d'essai CableHome (CTP)

6.4.1 Objectifs du portail CTP

Les objectifs du portail d'essai CableHome sont les suivants:

- permettre les diagnostics de dérangement de dispositif IP de réseau LAN et de serveur local CableHome;

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

6.4.2 Directives de conception du portail CTP

Les directives de conception du système de portail d'essai sont énumérées dans le Tableau 6-23. 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 6-23/J.192 – CTP: directives de conception du système

Référence	Directives
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'essai IPCable2Home) contient les "utilitaires distants" avec lesquels le système NMS peut collecter d'autres informations de dispositif de réseau LAN. Les essais doivent être effectués à distance, car contourner une fonction de traduction d'adresse de réseau (NAT, *network address translation*) dans un routeur risque d'être très difficile. Par exemple, un sondage par écho de réseau WAN à réseau LAN 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 LAN et de serveur local IPCable2Home sont définis sur la base des problèmes susceptibles d'être rencontrés dans les réseaux de type réseau domestique CableHome 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 PS et les dispositifs IP de réseau LAN 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 LAN domestique entre le dispositif PS et un dispositif IP de réseau LAN 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 6-23: *CTP: directives de conception du système* 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 LAN ou un serveur local IPCable2Home. Il envoie une rafale de paquets entre le dispositif PS et le dispositif IP de réseau LAN 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'incorporation d'une "fonction de bouclage" ou de "service d'écho" dans les dispositifs IP de réseau LAN et serveurs locaux IPCable2Home. L'Autorité d'attribution des numéros Internet (IANA, *Internet assigned numbers authority*) a attribué le point d'accès 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 traversée et le câblo-opérateur peut au besoin essayer directement des dispositifs IP de réseau LAN 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 LAN 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 point d'accès 7 comme point d'accès 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 WAN 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 point d'accès 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 LAN 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 millisecondes) 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 LAN 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 LAN 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 LAN ou un serveur local IPCable2Home dont l'adresse est transmise dans l'objet cabhCtpConnDestIp (le dispositif IP de réseau LAN 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 LAN 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 LAN 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 6-23 "CTP: Directives de conception du système" 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 LAN 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 LAN 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 demande de mise à jour envoyés par la console du système NMS du réseau câblé vers l'adresse de gestion des services 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 implémenté au moyen de la fonction "écho" du protocole de message de commande Internet (ICMP). Le portail CTP enverra une

demande d'écho ICMP et le dispositif IP de réseau LAN 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 LAN 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 LAN 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 LAN ou le dispositif de serveur local IPCable2Home dont l'adresse est transmise dans l'objet cabhCtpPingDestIp (le dispositif IP de réseau LAN 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 LAN 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 LAN 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 WAN 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).

6.5 Elément logique de point extrême – Point extrême de gestion (MBP)

Le paragraphe 5 définit le point extrême (point BP), qui est l'élément logique défini par le modèle IPCable2Home intégrant la fonctionnalité spécifiée par le modèle IPCable2Home d'un dispositif de serveur local IPCable2Home. Le point extrême de gestion (MBP) est l'élément logique du point extrême chargé des capacités de découverte définies par le modèle IPCable2Home du point extrême.

La découverte de dispositifs de serveur local IPCable2Home est la première étape de la gestion finale de la fonctionnalité spécifiée par le modèle IPCable2Home dans ces dispositifs. La présente Recommandation permet la découverte de dispositifs de serveur local CableHome par l'accès aux informations de profil par protocole HTTP à partir du portail CMP.

6.5.1 Objectifs du point MBP

L'objectif du point MBP est de répondre aux exigences du modèle IPCable2Home pour la découverte de dispositifs de serveur local IPCable2Home et pour la messagerie correspondante dans le réseau local. Le point MBP est tenu d'offrir au câblo-opérateur le profil de chaque dispositif de serveur local IPCable2Home, le dispositif PS jouant le rôle de mandataire.

6.5.2 Directives de conception du système de point MBP

Les directives de conception du système énumérées dans le Tableau 6-24 ont guidé la spécification du point MBP.

Tableau 6-24/J.192 – Directives de conception du système de point MBP

Référence	Directives
MBP 1	Le point MBP conservera des informations sur les attributs du dispositif de serveur local IPCable2Home dans lequel le point BP réside.
MBP 2	Le point MBP offrira des informations relatives aux dispositifs de serveur local IPCable2Home et à leurs applications au gestionnaire du système IPCable2Home, pendant le processus d'initialisation du point BP.
MBP 3	Le point MBP offrira périodiquement des informations relatives aux dispositifs de serveur local IPCable2Home et à leurs applications au gestionnaire du système IPCable2Home, après la fin du processus d'initialisation du point BP.

6.5.3 Description du système de point MBP

Le point BP est tenu de conserver un profil de dispositif comme décrit dans le § 6.5.3.1.3: Description du profil de dispositif, et un profil de qualité de service comme décrit dans le § 10.3.2.4.2.1: Schéma XML du profil de qualité de service.

Le point BP est également tenu d'envoyer le profil de dispositif aux services portail, ainsi que de fournir au gestionnaire du système IPCable2Home l'accès à des informations sur chaque attribut de dispositif de serveur local IPCable2Home, au moyen de la base MIB de dispositif PS (voir § E.4) par accès en protocole SNMP au réseau WAN de transmission de données par câble. En assurant l'accès aux informations relatives aux attributs de dispositif de serveur local IPCable2Home de cette manière, le point MBP répond aux exigences concernant la découverte de dispositifs.

Le point BP est également tenu de prendre en charge la messagerie dans le réseau local au moyen du transport du protocole SOAP par le protocole HTTP, en tant que moyen de transférer le profil de dispositif et le profil de qualité de service du point extrême aux services portail.

6.5.3.1 Profil du dispositif de point extrême

Le profil de dispositif et le profil de qualité de service sont des structures formatées en langage XML qui contiennent des informations sur le dispositif de serveur local IPCable2Home et sur les applications qu'il implémente. Le profil de dispositif sert à conserver et à communiquer des informations sur le dispositif de serveur local IPCable2Home. Le point BP est tenu d'implémenter un profil de dispositif et de fournir ses informations relatives au profil de dispositif aux services portail, qui rendent ces informations disponibles au moyen de la base MIB de dispositif PS (voir § E.4). Le système NMS du réseau de données du câblo-opérateur et d'autres organisations de prise en charge des abonnés peuvent obtenir des informations de base sur le dispositif de serveur local IPCable2Home par l'interrogation de la base MIB de dispositif PS dans le réseau de données par câble, au moyen de messages SNMP de demande de requête (GET).

6.5.3.1.1 Objectifs du profil de dispositif

Les objectifs du profil de dispositif de point extrême sont énumérés ci-dessous:

- rassembler des informations spécifiques et propres au dispositif de serveur local IPCable2Home implémentant le point extrême;
- offrir au gestionnaire du système IPCable2Home des informations sur le dispositif de serveur local IPCable2Home.

6.5.3.1.2 Profil de dispositif: directives de conception du système

Les directives de conception du système énumérées dans le Tableau 6-25 ont guidé la spécification du profil du dispositif de point MBP.

Tableau 6-25/J.192 – Profil du dispositif de point MBP: directives de conception du système

Référence	Directives
MBP DevProf 1	Le point MBP conservera un ensemble d'informations propres aux dispositifs, concernant le dispositif de serveur local IPCable2Home dans lequel le point BP réside.
MBP DevProf 2	Le format des informations propres aux dispositifs observera une norme ouverte.
MBP DevProf 3	Le format des informations propres aux dispositifs conservées par un point MBP sera compatible avec les systèmes d'exploitation de dispositif IP de réseau LAN et sera flexible afin de tenir compte de toute sorte ou quantité d'informations propres aux dispositifs; il sera aussi compatible que possible avec les protocoles et les tendances de l'industrie.

6.5.3.1.3 Description du profil de dispositif

La présente Recommandation spécifie l'implémentation d'un profil de dispositif et d'un profil de qualité de service dans les éléments logiques de point BP assurant la découverte de dispositifs de serveur local IPCable2Home et assurant l'approvisionnement de priorités de qualité de service dans les points BP. Le profil de dispositif et le profil de qualité de service sont des structures formatées en langage XML. Le profil de dispositif contient un ensemble d'attributs qui décrivent le dispositif de serveur local IPCable2Home. Un profil de dispositif comprend les attributs spécifiés par le modèle IPCable2Home. Il pourrait comprendre également les attributs spécifiés par le vendeur. Le profil de qualité de service contient une liste de numéros de point d'accès définis par l'autorité IANA qui reflètent les applications implémentées par chaque dispositif, la priorité attribuée à chaque application et des informations facultatives sur la priorité de qualité de service concernant l'adresse IP de destination et le numéro de point d'accès de destination. Le profil de dispositif est décrit dans le présent paragraphe. Le profil de qualité de service est décrit dans le § 10.3.2.4.2.1, Schéma XML du profil de qualité de service.

Le Tableau 6-26 présente une description de haut niveau du profil de dispositif requis pour les éléments de point BP.

Tableau 6-26/J.192 – Profil du dispositif de point extrême: attributs

Nom d'attribut	Type d'attribut	Usage
Type de dispositif	Chaîne	requis
Constructeur	Chaîne	requis
Adresse URL du constructeur	Chaîne	facultatif
Révision du matériel	Chaîne	requis
Options du matériel	Chaîne	facultatif
Numéro de série	Chaîne	requis
Nom du modèle	Chaîne	facultatif
Numéro du modèle	Chaîne	facultatif
Adresse URL du modèle	Chaîne	facultatif
Code UPC du modèle	Chaîne	facultatif
Système d'exploitation logicielle du modèle	Chaîne	requis

Tableau 6-26/J.192 – Profil du dispositif de point extrême: attributs

Nom d'attribut	Type d'attribut	Usage
Version logicielle du modèle	Chaîne	requis
Type d'interface LAN (ifType IANA)	Chaîne	requis
Numéro de priorité d'accès au support	Entier	requis
Emplacement physique	Chaîne	facultatif
Adresse physique	Chaîne	requis

Détails des attributs d'un profil de dispositif:

L'attribut *Type de dispositif* peut avoir une seule des valeurs suivantes: passerelle résidentielle IPCable2Home ou serveur local IPCable2Home.

L'attribut *Constructeur* est le nom du constructeur du dispositif.

L'attribut *Adresse URL du constructeur* est l'adresse universelle du site IP du constructeur.

L'attribut *Révision du matériel* est une chaîne attribuée par le constructeur afin d'identifier de façon univoque la révision du matériel d'un produit spécifique.

L'attribut *Options du matériel* est une chaîne attribuée par le constructeur afin d'identifier des caractéristiques facultatives du produit matériel, implémentées dans ce produit.

L'attribut *Numéro de série* est le numéro de série d'identification unique du dispositif de serveur local IPCable2Home, attribué par le constructeur du dispositif.

L'attribut *Nom du modèle* est le nom du modèle de dispositif de serveur local IPCable2Home ou un autre nom identificateur qui est attribué par le constructeur du dispositif.

L'attribut *numéro du modèle* est le numéro du modèle ou une autre valeur identificatrice qui est attribuée par le constructeur du dispositif.

L'attribut *Adresse URL du modèle* est l'adresse universelle du site IP du modèle.

L'attribut *Code UPC du modèle* est la valeur de code de produit universel attribuée au dispositif.

L'attribut *Système d'exploitation logicielle du modèle* est le système d'exploitation implémenté par le dispositif.

L'attribut *version logicielle du modèle* est la version du logiciel fonctionnant dans le dispositif.

L'attribut *Type d'interface LAN* est une chaîne contenant la valeur IANAifType [IANA1] pour la technique de mise en réseau de la couche 2 dans le modèle OSI de l'ISO, implémentée par le produit.

L'attribut *Numéro de priorité d'accès au support* renvoie au numéro de priorité d'accès au support que l'interface avec un réseau LAN du dispositif de serveur local IPCable2Home prend en charge. Cet attribut et ses usages sont décrits en détail dans le § 10, qualité de service.

L'attribut *Emplacement physique* est une valeur qui peut être attribuée par le propriétaire du dispositif et qui indique l'emplacement physique du dispositif, comme *Bureau* ou *Salon*.

L'attribut *Adresse physique* est l'adresse matérielle du dispositif, comme l'adresse de commande d'accès au support (MAC) d'un dispositif de type 802.3.

6.5.3.1.4 Profil de dispositif en format XML

Le profil de dispositif en format XML prescrit par le modèle IPCable2Home est représenté ci-dessous.

```
<xs: complexType name="ch:device">
        <xs:element name="ch:deviceType"                    type="xs:string"/>
        <xs:element name="ch:manufacturer"                  type="xs:string"/>
        <xs:element name="ch:manufacturerURL"               type="xs:string"/>
        <xs:element name="ch:hardwareRevision"              type="xs:string"/>
        <xs:element name="ch:hardwareOptions"               type="xs:string"/>
        <xs:element name="ch:serialNumber"                  type="xs:string"/>
        <xs:element name="ch:modelName"                     type="xs:string"/>
        <xs:element name="ch:modelNumber"                   type="xs:string"/>
        <xs:element name="ch:modelURL"                      type="xs:string"/>
        <xs:element name="ch:modelUPC"                      type="xs:string"/>
        <xs:element name="ch:modelSoftwareOS"               type="xs:string"/>
        <xs:element name="ch:modelSoftwareVersion"          type="xs:string"/>
        <xs:element name="ch:lanInterfaceType"              type="xs:string"/>
        <xs:element name="ch:numberMediaAccessPriorities"   type="xs:int"/>
        <xs:element name="ch:physicalLocation"              type="xs:string"/>
        <xs:element name="ch:physicalAddress"               type="xs:string"/>
    </xs:complexType>
```

6.5.3.1.5 Exigences relatives au profil de dispositif

Le point BP DOIT implémenter un profil de dispositif comme décrit dans le § 6.5.3.1.4, compatible avec les règles de formatage XML décrites dans [XML].

Le point BP DOIT remplir l'attribut "Type de dispositif" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec la chaîne "serveur local CableHome" (sans les guillemets).

Le point BP DOIT remplir l'attribut "Constructeur" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec une chaîne dont la valeur identifie le constructeur du dispositif de serveur local IPCable2Home dans lequel le point BP réside.

Le point BP DOIT remplir l'attribut "Révision du matériel" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec une chaîne dont la valeur représente précisément le numéro de révision du matériel du constructeur pour le dispositif de serveur local IPCable2Home dans lequel le point BP réside.

Le point BP DOIT remplir l'attribut "Numéro de série" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec une chaîne dont la valeur est égale au numéro de série identifiant de façon univoque le dispositif de serveur local IPCable2Home dans lequel le point BP réside.

Le point BP DOIT remplir l'attribut "Système d'exploitation logicielle du modèle" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec une chaîne dont la valeur représente précisément le système d'exploitation logicielle implémenté dans le dispositif de serveur local IPCable2Home dans lequel le point BP réside.

Le point BP DOIT remplir l'attribut "Version logicielle du modèle" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec une chaîne dont la valeur

représente précisément la version logicielle du dispositif BP implémentée dans le dispositif de serveur local IPCable2Home dans lequel le point BP réside.

Le point BP DOIT remplir l'attribut "Type d'interface avec le réseau LAN" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec une chaîne dont la valeur est égale au type IANAifType [IANAType] représentant la technique de réseau local prise en charge par le dispositif de serveur local IPCable2Home dans lequel le point BP réside.

Le point BP DOIT remplir l'attribut "Numéro de priorité d'accès au support" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec un entier dans l'étendue 1 à 8 dont la valeur est égale au numéro de la priorité d'interface avec un réseau LAN qui est pris en charge par le dispositif de serveur local IPCable2Home dans lequel le point BP réside.

Le point BP PEUT remplir l'attribut "Adresse URL du constructeur" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec une chaîne dont la valeur identifie précisément et de façon univoque une adresse universelle pour le constructeur du dispositif de serveur local IPCable2Home dans lequel le point BP réside.

Le point BP PEUT remplir l'attribut "Options du matériel" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec une chaîne dont la valeur représente les options du matériel du dispositif de serveur local IPCable2Home dans lequel le point BP réside.

Le point BP PEUT remplir l'attribut "Nom du modèle" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec une chaîne dont la valeur identifie précisément et de façon univoque le nom du modèle du constructeur pour le dispositif de serveur local IPCable2Home dans lequel le point BP réside.

Le point BP PEUT remplir l'attribut "Numéro du modèle" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec une chaîne dont la valeur identifie précisément et de façon univoque le numéro du modèle du constructeur pour le dispositif de serveur local IPCable2Home dans lequel le point BP réside.

Le point BP PEUT remplir l'attribut "Adresse URL du modèle" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec une chaîne dont la valeur identifie précisément et de façon univoque une adresse universelle pour le dispositif de serveur local IPCable2Home dans lequel le point BP réside.

Le point BP PEUT remplir l'attribut "Code UPC du modèle" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec une chaîne dont la valeur identifie précisément et de façon univoque le code de produit universel pour le dispositif de serveur local IPCable2Home dans lequel le point BP réside.

Le point BP PEUT remplir l'attribut "Emplacement physique" du profil de dispositif de point extrême (voir § 6.5.3.1.4, "Profil de dispositif en format XML") avec une chaîne dont la valeur identifie l'emplacement physique du dispositif de serveur local IPCable2Home dans lequel le point BP réside.

6.5.3.2 Fonction de messagerie LAN du point MBP

6.5.3.2.1 Fonction de messagerie LAN du point MBP: objectifs

Les objectifs de la fonction de messagerie LAN du point MBP sont énumérés dans le § 6.3.3.4.1, "Fonction de messagerie LAN: objectifs".

6.5.3.2.2 Fonction de messagerie LAN du point MBP: directives de conception du système

Les directives de conception du système de la fonction de messagerie LAN du point MBP sont énumérées dans le Tableau 6-21, "Fonction de messagerie LAN – Directives de conception du système".

6.5.3.2.3 Fonction de messagerie LAN du point MBP: description du système

La fonction de messagerie LAN du point MBP est comme décrit dans le § 6.3.3.4.3, "Fonction de messagerie LAN: description du système".

6.5.3.2.4 Fonction de messagerie LAN du point MBP: exigences

Le point BP DOIT implémenter un répondeur du service d'écho, de telle sorte que le point BP renvoie immédiatement en écho à son expéditeur tout paquet IP reçu au point d'accès 7, bit pour bit, en changeant seulement l'adresse IP et le point d'accès d'origine pour l'adresse IP et pour le point d'accès, et vice versa.

Le point BP DOIT implémenter les types de message ICMP d'écho et de réponse d'écho (type 8 et type 0) ainsi que les types de message ICMP de marqueur temporel et de réponse de marqueur temporel (type 13 et type 14) comme décrit dans le document [RFC 792] et répondre correctement aux demandes de sondage par écho reçues par une interface quelconque.

Le point BP DOIT implémenter un client du protocole HTTP conformément aux exigences relatives aux clients du document [RFC 2616].

Le point BP DOIT implémenter un analyseur de syntaxe XML conformément à [XML].

Le point BP DOIT implémenter un analyseur de syntaxe SOAP conformément à [SOAP].

Le point BP DOIT utiliser le protocole HTTP comme mécanisme de transport pour la messagerie en protocole SOAP afin d'assurer l'interopérabilité entre diverses implémentations de dispositifs PS et BP.

Si le point BP a reçu la sous-option 101 de l'option DHCP de code 43 contenant la chaîne 'CableHome 1.1 LAN-Trans' dans le message ACK du protocole DHCP, ce point BP DOIT adresser chaque message BP_Init à sa passerelle par défaut (valeur de l'option DHCP 3 reçue dans le message ACK du protocole DHCP).

Si le point BP n'a pas reçu la sous-option 101 de l'option DHCP de code 43 contenant la chaîne 'CableHome 1.1 LAN-Trans' dans le message ACK du protocole DHCP, ce point BP DOIT adresser chaque message BP_Init à l'adresse IP 192.168.0.1.

Le point BP NE DOIT PAS transmettre de message BP_Init à une fréquence supérieure à une fois toutes les 20 secondes.

Le point BP NE DOIT PAS transmettre de message BP_Init à un instant non spécifiquement cité dans le § 10.4.1.4.1.1, "Transfert des informations de point BP au dispositif PS au moyen du message BP_Init".

Le point BP NE DOIT PAS transmettre de message BP_Init à une adresse autre que l'adresse de la passerelle par défaut du point BP ou 192.168.0.1.

Le point BP DOIT observer les règles syntaxiques suivantes du protocole SOAP:

- un message SOAP DOIT être codé en langage XML;
- un message SOAP DOIT avoir une enveloppe SOAP;
- un message SOAP peut avoir un en-tête SOAP;
- un message SOAP DOIT avoir un corps SOAP;
- un message SOAP DOIT utiliser les espaces nominatifs d'enveloppe SOAP;
- un message SOAP DOIT utiliser l'espace nominatif de codage SOAP;
- un message SOAP NE DOIT PAS contenir de déclaration du type de document (DTD);
- un message SOAP NE DOIT PAS contenir d'instructions de traitement XML;
- le point BP DOIT utiliser les espaces nominatifs par défaut ci-après:

– pour la syntaxe d'enveloppe SOAP: http://schemas.xmlsoap.org/soap/envelope/
– pour les types de codage et de données SOAP: http://schemas.xmlsoap.org/soap/encoding/
– pour le message 'BP_Init': l'adresse IP du dispositif PS.

Le point BP DOIT exécuter les actions suivantes dans l'ordre énuméré quand il reçoit un message du protocole SOAP:

1) identifier toutes les parties du message SOAP destiné au point extrême;
2) vérifier que le message reçu est formaté comme spécifié dans le § 6.3.3.4.3.2.1 et traiter le message. Si le message ne contient pas tous les composants obligatoires, ignorer le message. Le processeur a l'option d'ignorer les parties facultatives identifiées au cours de l'étape 1 sans affecter le résultat du traitement;
3) si le message ne peut pas être traité parce qu'il est incorrectement formaté, contient une valeur non valide, ou n'est pas conforme à la présente Recommandation ou au protocole [SOAP] d'une autre façon, le point BP DOIT réémettre le message BP_Init par un total de trois tentatives sur une période de trois minutes. Si le point BP ne reçoit pas de message valide BP_Init_Response après avoir émis trois messages BP_Init dans une période de trois minutes, ce point BP DOIT arrêter ses réessais jusqu'à ce qu'il renouvelle ou acquière de nouveau sa location d'adresse IP.

6.5.3.3 Fonction de découverte de point MBP

6.5.3.3.1 Fonction de découverte de point MBP: objectifs

L'objectif de la fonctionnalité IPCable2Home de découverte de point MBP est d'offrir au gestionnaire du système IPCable2Home des informations sur le dispositif de serveur local IPCable2Home dans lequel le point BP réside.

6.5.3.3.2 Fonction de découverte de point MBP: directives de conception du système

Les directives de conception énumérées dans le Tableau 6-27 offrent des indications pour la spécification de la fonction de découverte de point MBP.

Tableau 6-27/J.192 – Fonction de découverte de point MBP – Directives de conception du système

Référence	Directives
MBP Disc 1	Le point MBP fournira au câblo-opérateur des informations spécifiques au sujet du serveur local IPCable2Home dans lequel il réside, le dispositif PS jouant le rôle de mandataire.
MBP Disc 2	Le point MBP fournira au câblo-opérateur des informations sur les applications implémentées par un dispositif de serveur local IPCable2Home, le dispositif PS jouant le rôle de mandataire.

6.5.3.3.3 Fonction de découverte de point MBP: description du système

Chaque point BP est tenu d'implémenter un profil de dispositif en format XML comme décrit dans le § 6.5.3.1.4, "Profil de dispositif en format XML". Chaque point BP est également tenu d'implémenter un profil de qualité de service comme décrit dans le § 10.3.2.4.2.1, "Schéma XML du profil de qualité de service". Quand le point BP est opérationnel et a achevé le processus d'initialisation, il est tenu d'envoyer des informations sur le profil de dispositif et sur le profil de qualité de service aux services portail au moyen de la messagerie dans le réseau local décrite dans le § 6.3.3.4, "Fonction de messagerie LAN du portail CMP". En fournissant au dispositif PS des informations sur le profil de dispositif et sur le profil de qualité de service, le point BP permet au

câblo-opérateur de découvrir les attributs du dispositif de serveur local IPCable2Home dans lequel le point BP réside et les applications qu'il fait fonctionner, le dispositif PS jouant le rôle de mandataire pour le système de gestion de réseau du câblo-opérateur.

6.5.3.3.4 Exigences relatives à la fonction de découverte

Dès réception d'un message ACK du protocole DHCP [RFC 2131] adressé à lui-même, le point BP DOIT transmettre un message BP_Init comme décrit dans le § 6.3.3.4.3.2, contenant son profil de dispositif et son profil de qualité de service dans le corps du message. Le point BP envoie le message BP_Init à d'autres instants, y compris quand son profil de qualité de service est rafraîchi comme décrit dans le § 10.4.1.4.1, "Echange d'informations du côté LAN".

Si le point BP ne reçoit pas de message valide BP_Init_Response dans le délai d'une minute après l'envoi par le point BP d'un message BP_Init, le point BP DOIT immédiatement réexpédier le message BP_Init avec le profil de dispositif BP et le profil de qualité de service dans le corps du message, en répétant le processus sur un total de trois tentatives ou jusqu'à ce que le point BP reçoive un message valide BP_Init_Response, selon ce qui se produit en premier.

Si le point BP ne reçoit pas de message valide BP_Init_Response après avoir envoyé une séquence de trois messages BP_Init, le point BP DOIT attendre de recevoir le prochain message ACK du protocole DHCP [RFC 2131] et DOIT répéter le processus.

7 Utilitaires d'approvisionnement

7.1 Introduction/Aperçu général

L'élément de services PS et les dispositifs IP de réseau LAN 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 d'approvisionnement 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 LAN. Les trois utilitaires d'approvisionnement définis afin d'accomplir cette tâche sont énumérés ci-dessous:

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

7.1.1 Objectifs

Les objectifs des utilitaires d'approvisionnement sont énumérés ci-dessous:

- permettre au dispositif PS d'acquérir une adresse réseau sur son interface avec un réseau WAN 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 WAN, à utiliser pour l'échange de trafic entre dispositifs IP de réseau LAN 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 actuelle à partir des services d'heure actuelle 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 LAN et à des dispositifs de serveur local IPCable2Home;
- permettre au dispositif PS d'attribuer des paramètres de configuration à des dispositifs IP de réseau LAN et à des dispositifs de serveur local IPCable2Home.

7.1.2 Hypothèses

Les hypothèses de fonctionnement des utilitaires d'approvisionnement sont énumérées ci-dessous:

- les dispositifs IP de réseau LAN et les dispositifs de serveur local IPCable2Home implémentent un client du protocole DHCP comme défini par RFC 2131;
- le système d'approvisionnement du réseau câblé implémente un serveur DHCP comme défini par RFC 2131;
- si le serveur DHCP du système d'approvisionnement 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 LAN 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 portail sera réalisée par le téléchargement d'un fichier de configuration du 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 d'approvisionnement

7.2.1 Modes d'approvisionnement

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

Tableau 7-1/J.192 – Modes d'approvisionnement

	Mode DHCP	Mode SNMP	Mode CableHome 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 177.	Ne reçoit aucun fichier d'informations de configuration. Reçoit des valeurs valides pour les sous-options 3, 6 et 51 de l'option 177.	Ne reçoit aucune information du fichier de configuration ni aucune option 177, ou reçoit une combinaison non valide d'informations du fichier de configuration et de sous-options de l'option 177.

Tableau 7-1/J.192 – Modes d'approvisionnement

	Mode DHCP	Mode SNMP	Mode CableHome inactif
Déclenchement du fichier de configuration du 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 PS	Le téléchargement du fichier de configuration du PS est requis	Le téléchargement du fichier de configuration du PS n'est pas requis	Le fichier de configuration du PS n'est pas requis

Le comportement spécifié des utilitaires d'approvisionnement dépend du mode d'approvisionnement dans lequel le dispositif PS fonctionne.

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

7.2.2 Description de l'architecture d'approvisionnement

L'architecture d'approvisionnement est illustrée dans la Figure 7-1. Les éléments de services PS 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.

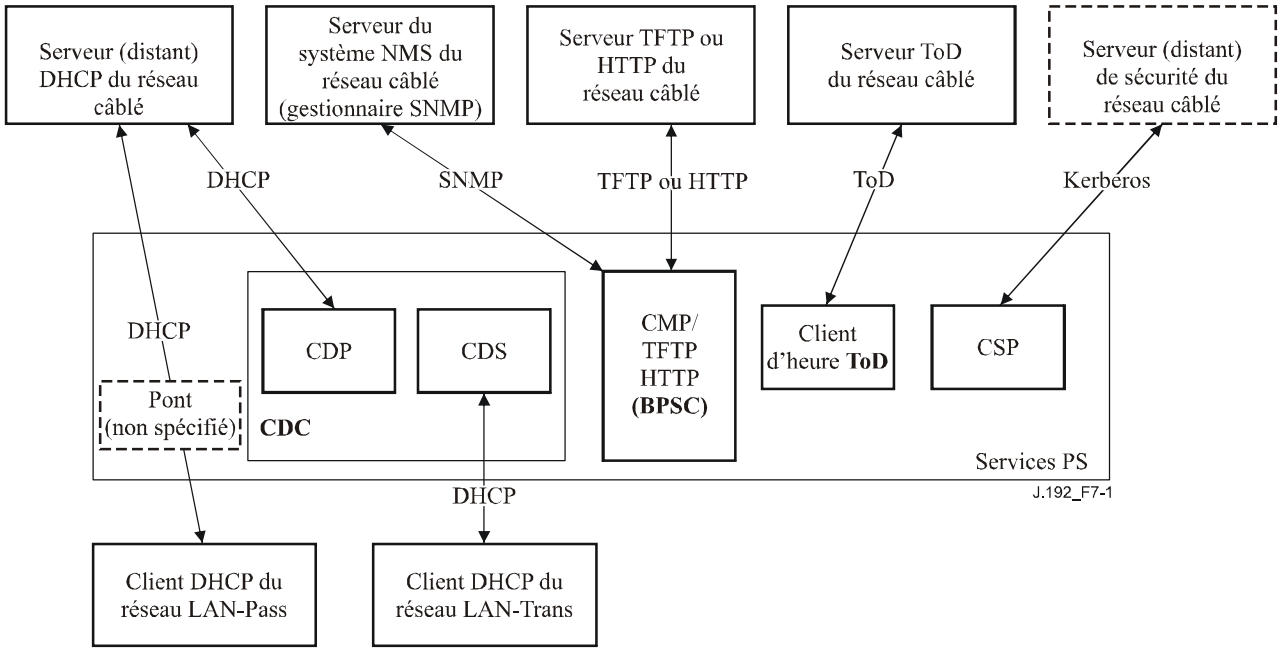


Figure 7-1/J.192 – Architecture d'approvisionnement

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

Le portail DHCP IPCable2Home (CDP) est un sous-élément de l'élément logique des services 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 LAN et à des dispositifs de serveur local IPCable2Home dans le réseau LAN. C'est un des trois utilitaires d'approvisionnement 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 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 LAN, 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 LAN.
CDP 4	Il est préférable que les adresses des dispositifs IP de réseau LAN 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 LAN dans le secteur LAN-Trans.
CDP 6	Les communications domestiques 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 LAN 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 LAN 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 PS;
- 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 LAN.

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 PS exige une adresse IP dans le réseau LAN domestique pour son rôle de routeur dans le réseau LAN (voir § 8, "Traitement de paquet et conversion d'adresse"), de serveur DHCP (CDS) et de serveur DNS (voir § 9, "Résolution du nom"). Pour chacune de ces trois fonctions de l'élément de services portail en tant que serveur distant et routeur, une adresse IP de réseau LAN est sauvegardée dans la base de données PS. Chaque adresse peut être atteinte par un objet de base MIB différent, dont la liste figure ci-dessous et dans le Tableau 7-2.

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

La valeur par défaut de l'objet cabhCdpServerRouter est 192.168.0.1. Les valeurs par défaut de l'objet cabhCdpServerDnsAddress et de l'objet cabhCdpServerDhcpAddress sont donc égales à l'adresse 192.168.0.1. L'un quelconque de ces trois objets de base MIB du portail CDP peut être modifié sans affecter les deux autres.

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 LAN situés dans le secteur LAN-Trans. Le serveur CDS échange des messages DHCP avec les dispositifs IP de réseau LAN 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 LAN.

Les dispositifs IP de réseau LAN 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 LAN implantés dans le secteur LAN-Pass.

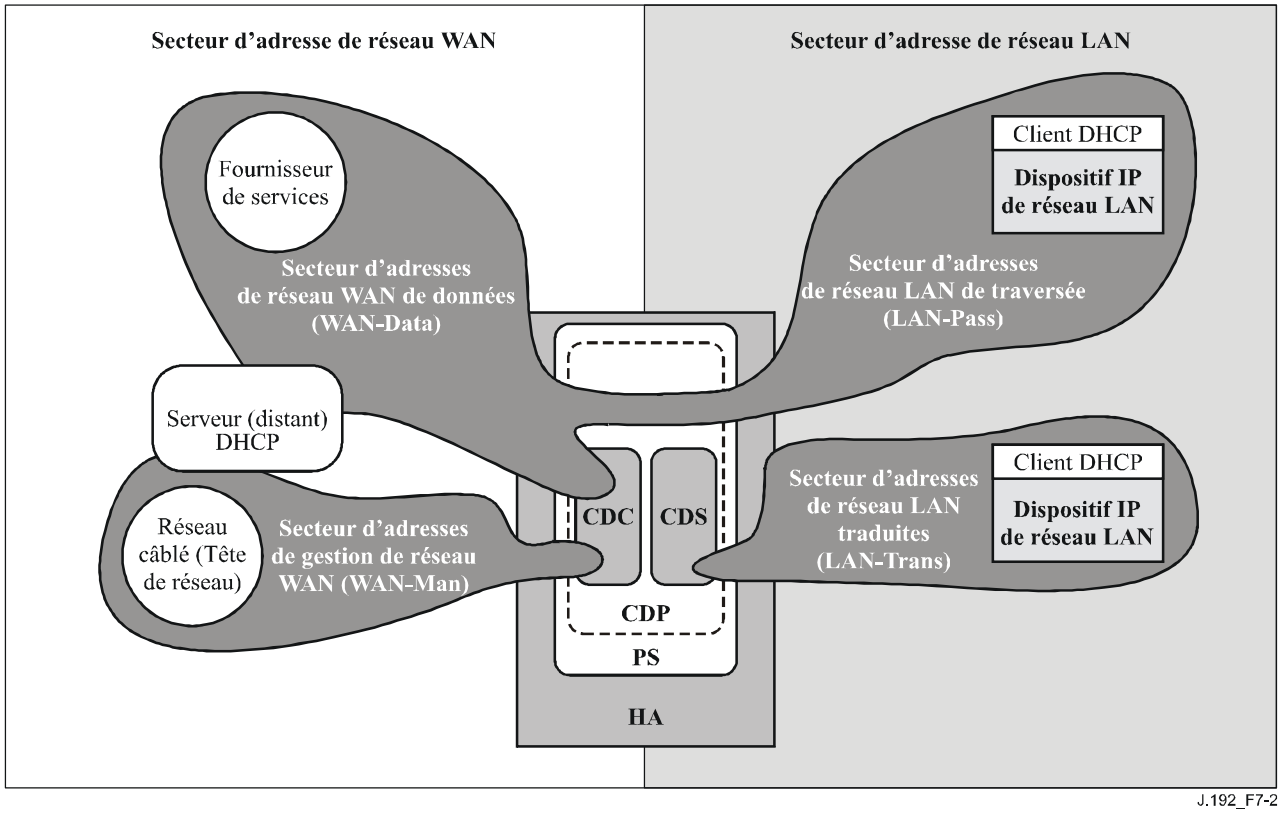


Figure 7-2/J.192 – Fonctions du portail CDP

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 LAN dans le secteur LAN-Trans. Il est également chargé de fournir aux dispositifs IP de réseau LAN des informations de configuration par codes d'option DHCP, comme spécifié dans le document 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 LAN dans le secteur LAN-Trans conformément aux réglages de la base MIB du portail CDP et conformément au document RFC 2131;
- attribuer des informations de configuration conformément au document 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 LAN 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 LAN 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
CDS 1	Permettre aux dispositifs IP de réseau LAN 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 LAN 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 le document 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 LAN 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 LAN. 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 LAN, indépendamment de l'état de connexité du réseau WAN;
- le nombre d'adresses fournies par le serveur CDS à des dispositifs IP de réseau LAN 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 LAN 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 actuelle à partir du serveur temporel (ToD, *time of day*), le serveur CDS fait appel à l'instant de début par défaut du service 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 LAN, 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 à la traversée et si le processus d'approvisionnement 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 LAN 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 WAN, 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 traversée ou en mode mixte de dérivation/acheminement (voir § 8.3.4.3, "Exigences relatives au mode de traversée, pour plus de détails"). Dans ces cas, les interactions DHCP surviendront directement entre dispositifs IP de réseau LAN 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 le document 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 approvisionnées par le système NMS et qui sont offertes par le serveur CDS à des dispositifs IP de réseau LAN munis d'une adresse LAN-Trans. Les options DHCP approvisionnées 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 approvisionnées 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 LAN 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 le document RFC 2132, section 2.1. Les valeurs par défaut des options DHCP approvisionnées 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 LAN 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 LAN 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 LAN.

La table d'adresses LAN du portail CDP (objet cabhCdpLanAddrTable) contient la liste des paramètres associés aux adresses attribuées aux dispositifs IP de réseau LAN 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 LAN 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 LAN 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 LAN 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 LAN. 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 LAN.

Les entrées de table de portail CDP approvisionnées 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 le document RFC 2131, section 4.3.

Le dispositif PS DOIT prendre en charge l'attribution d'adresse dynamique et manuelle conformément au document 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 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 LAN approvisionnées 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 LAN activés par le dispositif PS, indépendamment de l'état de connexité du réseau WAN.

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 LAN 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 d'approvisionnement IPCable2Home"):

- quand le dispositif PS doit fonctionner en mode d'approvisionnement 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 PS;
- quand le dispositif PS doit fonctionner en mode d'approvisionnement 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 d'approvisionnement DHCP et que la première tentative de téléchargement ou de traitement du fichier de configuration du PS échoue;
- quand le dispositif PS doit fonctionner en mode d'approvisionnement SNMP et que la tentative d'authentification auprès du serveur de centre KDC échoue;
- quand le dispositif PS doit fonctionner en mode d'approvisionnement SNMP et est appelé à télécharger un fichier de configuration du 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 PS échoue.

Le dispositif PS DOIT attribuer – à chaque dispositif IP de réseau LAN 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 LAN.

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 LAN 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 LAN 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 LAN 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 approvisionné.

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 LAN recevant une adresse dans le secteur d'adresses du réseau LAN-Trans.

Si le câblo-opérateur approvisionne 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 approvisionnée, au dispositif IP de réseau LAN dont l'adresse matérielle correspond à l'identificateur cabhCdpLanAddrClientID approvisionné, en réponse à un message DHCP DISCOVER reçu de ce dispositif IP de réseau LAN.

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

Si le serveur CDS reçoit, d'un dispositif IP de réseau LAN, 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 LAN quand une location active est créée pour le dispositif IP de réseau LAN.

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 les 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 les 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 à la construction du serveur CDS" du Tableau 7-4, "Options DHCP du serveur CDS", si l'option DHCP n'a pas été approvisionnée avec d'autres valeurs.

Si le mode primaire de traitement de paquet du dispositif PS (objet cabhCapPrimaryMode) a été réglé à "traversée" et que le processus d'approvisionnement 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 WAN, ni émettre de messages DHCP à partir d'une quelconque interface avec un réseau WAN.

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 LAN.

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".

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 à la construction 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 temporel	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: "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 s	cabhCdpServerLeaseTime
54	Identificateur de serveur (distant)	M	192.168.0.1	cabhCdpServerDhcpAddress
55	Liste de demande de paramètres	M	N/A	N/A

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 à la construction du serveur CDS	Nom de l'objet de base MIB
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 dans les messages OFFER et ACK du protocole DHCP qu'il envoie *seulement* aux dispositifs IP de réseau LAN conformes au modèle CableHome. La conformité au modèle CableHome des dispositifs IP de réseau LAN est indiquée par la présence de la chaîne *CableHome1.1BP* 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 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 d'approvisionnement dans lequel le dispositif PS doit fonctionner;
- acquérir une ou plusieurs location(s) d'adresse IP pour mappage sur des dispositifs IP de réseau LAN 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
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 LAN 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 le document 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 d'approvisionnement dans lequel les services 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 portail CDP prend en charge diverses options DHCP et extensions BOOTP de vendeur, autorisées par RFC 2132.

Le client CDC détermine le mode d'approvisionnement 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".

Fonctionnement en mode d'approvisionnement DHCP

Le dispositif PS fonctionne en mode d'approvisionnement DHCP s'il reçoit un nom de fichier valide pour le fichier de configuration du 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 51 de l'option DHCP 177.

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

- exige qu'un fichier de configuration du PS soit téléchargé à partir d'un serveur de fichiers dans le réseau câblé;
- utilise par défaut les versions SNMPv1 et SNMPv2c pour la messagerie de gestion;
- 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;
- peut être configuré de façon à utiliser la fonction de sécurité de la couche Transport (TLS) [RFC 2246] afin d'authentifier et de chiffrer le fichier de configuration du PS (voir § 11.9, "Sécurité du fichier de configuration du PS en mode d'approvisionnement DHCP");
- 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 d'approvisionnement SNMP

Le dispositif PS fonctionne en mode d'approvisionnement SNMP s'il reçoit l'option DHCP 177 avec les champs de sous-option 3, 6 et 51, *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 d'approvisionnement SNMP est résumé ci-dessous:

- n'est pas tenu de télécharger un fichier de configuration du 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 PS à tout instant mais il fonctionnera au moyen des paramètres par défaut à la construction sans téléchargement d'un fichier de configuration du 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");
- 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);
- fait appel à l'échange de messages par serveur Kerberos avec un serveur de centre de distribution de clés dont l'adresse IP est fournie aux services 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 d'approvisionnement SNMP");
- peut être configuré de façon à recevoir et à traiter les messages SNMPv1 et SNMPv2c ainsi que les messages SNMPv3.

Mode CableHome inactif

Le dispositif PS fonctionne en mode CableHome inactif s'il ne reçoit pas la combinaison du champ "*file*", du champ "*siaddr*" ou des sous-options de l'option DHCP de code 177 afin du configurer en mode d'approvisionnement DHCP, ni la combinaison de ces champs et sous-options afin du configurer en mode d'approvisionnement SNMP.

Quand le dispositif PS doit fonctionner en mode CableHome 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 d'approvisionnement et de gestion CableHome:

- ignorer tout message SNMP reçu par une quelconque interface avec un réseau WAN;
- désactiver la fonction de client TFTP;
- désactiver la signalisation des événements par serveur SYSLOG;
- fermer le temporisateur d'approvisionnement;
- 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 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.

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 WAN 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

L'élément de services PS peut avoir une ou plusieurs adresses IP de réseau WAN associées à une ou 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 WAN 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 WAN 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 WAN 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 WAN

Afin d'activer la compatibilité avec autant de systèmes d'approvisionnement de câblo-opérateur que possible, le client CDC prendra en charge les modes configurables suivants des adresses de réseau WAN.

Mode 0 d'adresse WAN

L'élément de services PS utilise une seule adresse IP de réseau WAN, acquise par protocole DHCP au moyen de l'adresse matérielle du réseau WAN-Man. L'élément de services PS 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 "Traversée" (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 WAN, la valeur de l'objet cabhCdpWanDataIpAddrCount est zéro.

Mode 1 d'adresse de réseau WAN

L'élément de services PS utilise une seule adresse IP de réseau WAN, acquise par protocole DHCP au moyen de l'adresse matérielle de réseau WAN-Man. L'élément de services PS a une seule interface IP/WAN-Man et une seule interface IP/WAN-Data. Ces deux interfaces se partagent une même 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 WAN, la valeur de l'objet cabhCdpWanDataIpAddrCount est zéro.

Mode 2 d'adresse de réseau WAN

L'élément de services PS 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 PS 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 WAN par écriture d'une valeur différente de zéro dans l'objet cabhCdpWanDataIpAddrCount, au moyen du fichier de configuration du PS ou d'une demande 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 MSO, 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 MSO dans l'objet cabhCdpWanDataAddrClientId qu'indiqué par la valeur de l'objet cabhCdpWanDataIpAddrCount, c'est-à-dire que l'opérateur MSO a approvisionné 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 MSO dans l'objet cabhCdpWanDataAddrClientId qu'indiqué par la valeur de l'objet cabhCdpWanDataIpAddrCount, c'est-à-dire que l'opérateur MSO a approvisionné 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 WAN, 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 approvisionne 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 PS ou de message(s) SNMP de demande de mise à jour (SET);

2) le câblo-opérateur configure le portail CDP de façon à fonctionner en mode 2 d'adresse de réseau WAN par écriture, dans l'objet cabhCdpWanDataIpAddrCount, d'une valeur différente de zéro au moyen du fichier de configuration du 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 WAN comme décrit au cours de l'étape 2, le dispositif PS vérifie si des valeurs d'identificateur de client ont été approvisionnées 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 approvisionné, 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 approvisionnées, c'est-à-dire si les entrées de l'objet cabhCdpWanDataAddrClientId n'existent pas ou si le nombre de valeurs d'identificateur de client approvisionnées 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 approvisionnés, 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 approvisionné 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 approvisionné 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=<0xFF);

   si certains identificateurs de client ont été approvisionnés 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 approvisionné. Si les identificateurs de client approvisionnés 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 approvisionné.

Exemple dans le cas où des identificateurs de client ont été approvisionnés par le système NMS (trois valeurs d'identificateur de client approvisionnées, objet cabhCdpWanDataIpAddrCount à la valeur = 5):

adresse matérielle indiquée de réseau WAN-Data: 0xCDCDCDCDCDCD;

premier identificateur de client approvisionné pour la première adresse IP de réseau WAN-Data: 0x0A0A0A0A0A1A;

deuxième identificateur de client approvisionné pour la deuxième adresse IP de réseau WAN-Data: 0x0A0A0A0A0A2A;

troisième identificateur de client approvisionné 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 d'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 approvisionnés 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 le document RFC 2131.

Le dispositif PS DOIT implémenter une fonction de client du protocole TFTP conformément aux exigences relatives aux clients figurant dans le document RFC 1350.

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 WAN: 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 PS DOIT avoir des adresses matérielles d'interface avec un réseau WAN 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 le document 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 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.

Le dispositif PS DOIT utiliser l'adresse matérielle de l'interface PS/WAN-Man 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.

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.

La sous-option 11 de l'option 43 du protocole DHCP est un paramètre propre au dispositif qui est défini par la présente Recommandation. Ce paramètre indique si une adresse est actuellement demandée dans le secteur de gestion PS/WAN-Man ou dans le secteur de données PS/WAN-Data.

Le Tableau 7-6 indique comment le dispositif PS DOIT régler les valeurs pour la sous-option 11 de l'option 43 du protocole DHCP dans ses interfaces avec un réseau WAN.

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

Dans le cas d'un dispositif PS intégré avec un câblo-modem, celui-ci et l'élément de services PS 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 PS 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 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 s.a. 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 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 cabhSecFwPolicyFileCurrentVersion
Demande DHCP d'adresse de réseau WAN-Data pour services portail intégrés		

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
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 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 s.a. 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 cabhSecFwPolicyFileCurrentVersion
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 PS 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, 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 temporel	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

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)
15	Nom de domaine	M
23	Temps par défaut de recherche de relais	M
26	Unité MTU d'interface	M
43	Informations propres au vendeur	M
50	Adresse IP demandée	M
51	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
177	Sous-option 3 – Adresse d'entité SNMP du fournisseur de services	M
177	Sous-option 6 – Nom du secteur Kerberos du secteur d'approvisionnement	M
177	Sous-option 51 – 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
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 temporel	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
51	Durée de location d'adresse IP	M
54	Identificateur de serveur (distant)	M
177	Option de configuration de client compatible avec le modèle PacketCable	M

Le dispositif PS DOIT prendre en charge une adresse d'entité SNMP de fournisseur de services (sous-option 3 de l'option DHCP 177) configurée comme une adresse IPv4. Le format de la sous-option 3 de l'option DHCP 177 est décrit ci-dessous:

la longueur de la sous-option DOIT être de 5 octets. L'octet de longueur DOIT être suivi par un seul octet qui indique le type d'adresse spécifique qui suit. Cet octet de type d'adresse DOIT être réglé à 1 afin d'indiquer une adresse IPv4. L'octet de type DOIT être suivi par 4 octets d'adresse IPv4.

Code	Longueur	Type	Adresse			
3	5	1	a1	a2	a3	a4

Le dispositif PS DOIT prendre en charge un nom du secteur Kerberos (option DHCP 177, 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 177 est décrit ci-dessous.

Le nom du secteur DOIT être codé en fonction du nom du secteur de style domanial décrit dans le document RFC 1510. Le nom du secteur DOIT être écrit entièrement en majuscules et être conforme à la syntaxe décrite dans le document RFC 1035, section 3.1. La sous-option est codée comme suit:

Code	Longueur	Nom du secteur Kerberos			
6	n	k1	k2	. . .	k_n

Le dispositif PS DOIT prendre en charge une adresse IP du serveur Kerberos (option DHCP 177, sous-option 51). La sous-option d'adresse IP du serveur Kerberos 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 de serveur de centre KDC sera conforme au format d'une adresse IPv4 utilisant le point d'accès par défaut. La longueur minimale de cette option est de 4 octets et cette longueur DOIT toujours être un multiple de 4. Si de multiples serveurs KDC sont

énumérés, ils DOIVENT l'être en ordre de priorité décroissante. La sous-option d'adresse de serveur de centre KDC est codée comme suit:

Code	Longueur	Adresse 1				Adresse 2		
51	n	a1	a2	a3	a4	a1	a2	...

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 LAN. L'adresse IP "de repli" de réseau WAN-Data NE DOIT être utilisée qu'en tant que partie d'adresse IP de réseau WAN du nuplet de conversion dynamique NAT ou NAPT d'un mappage d'adresse de conversion C-NAT ou C-NAPT, selon le cas. Si le dispositif PS doit fonctionner en mode 2 d'adresse de réseau WAN et est tenu d'essayer d'acquérir de multiples locations d'adresse IP de réseau WAN-Data et si le dispositif PS n'est pas en mesure d'acquérir ces connexions louées après avoir émis trois messages DHCP DISCOVER (conformément aux procédures DHCP de réessai spécifiées dans le § 7.3.3.2.4, "Exigences relatives au client CDC"), le dispositif PS DOIT utiliser l'adresse IP "de repli" de réseau WAN-Data en tant que partie WAN de chaque Nuplet de conversion dynamique NAT, jusqu'à ce que le dispositif PS obtienne la ou les locations nécessaires d'adresse IP de réseau WAN-Data à partir d'un serveur DHCP, par l'intermédiaire d'une interface PS/WAN.

Le dispositif PS NE DOIT PAS utiliser l'adresse IP "de repli" de réseau WAN-Data quand le dispositif PS est configuré de façon à fonctionner en mode primaire de traitement de paquet par traversée.

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 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 s 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 WAN pour son interface WAN-Man, le dispositif PS DOIT toujours insérer son adresse matérielle de réseau WAN 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 d'approvisionnement 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 WAN, 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 WAN toutes les 10 s jusqu'à ce qu'une location DHCP valide soit accordée pour l'adresse IP de réseau WAN-Man.

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 177, la sous-option 3, la sous-option 6 ou la sous-option 51 (combinaison valide 1), le dispositif PS DOIT régler l'objet cabhPsDevProvMode à la valeur dhcpmode(1) et essayer de synchroniser l'heure actuelle avec le serveur temporel ToD comme décrit dans le § 7.5.4, "Fonction de client d'heure actuelle: exigences".

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 177 avec une adresse IP valide (adresse d'entité SNMP) dans la sous-option 3, un nom valide du secteur Kerberos dans la sous-option 6 et une adresse IP valide (adresse IP du serveur Kerberos) dans la sous-option 51 et 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 actuelle 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".

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 177 du message ACK en protocole DHCP reçu du serveur DHCP dans le réseau câblé, une combinaison quelconque des sous-options 3, 6 et 51, 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'événement approprié et rediffuser un message DHCP DISCOVER (c'est-à-dire relancer la séquence d'approvisionnement si cette condition d'échec apparaît) – en répétant jusqu'à 5 fois la totalité de ce processus 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, reçoit dans l'option DHCP 177 du message ACK en protocole DHCP issu du serveur DHCP dans le réseau câblé, une combinaison quelconque, des sous-options 3, 6 et 51, d'un champ 'siaddr' et d'un champ 'file' autre que les deux combinaisons valides décrites ci-dessus, le dispositif PS DOIT 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 l'approvisionnement IPCable2Home (mode CableHome inactif):

- désactiver l'agent SNMP (portail CMP) pour l'accès à l'interface avec un réseau WAN. Laisser l'agent SNMP activé pour les messages reçus par l'intermédiaire de l'interface avec un réseau LAN (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 WAN décrits dans le § 7.3.3.2.3.2;

- fermer le temporisateur d'approvisionnement;
- 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 approvisionnés, y compris ceux qui ont été extraits des valeurs d'objets de base MIB persistants. Le dispositif PS fonctionnant en mode CableHome inactif NE DOIT PAS réinitialiser ses objets de base MIB aux réglages par défaut à la construction.

Quand un dispositif PS fonctionnant en mode 2 d'adresse de réseau WAN (comme décrit dans le § 7.3.3.2) doit acquérir une adresse IP de réseau WAN-Data pour une interface WAN-Data qui utilisera une adresse IP distincte de celle de l'interface WAN-Man, le dispositif PS DOIT inclure l'option d'identificateur de client (objet cabhCdpWanDataAddrClientId) dans le message DHCP DISCOVER. Afin d'activer ces identificateurs uniques de client du réseau WAN-Data, le client CDC DOIT permettre au système NMS de créer des entrées d'objet cabhCdpWanDataAddrClientId dans la table cabhCdpWanDataAddrTable.

Si un dispositif PS doit fonctionner en mode 2 d'adresse de réseau WAN (comme décrit dans le § 7.3.3.2), le dispositif PS DOIT essayer d'obtenir une adresse IP, par protocole DHCP, pour chaque identificateur unique de client (objet cabhCdpWanDataAddrClientId) dans l'objet cabhCdpWanDataAddrTable, jusqu'à la limite définie par l'objet cabhCdpWanDataIpAddrCount.

Le dispositif PS DOIT continuer à réexpédier le message diffusé DHCP DISCOVER en implémentant un algorithme exponentiel d'attente aléatoire de données compatible avec celui qui est décrit dans le document RFC 2131, jusqu'à ce qu'il obtienne une adresse IP valide d'interface PS/WAN-Man et/ou une location d'adresse IP valide d'interface PS/WAN-Data, selon les besoins.

Si le dispositif PS (client CDC) réussit à acquérir l'adresse IP du réseau WAN-Man (c'est-à-dire s'il reçoit un message DHCP ACK à partir d'un serveur DHCP par l'interface PS/WAN-Man) lors de sa première tentative et si le dispositif PS doit fonctionner en mode d'approvisionnement DHCP, le dispositif PS DOIT essayer de synchroniser son heure actuelle avec le serveur ToD par l'envoi une demande de ToD comme décrit dans le § 7.5.4, avant d'essayer un téléchargement du fichier de configuration du PS.

Si le dispositif PS (client CDC) ne réussit pas à acquérir l'adresse IP du réseau WAN-Man (c'est-à-dire la demande DHCP expire conformément au document RFC 2131) à son premier essai, le dispositif PS DOIT déclencher le serveur CDS (c'est-à-dire lancer le fonctionnement du serveur CDS) de façon que celui-ci puisse répondre aux demandes DHCP provenant de dispositifs IP de réseau LAN situés dans le secteur LAN-Trans.

La fonction de client CDC du dispositif PS ne DOIT répondre aux messages DHCP – ou en envoyer – que par l'intermédiaire d'une interface avec un réseau WAN.

Quand la location DHCP du réseau WAN-Man arrive à expiration, le dispositif PS DOIT supprimer toutes les entrées extraites des rangées de la table cabhCdpWanDnsServerTable.

7.4 Fonction de services portail – Configuration globale des services portail (BPSC)

7.4.1 Objectifs de la fonction de configuration globale des services 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 portail: directives de conception du système

Les directives identifiées dans le Tableau 7-12 ont guidé la spécification des capacités pour la fonction de configuration globale des services portail:

Tableau 7-12/J.192 – Configuration globale des services 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 portail: description du système

La configuration globale des services portail est normalement effectuée pendant l'approvisionnement de l'élément de services PS, 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 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 PS" ou "Fichier de configuration du pare-feu". L'utilitaire de configuration globale des services 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 portail (BPSC) est un utilitaire que les opérateurs MSO 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 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 d'approvisionnement SNMP n'a pas besoin d'avoir un fichier de configuration du PS chargé avant de pouvoir fonctionner. On suppose qu'un dispositif PS fonctionnant en mode d'approvisionnement 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 PS chargé. Cependant, un dispositif PS acceptera et traitera un fichier de configuration du PS lorsqu'on lui en fournira un.

7.4.4 Fonction de configuration globale des services portail: exigences

Un dispositif PS fonctionnant en mode d'approvisionnement DHCP DOIT télécharger et traiter un fichier de configuration du PS.

Un dispositif PS fonctionnant en mode d'approvisionnement SNMP DOIT être capable de fonctionner sans fichier de configuration du PS, mais DOIT être capable de télécharger et de traiter un fichier de configuration du 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 d'approvisionnement DHCP ou SNMP.

Les réglages d'objet de base MIB transmis dans le fichier de configuration du 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 7-13.

Tableau 7-13/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 § 7.3.3.1.1 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 ou de pare-feu peut contenir de nombreux paramètres différents, mais les seuls paramètres qui DOIVENT être inclus dans un fichier de configuration quelconque 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).

Afin de permettre une gestion uniforme du dispositif PS, celui-ci DOIT prendre en charge un fichier de configuration dont la longueur peut atteindre 64K octets.

Chaque élément de services PS 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 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 ignorer 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 [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

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 liaison variable (VarBind) du protocole SNMP, comme défini dans le document 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 demande SNMP de mise à jour (SET).

Type	Longueur	Valeur
28	Variable	liaison variable

Le dispositif PS DOIT traiter la liaison variable, contenue dans un nuplet TLV de type 28, comme si elle faisait partie d'une demande SNMP de mise à jour (SET) avec les précautions suivantes:

- il DOIT traiter la requête comme étant entièrement autorisée (il ne peut pas refuser la requête 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 contenues dans un fichier de configuration DOIVENT être traitées comme si elles étaient simultanées. Chaque valeur VarBind DOIT être limitée à 65535 octets.

7.4.4.1.6 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)

7.4.4.1.7 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)

7.4.4.1.8 Valeur de démarrage SNMPv3

(Voir section C.1.2.8, DOCSIS 1.1 – RFI Specification, SP-RFIv1.1-I09-020830.)

Les éléments de services portail conformes DOIVENT comprendre le nuplet TLV suivant avec ses sous-éléments et être capables d'ouvrir l'accès SNMPv3 aux services 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.

7.4.4.1.8.1 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.

7.4.4.1.8.2 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 au document 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.

7.4.4.1.9 Récepteur de notification SNMP

Type	Longueur	Valeur
38	n	Composite

Cet élément de fichier de configuration du 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 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.

7.4.4.1.9.1 Sous-TLV 38.1 – Adresse IP du récepteur de transferts

Adresse IPv4 du récepteur de transferts, en binaire.

Type	Longueur	Valeur
38.1	4	Adresse IP

7.4.4.1.9.2 Sous-TLV 38.2 – Numéro de point d'accès UDP du récepteur de transferts

Numéro de point d'accès UDP du récepteur de transferts, en binaire.

Type	Longueur	Valeur
38.2	2	Point d'accès UDP

Si ce sous-TLV n'est pas présent dans un fichier de configuration, la valeur par défaut 162 est utilisée.

7.4.4.1.9.3 Sous-TLV 38.3 – Type de transfert émis par le dispositif PS (voir Note 2 ci-dessous)

Type de transfert.

Type	Longueur	Valeur
38.3	2	Type de transfert

Le dispositif PS DOIT prendre en charge les valeurs suivantes de type de transfert:

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

7.4.4.1.9.4 Sous-TLV 38.4 – Temporisation

Temporisation, en millisecondes, utilisée pour envoyer les messages INFORM du protocole SNMP.

Type	Longueur	Valeur
38.4	2	0 – 65535

7.4.4.1.9.5 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 – 65535

7.4.4.1.9.6 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.

7.4.4.1.9.7 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 transferts de type = 1, 2, ou 3. Le dispositif PS DOIT ignorer le sous-TLV 38.7 si le type de transfert contenu dans le sous-TLV 38.3 est 1, 2, ou 3. Si le

sous-TLV 38.7 n'est pas fourni avec un transfert 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 transfert 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.

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 transfert recherchée: snmpNotifyTable, snmpTargetAddrTable, snmpTargetParamsTable, snmpNotifyFilterProfileTable, snmpNotifyFilterTable, snmpCommunityTable, usmUserTable, vacmSecurityToGroupTable, vacmAccessTable et vacmViewTreeFamilyTable

NOTE 2 – Type de transfert: la chaîne communautaire pour les transferts automatiques 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 transferts. 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 transfert. Tous les messages TRAP ayant un OID de transfert contenu dans ce sous-arbre de filtre de transfert DOIVENT être envoyés au récepteur de transferts.

NOTE 4 – Le fichier de configuration du 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".

NOTE 5 – Le dispositif PS ne DOIT traiter le TLV-38 que s'il est entré dans le mode de coexistence SNMPv3 pendant le traitement du fichier de configuration du PS.

7.4.4.1.10 Informations propres au vendeur

Si des informations propres au vendeur sont fournies aux services portail, elles DOIVENT être codées dans le champ d'informations propres au vendeur (VSIF) (code 43) au moyen du champ d'identificateur de vendeur afin de spécifier quels nuplets TLV s'appliquent à quels produits de vendeur. L'identificateur de vendeur DOIT être le premier sous-TLV intégré à l'intérieur du champ VSIF. Si le premier TLV à l'intérieur du champ VSIF n'est pas un identificateur de vendeur, le fichier de configuration du PS DOIT être ignoré.

Ce réglage de configuration est autorisé à apparaître plusieurs fois dans un fichier de configuration et le même identificateur de vendeur est autorisé à apparaître plusieurs fois. Le dispositif PS DOIT ignorer le fichier de configuration si plus d'un seul sous-TLV d'identificateur de vendeur est présent dans un même champ VSIF.

Des sous-types propres au vendeur sont autorisés à être ajoutés 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

7.4.4.1.11 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 [FIPS 180-1]. Ce nuplet TLV n'est utilisé que dans le fichier de configuration, immédiatement avant le marqueur de fin de données.

7.4.4.1.12 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 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 PS dépend du mode d'approvisionnement 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 PS. La méthode de déclenchement du téléchargement du fichier de configuration du pare-feu ne dépend pas du mode d'approvisionnement.

7.4.4.2.1 Déclenchement du téléchargement du fichier de configuration du PS dans le mode d'approvisionnement 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 PS dans le champ 'file' du message DHCP ACK, le dispositif PS DOIT combiner l'adresse du serveur et le nom du fichier de configuration du 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 PS:

tftp://adresse_IPv4_du_serveur_TFTP/chemin_complet_du_fichier_de
configuration_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 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 PS, par un dispositif PS fonctionnant en mode d'approvisionnement DHCP, est déclenché par la présence de l'emplacement du fichier de configuration du PS (adresse IP du serveur TFTP ou HTTPS) et par la présence de son nom dans le message DHCP envoyé aux services 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 d'approvisionnement 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, alors le dispositif PS DOIT envoyer une demande de 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 d'approvisionnement 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 demande de 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 d'approvisionnement 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 demande de 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 d'approvisionnement DHCP, d'un fichier de configuration. Un dispositif PS fonctionnant en mode d'approvisionnement DHCP DOIT traiter l'objet cabhPsDevProvConfigFile comme étant en lecture seule.

7.4.4.2.2 Déclenchement du téléchargement du fichier de configuration du PS dans le mode d'approvisionnement SNMP

Si le dispositif PS doit fonctionner en mode d'approvisionnement SNMP (ce qui est indiqué par la valeur de l'objet cabhPsDevProvMode), le téléchargement du fichier de configuration du 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 d'approvisionnement SNMP (ce qui est indiqué par la valeur de l'objet cabhPsdevProvMode), l'élément de services PS NE DOIT PAS lancer un téléchargement du fichier de configuration du PS si l'objet de base MIB cabhPsDevTodSyncStatus a une valeur égale à '2' (échec d'accès au serveur ToD).

Une fois que le dispositif PS, fonctionnant en mode d'approvisionnement SNMP (ce qui est indiqué par la valeur de l'objet cabhPsDevProvMode), envoie une demande TFTP afin de télécharger un fichier de configuration du 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 PS demandé, il DOIT traiter ce fichier avant d'envoyer une demande TFTP afin de recevoir un autre fichier de configuration du 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 demande SET (mise à jour) du protocole SNMP pour l'objet cabhPsDevProvConfigFile, si les conditions suivantes sont vraies:

- le dispositif PS doit fonctionner en mode d'approvisionnement 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 d'approvisionnement SNMP reçoit une demande 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 demande 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 cabhSecFwPolicyFileURL MIB, soit par le fichier de configuration du PS ou par une demande SET (mise à jour) du protocole SNMP, est différente de la valeur de l'objet de base MIB cabhSecFwPolicySuccessfulFileURL. Si la valeur servant à mettre à jour (SET) l'objet de base MIB cabhSecFwPolicyFileURL, soit par le fichier de configuration du PS ou par une demande SET (mise à jour) du protocole SNMP, est la même que celle de l'objet de base MIB cabhSecFwPolicySuccessfulFileURL, le téléchargement du fichier de configuration du pare-feu NE DOIT PAS être déclenché.

7.4.4.2.4 Fonctionnement après déclenchement

Une fois déclenché, le dispositif PS DOIT utiliser un client TFTP selon RFC 1350 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 de gestion 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 demande 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 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 PS 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 d'approvisionnement 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 PS ou du pare-feu a la valeur n = [0, 1, 2, 3, 4, ou 5];
- n = 0 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 PS demandé après la tentative avec n = 5, n doit être réinitialisé à 0 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 0 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 d'approvisionnement 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 demande 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-28 du fichier de configuration en une seule unité PDU du protocole SNMP contenant (n) composants d'identificateur OID de base MIB ou d'instance et valeur (éléments 'VarBind' du protocole SNMP). Conformément au document RFC 3416, l'unique unité PDU du protocole SNMP produite par un fichier de configuration 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 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 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 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 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 portail selon leur propre champ de valeurs mais qui n'y réussissent pas) à partir d'un fichier de configuration du 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 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 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 d'approvisionnement SNMP

L'algorithme servant à authentifier le fichier de configuration dépend du mode d'approvisionnement dans lequel le dispositif PS doit fonctionner (voir § 5.5, "Modes de fonctionnement IPCable2Home"). Le dispositif PS prend en charge deux modes d'approvisionnement: le mode d'approvisionnement DHCP et le mode d'approvisionnement SNMP. Deux méthodes d'authentification du fichier de configuration sont prises en charge dans le mode d'approvisionnement 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 d'approvisionnement de l'élément de services PS, lequel DOIT prendre en charge les deux algorithmes de sécurité spécifiés dans les § 7.4.4.3.1, "Vérification du fichier de configuration du PS en mode d'approvisionnement DHCP" et 7.4.4.3.2, "Algorithme d'authentification du fichier de configuration du PS en mode d'approvisionnement SNMP".

7.4.4.3.1 Vérification du fichier de configuration du PS en mode d'approvisionnement DHCP

Lorsqu'il fonctionne en mode d'approvisionnement 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 d'approvisionnement 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 d'approvisionnement crée un nouveau fichier de configuration du 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 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 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 PS est alors mis à la disposition du serveur TFTP approprié;
3) l'élément de services PS télécharge le fichier de configuration du 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;
5) l'élément de services PS DOIT calculer un hachage SHA-1 sur le contenu du fichier de configuration du PS à l'exception du hachage de TLV (servant à configurer l'objet

[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.

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 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 PS en mode d'approvisionnement SNMP

La procédure de vérification du hachage du fichier de configuration du PS par l'élément de services PS en mode d'approvisionnement SNMP est reproduite ci-dessous:

1) quand le générateur de fichiers de configuration du système d'approvisionnement crée un nouveau fichier de configuration du 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 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 PS par demande 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 PS par demande 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 PS télécharge le fichier nommé à partir du serveur TFTP configuré. Si le fichier de configuration du PS contient un nuplet TLV de type 53, le dispositif PS DOIT l'ignorer;
5) l'élément de services PS DOIT calculer un hachage SHA-1 sur le contenu du fichier de configuration du 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 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 d'approvisionnement SNMP ou en mode d'approvisionnement DHCP sans l'utilisation du protocole HTTPS/TLS comme défini dans le § 11.9, "Sécurité du fichier de configuration du PS en mode d'approvisionnement 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 d'approvisionnement envoie la valeur de hachage calculée au cours de l'étape 1 à l'élément de services PS 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 PS;
   b) en envoyant une demande SET (mise à jour) du protocole SNMP afin de mettre à jour l'objet cabhSec2FwPolicyHash de base MIB;

3) le système d'approvisionnement 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 PS;

   b) en envoyant une demande 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 PS 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 7-14 identifie les modes de succès et d'échec qui pourraient être rencontrés lors du téléchargement et du traitement du fichier de configuration du PS, ainsi que l'action que le dispositif PS DOIT entreprendre quand il détecte ces modes.

Tableau 7-14/J.192 – Traitement du fichier de configuration: modes de succès et d'échec

Mode d'échec	Action
TFTP échoué – Demande GET envoyée, aucune réponse reçue	Signaler un événement (identificateur d'événement 68000500) et réessayer le transfert TFTP.
TFTP échoué – Fichier de configuration non trouvé	Signaler un événement (identificateur d'événement 68000600) et réessayer le transfert TFTP.
TFTP échoué – Paquets dans le désordre	Signaler un événement (identificateur d'événement 68000700) et réessayer le transfert TFTP.
Téléchargement TFTP échoué – Nombre maximal de réessais dépassé	Signaler un événement (identificateur d'événement 68000900) et réinitialiser.
Téléchargement TFTP réussi	Signaler un événement (identificateur d'événement 68001000 si TLS n'a pas été utilisé ou ID d'événement 68003200 si TLS a été utilisé) 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.

Tableau 7-14/J.192 – Traitement du fichier de configuration: modes de succès et d'échec

Mode d'échec	Action
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-28	Signaler un événement (identificateur d'événement 73040102), ignorer 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.
Type reconnu mais mauvaise valeur MIB, ou OID de TLV-28 valide mais mauvaise valeur MIB	Signaler un événement (identificateur d'événement 73040102), ignorer 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.
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 7-14, 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 PS est inférieur à 5 et si la demande GET du protocole TFTP ou HTTPS arrive à expiration, ou si le fichier de configuration du PS n'est pas trouvé sur le serveur (distant), ou si la demande 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 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 demande 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 demande 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 PS est égal à 5 et si le dispositif PS n'a pas correctement téléchargé le fichier de configuration du PS, le dispositif PS DOIT signaler l'événement indiqué dans le Tableau 7-14, "Traitement du fichier de configuration: modes de succès

et d'échec", afin d'indiquer l'échec du processus de téléchargement du fichier de configuration du PS et libérer son adresse IP d'interface PS/WAN-Man conformément au document 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 PS, le dispositif PS DOIT signaler l'événement indiqué dans le Tableau 7-14, "Traitement du fichier de configuration: modes de succès et d'échec", 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 PS

Un téléchargement réussi du fichier de configuration du PS est défini comme une réception complète et correcte par l'élément de services PS du contenu du fichier de configuration du 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 PS sans erreurs provenant de cette autorité calcul.

Si le dispositif PS télécharge correctement le fichier de configuration du PS, le dispositif PS DOIT remettre à zéro le compteur de réessais du fichier de configuration du PS et signaler l'événement indiqué par "Téléchargement TFTP réussi" dans la colonne 'Mode d'échec' du Tableau 7-14, "Traitement du fichier de configuration: modes de succès et d'échec".

7.4.4.4.4 Echec du téléchargement du fichier de configuration du PS

En cas d'échec de la vérification du fichier de configuration du PS comme spécifié dans le § 7.4.4.3, "Exigences relatives à la vérification du fichier de configuration et à l'authentification du mode d'approvisionnement SNMP", ou dans le § 11.9, "Sécurité du fichier de configuration du PS en mode d'approvisionnement DHCP", le dispositif PS DOIT arrêter le processus d'approvisionnement, ignorer le fichier de configuration du 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 PS ne contient aucun TLV marqueur de fin de données (TLV-255), aucun TLV de vérification MIC du PS (TLV-53), ou est trop volumineux pour être traité, le dispositif PS DOIT arrêter le processus d'approvisionnement, ignorer le fichier de configuration du 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 PS contient des éléments en double 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 d'approvisionnement, ignorer le fichier de configuration du 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 PS contient un champ de type reconnu mais un mauvais champ de valeur ou un identificateur OID de TLV-28 valide mais une mauvaise valeur de base MIB, le dispositif PS DOIT arrêter le processus d'approvisionnement, ignorer le fichier de configuration du 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 PS 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 et continuer le traitement du fichier de configuration du PS.

7.4.4.4.5 Téléchargement réussi du fichier 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 PS 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 d'approvisionnement 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 68003200 (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, le pare-feu 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 d'approvisionnement 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-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-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 portail – Client d'heure actuelle

7.5.1 Fonction de client d'heure actuelle: objectifs

L'objectif des fonctions de client d'heure actuelle du dispositif PS est d'acquérir l'heure actuelle à partir du serveur temporel dans le réseau du câblo-opérateur.

7.5.2 Fonction de client d'heure actuelle: directives de conception du système

Les directives identifiées dans le Tableau 7-15 ont guidé la spécification des capacités définies pour la fonction de client d'heure actuelle des services portail:

Tableau 7-15/J.192 – Client d'heure actuelle: directives de conception du système

Numéro	Directives
ToD 1	Offrir un mécanisme permettant au dispositif PS d'implémenter la synchronisation horaire avec la tête de réseau.

7.5.3 Fonction de client d'heure actuelle: description du système

L'élément de services PS utilise un client d'heure actuelle conforme au document [RFC 868], afin de réaliser la synchronisation horaire avec un serveur temporel situé en tête de réseau. La synchronisation horaire est essentielle pour les fonctions de sécurité des services 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 de la tête de réseau – pour le réseau WAN-Man, ce client du protocole DHCP va recevoir l'adresse IP du serveur temporel ToD de tête de réseau dans l'option 4 du protocole DHCP. Le client du protocole DHCP va également recevoir le décalage temporel (par rapport au temps UTC), dans l'option 2 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, elle devrait envoyer une interrogation temporelle [RFC 868] au serveur ToD. Si celui-ci renvoie une réponse valide, le dispositif PS commencera à utiliser cette heure actuelle pour les marqueurs temporels des messages événementiels et pour les fonctions de sécurité.

7.5.4 Fonction de client d'heure actuelle: exigences

L'élément de services PS DOIT implémenter un client d'heure actuelle.

Le client d'heure actuelle des services portail DOIT être conforme au protocole horaire [RFC 868] et ne doit utiliser que le protocole UDP.

Lors d'une réinitialisation, l'élément de services PS DOIT initialiser sa date à 00:00.0 (minuit) GMT du 1er janvier 1970.

L'élément de services PS DOIT essayer de synchroniser son heure actuelle avec les serveurs temporels offerts dans l'option 4 du protocole DHCP du message DHCP ACK, reçu par le réseau WAN-Man pendant l'acquisition de location DHCP d'adresse WAN-Man.

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.

Le dispositif PS DOIT combiner l'heure récupérée à partir du serveur temporel avec le décalage temporel offert par l'option 2 du protocole DHCP, afin de créer l'heure locale actuelle.

L'élément de services PS DOIT utiliser l'heure locale actuelle calculée à partir de l'heure récupérée à partir du serveur temporel ToD et du décalage temporel reçu par l'option 2 du protocole DHCP pour toutes fonctions qui nécessitent l'heure actuelle et qui ne doivent être exactes qu'à la seconde près.

La priorité pour l'horloge du système en temps réel pour un dispositif PS intégré est la suivante:

- première priorité: heure actuelle acquise à partir du serveur ToD;
- deuxième priorité: heure actuelle acquise à partir du câblo-modem;
- troisième priorité: heure initialisée au 1er janvier 1970.

Un dispositif PS intégré DOIT utiliser la plus récente heure valide qui a été acquise à partir du serveur temporel ToD pour l'horloge du système en temps réel, même si cela implique la surécriture du temps système acquis par le CM.

Si un dispositif PS intégré n'est pas en mesure d'acquérir l'heure actuelle à partir du serveur ToD, il DOIT utiliser l'heure actuelle acquise par le câblo-modem pour l'horloge du système en temps réel.

Si un dispositif PS intégré n'est pas en mesure d'acquérir l'heure actuelle à partir du serveur temporel ToD et n'est pas en mesure d'acquérir une heure valide à partir du câblo-modem, il DOIT utiliser l'heure initialisée par le processus d'amorçage au 1er janvier 1970 pour l'horloge du système en temps réel.

La priorité de l'horloge du système en temps réel pour un dispositif PS autonome est la suivante:

- première priorité: heure actuelle acquise à partir du serveur ToD;
- deuxième priorité: heure initialisée au 1er janvier 1970.

Un dispositif PS autonome DOIT utiliser la plus récente heure valide acquise à partir du serveur temporel ToD pour l'horloge du système en temps réel.

Si un dispositif PS autonome n'est pas en mesure d'acquérir l'heure actuelle à partir du serveur ToD, il DOIT utiliser l'heure actuelle initialisée par le processus d'amorçage au 1er janvier 1970 pour l'horloge du système en temps réel.

L'élément de services PS DOIT continuer à essayer de communiquer avec le serveur temporel, jusqu'à ce que l'heure locale ait été établie. La temporisation propre aux demandes d'heure dépend de l'implémentation. Cependant, le client d'heure actuelle du dispositif PS NE DOIT PAS dépasser 3 demandes d'heure par période de 5 min. Au minimum, le client d'heure actuelle du dispositif PS DOIT envoyer au moins 1 demande d'heure par période de 5 min, jusqu'à ce que l'heure locale soit établie.

Si le serveur temporel ToD ne renvoie pas de réponse valide, le dispositif PS DOIT effectuer ce qui suit, non nécessairement dans l'ordre énuméré:

- mettre la valeur de l'objet cabhPsDevTodSyncStatus à '2' (échec d'accès au serveur ToD);
- s'il y a des connexions louées actives dans le secteur LAN-Trans comme indiqué par une valeur différente de zéro pour l'objet cabhCdpLanTransCurCount, régler l'objet cabhCdpLanAddrCreateTime à l'heure actuelle et régler l'objet cabhCdpLanAddrExpireTime à la valeur de l'objet cabhCdpLanAddrCreateTime plus la valeur de l'objet cabhCdpServerLeaseTime pour chaque location active (heure d'expiration = heure de création + durée de location);
- enregistrer l'échec et produire un événement normalisé comme défini dans l'Annexe B;
- continuer de réessayer les communications avec le serveur temporel ToD jusqu'à ce que l'heure locale soit établie;
- si cette opération a été déclenchée, essayer de télécharger le fichier de configuration du PS comme décrit dans le § 7.4.4.2.4, "Fonctionnement après déclenchement".

Si le serveur temporel ToD renvoie effectivement une réponse valide, le dispositif PS DOIT effectuer ce qui suit, non nécessairement dans l'ordre énuméré:

- mettre la valeur de l'objet cabhPsDevTodSyncStatus à '1' (accès au serveur ToD réussi);
- s'il y a des connexions louées actives dans le secteur LAN-Trans comme indiqué par une valeur différente de zéro pour l'objet cabhCdpLanTransCurCount, régler l'objet cabhCdpLanAddrCreateTime à l'heure actuelle et régler l'objet cabhCdpLanAddrExpireTime à la valeur de l'objet cabhCdpLanAddrCreateTime plus la valeur de l'objet cabhCdpServerLeaseTime pour chaque location active (heure d'expiration = heure de création + durée de location);
- si cette opération a été déclenchée, essayer de télécharger le fichier de configuration du PS comme décrit dans le § 7.4.4.2.4, "Fonctionnement après déclenchement".

Si la valeur de l'objet cabhPsDevTodSyncStatus est '1', c'est-à-dire si l'heure locale a déjà été établie, il n'est pas nécessaire que le client d'heure actuelle envoie une demande d'heure.

Le dispositif PS NE DOIT envoyer et recevoir de messages ToD que par une interface avec un réseau WAN-Man.

7.6 Fonction de point extrême – Client du protocole DHCP

7.6.1 Fonction de point extrême de client du protocole DHCP: objectifs

L'objectif des fonctions 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 7-16 ont guidé la spécification des fonctions de point extrême de client du protocole DHCP.

Tableau 7-16/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 le document 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 7-17.

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";
- Option DHCP de code 255: fin.

Tableau 7-17/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 à la construction
0	Bourrage	–	N/A
255	Fin	M	N/A
1	Masque de sous-réseau	M	N/A
2	Décalage temporel	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
43	Informations propres au vendeur	M	Choisies par le vendeur
50	Adresse IP demandée	M	Valeur néant ou choisie par le vendeur
51	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 LAN de telle sorte qu'ils résident dans le même sous-réseau logique.

8.1.2 Hypothèses

- On suppose que, quand des serveurs d'approvisionnement 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 portail – Portail d'adressage IPCable2Home (CAP)

Le portail d'adressage IPCable2Home (CAP) est un sous-élément logique de l'élément logique de services portail. Ses fonctions consistent à acheminer le trafic entre le réseau LAN et le réseau WAN, à acheminer le trafic de réseau LAN à réseau LAN, et à exécuter des fonctions de conversion d'adresse et de point d'accès.

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 LAN et entre dispositifs IP de réseau LAN et passerelle par défaut des services portail sur le réseau WAN;
- offrir une capacité de conversion d'adresse de réseau et de point d'accès (NAPT) pour mappage entre une unique adresse IP mondiale à l'interface PS/WAN et une ou plusieurs adresses IP privées dans le réseau LAN;
- 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 LAN;
- maintenir dans le réseau LAN le trafic entre dispositifs IP de réseau LAN et ne pas permettre qu'il traverse le réseau WAN.

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 de conception du système de portail CAP
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).

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 traversée 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 traversée 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 point d'accès 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 points d'accès TCP/UDP (protocole de commande de transmission/protocole de datagramme d'utilisateur) sont converties en une seule adresse de couche Réseau avec ses points d'accès 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 traversée IPCable2Home est un processus de dérivation 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 LAN et qui est destiné à des secteurs d'adresses IP de réseau LAN. 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.

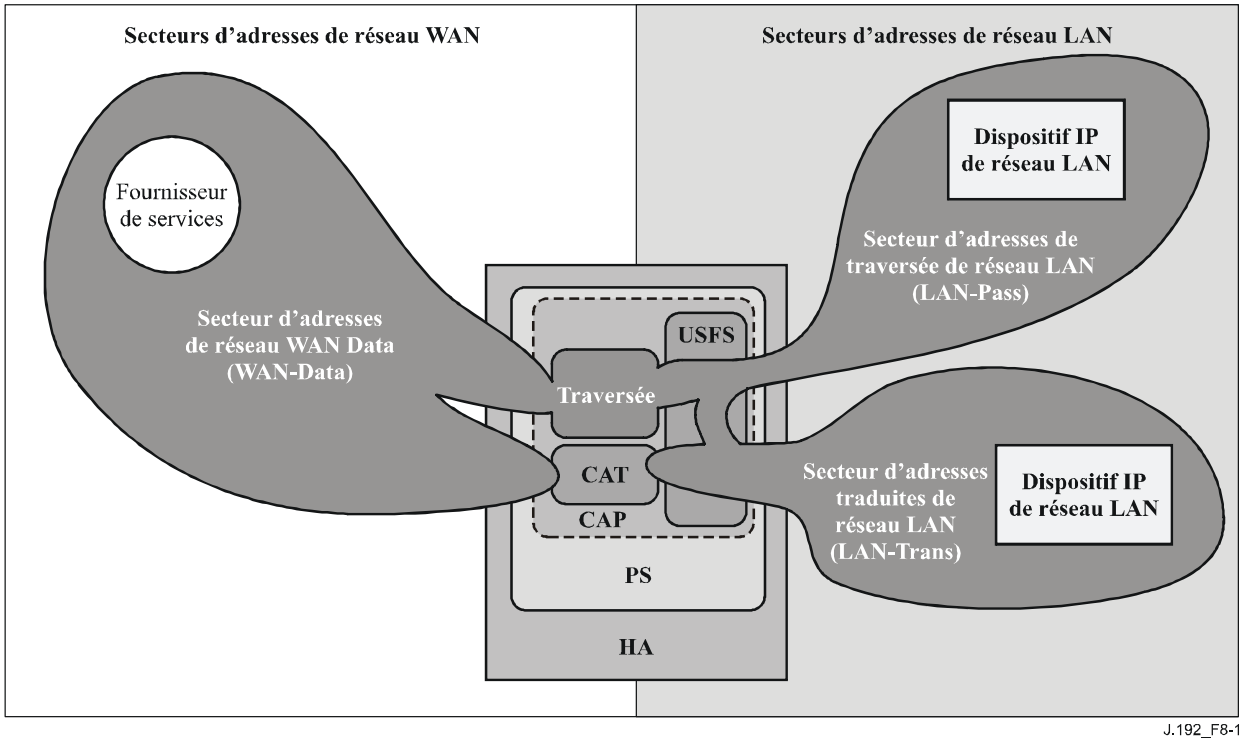


Figure 8-1/J.192 – Fonctions du portail d'adressage IPCable2Home (CAP)

Dans l'ensemble de la présente Recommandation, les termes *liaison d'adresse, non-liaison 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 point d'accès TCP/UDP, adresse IP de réseau LAN-Trans et point d'accès 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 numéro séquentiel ICMP est utilisé à la place du numéro de point d'accès TCP/UDP.

Le trafic de réseau LAN à réseau WAN est défini comme étant formé de paquets issus de dispositifs IP de réseau LAN et destinés à des dispositifs situés du côté PS/WAN. Le trafic de réseau WAN à réseau LAN est défini comme étant formé de paquets issus de serveurs WAN destinés à des dispositifs IP de réseau LAN. Le trafic de réseau LAN à réseau LAN est défini comme étant formé de paquets issus de dispositifs IP de réseau LAN et destinés à des dispositifs IP de réseau LAN 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 PS 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 LAN à réseau WAN et du trafic de réseau WAN à réseau LAN: le mode de traversée, 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 traversée, le portail CAP agit comme un pont transparent [ISO/CEI 10038] Contrôle d'accès au support (MAC) – Ponts entre le secteur WAN-Data et le secteur LAN-Pass. En mode de traversée, 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 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 PS (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 WAN 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 LAN à réseau WAN 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 points d'accès aux réseaux WAN et LAN, la méthode de mappage et le protocole de transport servant au mappage. Le numéro de point d'accès ne sera pas converti par le portail CAP pour les mappages C-NAT: les numéros des points d'accès 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 point d'accès aux réseaux WAN et LAN. Le portail CAP doit également introduire la valeur 0 dans les entrées relatives aux numéros de point d'accès aux réseaux WAN et LAN de la table de mappage du portail CAP, pour les entrées approvisionnées de réexpédition par point d'accès 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 point d'accès statique approvisionnée 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 point d'accès de valeur 0 aura deux fonctions:

1) indiquer au portail CAP que les numéros de point d'accès ne doivent pas être convertis, c'est-à-dire que les points d'accès sont "remplacés par une structure générique";
2) indiquer à tout lecteur de la table de mappage du portail CAP que ce mappage de point d'accès statique est effectivement un mappage C-NAT, ce qui permet d'établir une distinction entre entrées de réexpédition par point d'accès statique (mappages C-NAT avec numéro de point d'accès 0) et mappages C-NAPT (avec numéro de point d'accès différent de zéro).

Voir le paragraphe 8.3.3.2, "Structures génériques de réexpédition par point d'accès statique", pour de plus amples informations sur l'opération de réexpédition par point d'accès 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 à la construction pour le système) l'élément de services PS (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 LAN à réseau WAN 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 WAN et le dispositif IP de réseau LAN a déjà obtenu une adresse IP dans le secteur LAN-Trans.

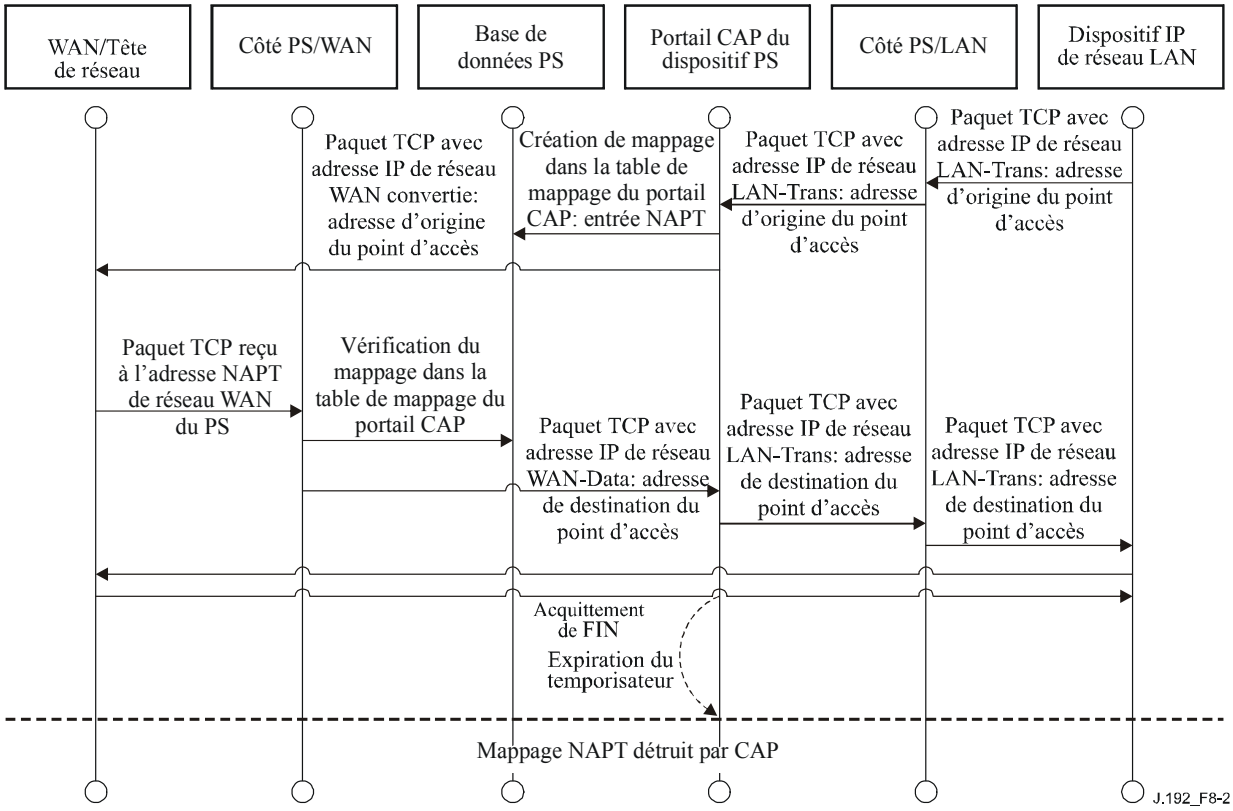


Figure 8-2/J.192 – Configuration des services portail (table de mappage CAP-NAPT) – Diagramme séquentiel

Il est également possible que le dispositif PS fonctionne en mode mixte de dérivation/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 traversée (objet cabhCapPassthroughTable), une ou plusieurs adresses MAC appartenant à des dispositifs IP de réseau LAN 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 LAN à réseau WAN, 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 WAN à réseau LAN, 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 LAN. 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 traversée, le trafic diffusé sera dérivé vers toutes les interfaces.

Quand le dispositif PS est en mode mixte de dérivation/acheminement et reçoit le trafic diffusé qui provient d'un dispositif figurant dans la table de traversée, ce dispositif PS est censé dériver le trafic diffusé vers toutes les interfaces. Quand le dispositif PS est en mode mixte de dérivation/acheminement et reçoit le trafic diffusé par une interface quelconque avec un

réseau WAN, le dispositif PS est censé dériver le trafic diffusé vers toutes les interfaces avec un réseau LAN.

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 LAN vers le réseau WAN.

8.3.3.2 Structures génériques de réexpédition par point d'accès statique

Quand le dispositif PS est approvisionné de façon à fonctionner en mode primaire de traitement de paquet C-NAPT et qu'une liaison de conversion C-NAPT est statiquement créée avec le numéro de point d'accès réglé à zéro, alors le portail CAP doit traiter le trafic entrant de manière particulière. Le portail CAP va réexpédier tout le trafic entrant, non associé à une session de conversion C-NAPT existante ou à une liaison statique de conversion C-NAPT existante, à l'adresse IP de réseau LAN spécifiée dans ce type spécial de liaison de conversion C-NAPT.

Le portail CAP va traiter les paquets comme suit:

1) vérifier tous les paquets entrants afin de savoir s'ils sont associés à une session existante, spécifiée par une liaison dynamique de conversion C-NAPT. Si tel est le cas, alors le paquet est converti comme spécifié puis réexpédié;
2) sinon, le portail CAP vérifie s'il y a une liaison statique de conversion C-NAPT associée au paquet. Si tel est le cas, alors le paquet est converti comme spécifié puis réexpédié;
3) sinon, le portail CAP vérifie s'il y a une liaison statique de conversion C-NAPT pour cette adresse IP de réseau WAN avec le numéro de point d'accès réglé à 0. Si tel est le cas, alors le portail CAP convertit l'adresse IP en l'adresse IP de réseau LAN spécifiée dans cette liaison statique spéciale de conversion C-NAPT. Noter que la fonction C-NAPT ne convertit pas le point d'accès 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.

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 d'implémenter une fonction de *Traversée de 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 LAN 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 LAN fait appel à IPsec en tant que protocole de VPN;
- le dispositif IP de réseau LAN fait appel à l'échange de clés IP (IKE) afin d'échanger dynamiquement les clés de chiffrement avec le serveur de 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 LAN dont l'adresse de commande MAC est dans la table de traversée 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 points d'accès appropriés au trafic entrant (de réseau WAN à réseau LAN), plus précisément le point d'accès 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 point d'accès 500 comme point d'accès 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 point d'accès servant au trafic entrant et sortant, par le point d'accès 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 point d'accès 500, le trafic entrant au point d'accès 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 points d'accès utilisés par l'adresse IP de réseau WAN-Data pour le trafic et l'échange de clés et les convertir en points d'accès 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 LAN 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 LAN connectés au même élément de services PS. Il est important d'empêcher le trafic entre ces dispositifs IP de réseau LAN 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 LAN dont l'adresse IP de destination est hors du secteur d'adresses du réseau LAN est transmise sans changement à la fonctionnalité de dérivation/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 PS. 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 LAN à réseau WAN. 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 LAN de destination et le trafic est – par la fonctionnalité de réexpédition et accès au support

de la qualité de service (QFM) (voir § 10.3, "Elément logique des services portail CQP") 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 dérivation de traversée (selon le mode de traitement de paquet activé).

8.3.3.5 Multidiffusion

Le portail CAP prend en charge le trafic multidiffusé de réseau WAN à réseau LAN par dérivation transparente en aval des paquets de messagerie IGMP [RFC 2236] et des paquets IP multidiffusés en aval [ID-IGMP]. 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 LAN résidant dans le domaine du réseau LAN-Trans. Le portail CAP réexpédie le trafic IGMP provenant du réseau WAN vers le réseau LAN afin de permettre aux notifications d'atteindre les dispositifs IP de réseau LAN. Un dispositif IP de réseau LAN 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 LAN. Quand le service de multidiffusion n'est plus désiré, le dispositif IP de réseau LAN 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.

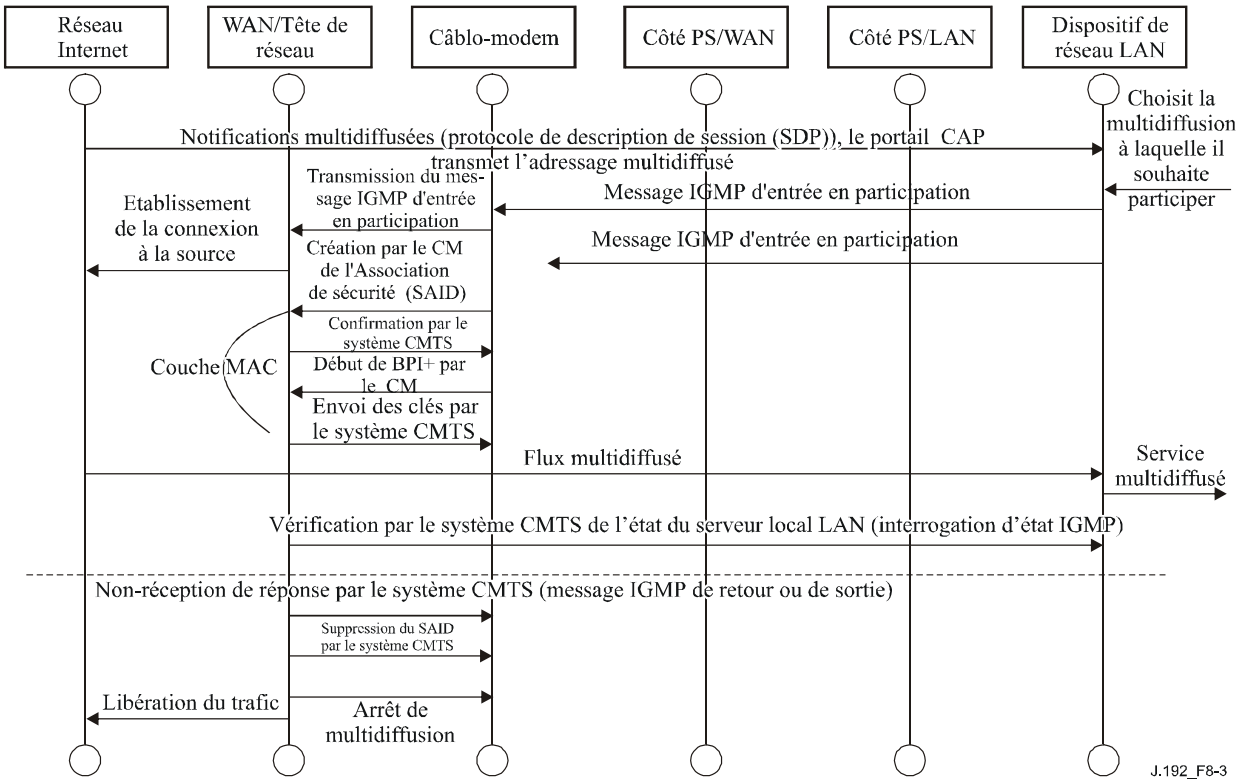


Figure 8-3/J.192 – Séquence de multidiffusion par protocole IGMP

8.3.3.6 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 LAN à réseau WAN et la Figure 8-5 montre un exemple d'étapes possibles de traitement de paquet pour le trafic unidiffusé de réseau WAN à réseau LAN.

NOTE – Ces exemples ne sont qu'informatifs et n'impliquent aucune obligation quant à leur implémentation.

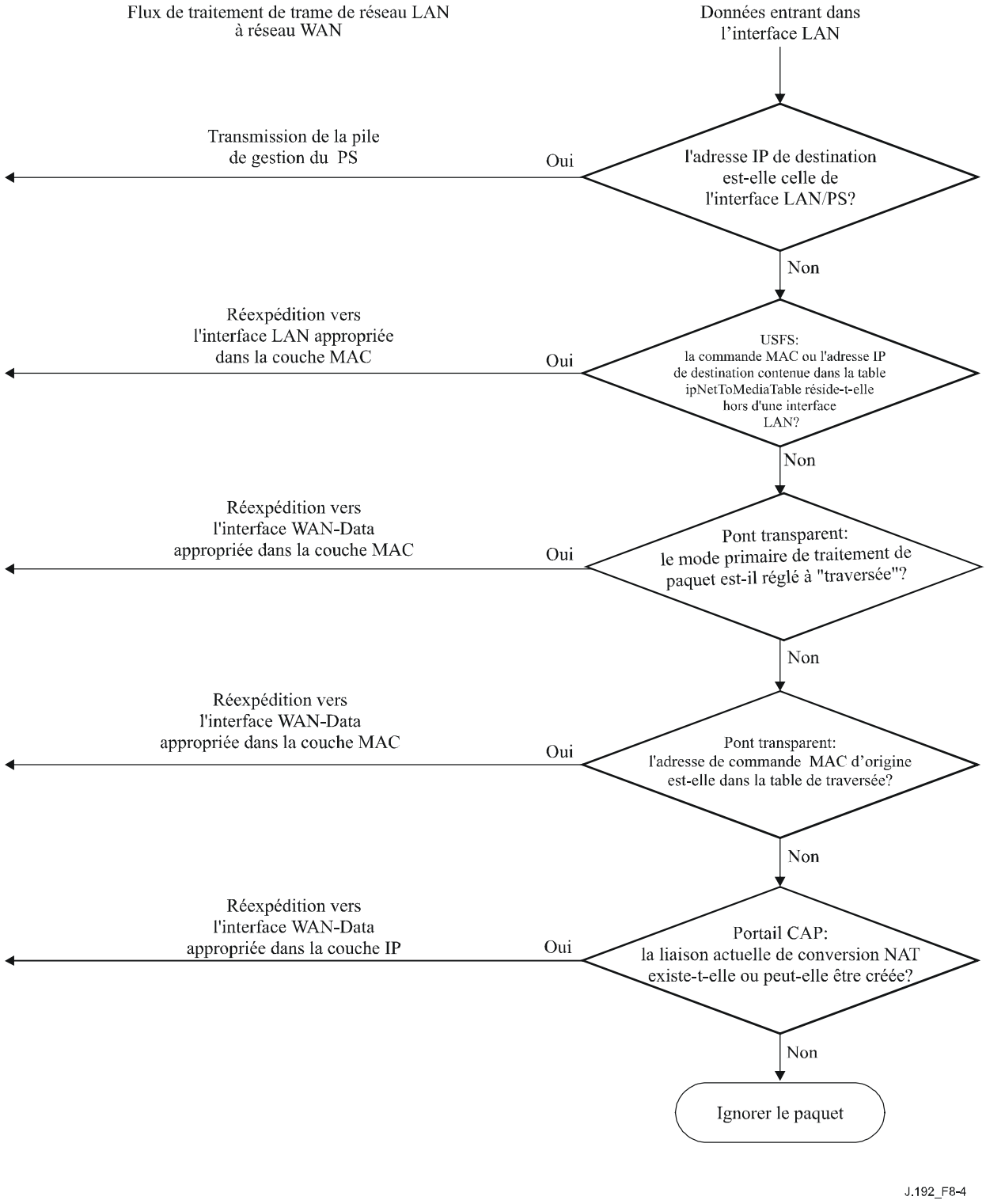


Figure 8-4/J.192 – Exemple de traitement de paquet de réseau LAN à réseau WAN

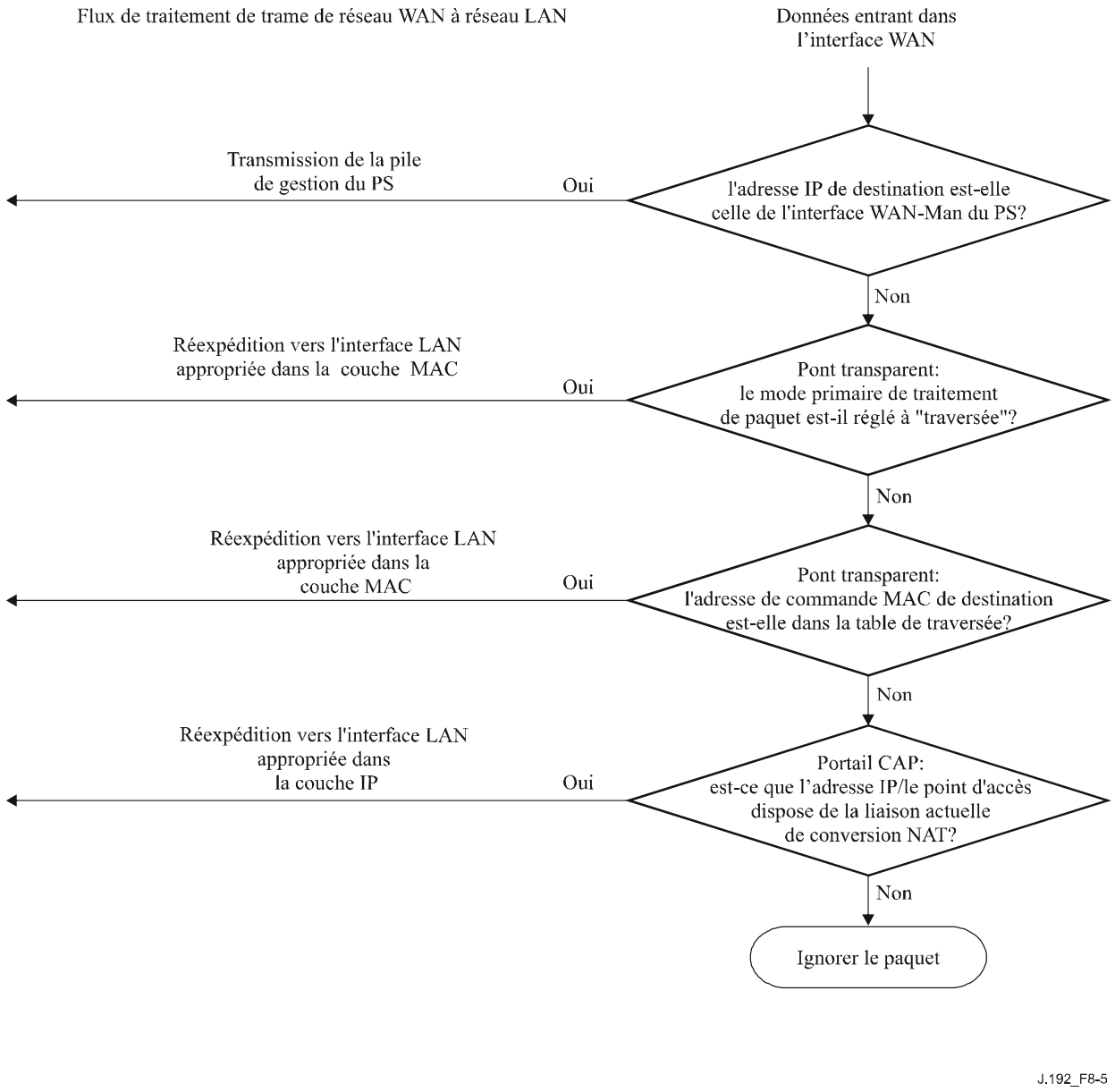


Figure 8-5/J.192 – Exemple de traitement de paquet de réseau WAN à réseau LAN

8.3.4 Exigences relatives au portail CAP

8.3.4.1 Exigences générales

Toutes les interfaces IP logiques avec l'élément de services PS 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 WAN à réseau LAN par dérivation transparente des paquets IP de messagerie IGMP de réseau WAN à réseau LAN et des paquets IP de multidiffusion de réseau WAN à réseau LAN comme défini dans le document [RFC 2236].

Si le mode primaire de traitement de paquet, objet cabhCapPrimaryMode, est réglé à "traversée", toute la messagerie IGMP de réseau LAN à réseau WAN 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 LAN à réseau WAN provenant de dispositifs IP de réseau LAN 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 WAN.

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 LAN à réseau WAN provenant de dispositifs IP de réseau LAN 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 WAN.

8.3.4.2 Exigences relatives au traitement des paquets

Le dispositif PS DOIT prendre en charge le mode de traversée, 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 point d'accès 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 point d'accès 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 point d'accès d'un paquet dont l'adresse IP figure dans la table de mappage du portail CAP avec un numéro de point d'accès 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 WAN en cours (avec une location DHCP en cours venant de l'approvisionnement 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 WAN en cours ou du fait qu'il manque des numéros de point d'accès, ce portail DOIT produire un événement normalisé (comme défini dans l'Annexe B).

Le trafic unidiffusé de réseau LAN à réseau LAN NE DOIT jamais être acheminé ou dérivé à la sortie d'une interface avec un réseau WAN.

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 traversée

Quand le mode primaire de traitement de paquet du portail CAP, cabhCapPrimaryMode, est réglé à "traversée", 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. Même quand le mode primaire de traitement de paquet est réglé à "traversée", le

traitement par la fonction USFS DOIT avoir priorité sur les décisions de dérivation de réseau LAN à réseau WAN .

8.3.4.4 Exigences relatives à l'acheminement transparent C-NAT/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 LAN à réseau WAN. 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 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 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 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.

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 point d'accès 500 au trafic entrant (de réseau WAN à réseau LAN) vers l'adresse IP de réseau LAN-Trans associée au dispositif IP de réseau LAN 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 point d'accès.

Si le trafic entrant au point d'accès 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 point d'accès 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 prise en charge de la réexpédition par liaison statique avec un point d'accès

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 point d'accès au réseau WAN réglé à 0, alors le dispositif PS DOIT convertir les adresses IP spécifiées dans la liaison pour les paquets qui ne sont pas associés à une liaison dynamique ou statique de conversion C-NAPT existante.

8.3.4.7 Exigences relatives au mode mixte de dérivation/acheminement

Le dispositif PS DOIT prendre en charge le mode mixte de dérivation/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 LAN, le dispositif PS DOIT dériver en transparence le trafic de réseau LAN à réseau WAN issu de cette adresse de commande MAC, ainsi que le trafic de réseau WAN à réseau LAN destiné à cette adresse MAC.

En mode mixte de dérivation/acheminement, comme décrit dans le § 8.3, la fonction de commutation USFS DOIT être appliquée à tout le trafic reçu d'un réseau LAN.

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 (traversée, C-NAT, C-NAPT, ou mode mixte de dérivation/acheminement).

L'élément de services PS DOIT apprendre toutes les adresses IP de réseau LAN-Trans IP, toutes les adresses IP de réseau LAN-Pass et toutes les adresses MAC de dispositifs IP de réseau LAN qui sont associées à chacune de ses interfaces de réseau physique actives. Les adresses IP et MAC apprises par l'élément de services PS et les numéros d'indice d'interface physique du dispositif PS DOIVENT être accessibles au système NMS (à travers le portail CMP) par la table [RFC 2011] ipNetToMediaTable. L'élément de services PS DOIT supprimer les entrées de la table ipNetToMediaTable quand une temporisation d'inactivité arrive à expiration.

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 LAN 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 LAN de destination et réexpédier la trame vers l'entité de réexpédition/accès au support de la qualité de service (QMA) (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 LAN, selon la priorité des paquets.

La fonction de commutation USFS NE DOIT PAS réexpédier de paquets destinés à un dispositif IP de réseau LAN, à la sortie d'une quelconque interface avec un réseau WAN.

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 LAN, 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 LAN 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 PS est le seul serveur DNS qui fait foi pour les dispositifs IP de réseau LAN situés le secteur LAN-Trans;
- l'élément de services PS ne fournira pas le service DNS aux dispositifs IP de réseau LAN situés dans le secteur LAN-Pass;
- si l'élément de services PS utilise de multiples adresses de réseau WAN-Data, les informations de serveur DNS du réseau WAN 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

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 (DNS) à partir d'un serveur situé dans le dispositif PS aux clients du service DNS situés dans des dispositifs IP de réseau LAN, pour résolution du nom de dispositifs IP de réseau LAN (indépendamment de l'état de la connexion du réseau WAN).
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 LAN, 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 PS.

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 LAN situés dans le secteur d'adresses du réseau LAN-Trans. Le portail CNP n'est pas utilisé par les dispositifs IP de réseau LAN situés dans

le secteur d'adresses du réseau LAN-Pass, parce que ceux-ci seront directement servis par des serveurs DNS extérieurs à la résidence.

En principe, les dispositifs IP de réseau LAN 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 portail CNP dans le secteur LAN-Trans ne dépend pas de l'état de la connexion du réseau WAN. Le portail CNP effectue les tâches suivantes:

- résolution des noms de serveur pour les dispositifs IP de réseau LAN, 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 WAN 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 LAN évite d'avoir à reconfigurer les dispositifs IP de réseau LAN lors d'un changement d'état de la connexion du réseau WAN. Cela permet également de modifier l'attribution de serveur DNS extérieur sans reconfiguration du dispositif IP de réseau LAN.

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 LAN. Il lui appartient également de répondre à ce dispositif IP de réseau LAN par un message de réponse ou d'erreur.

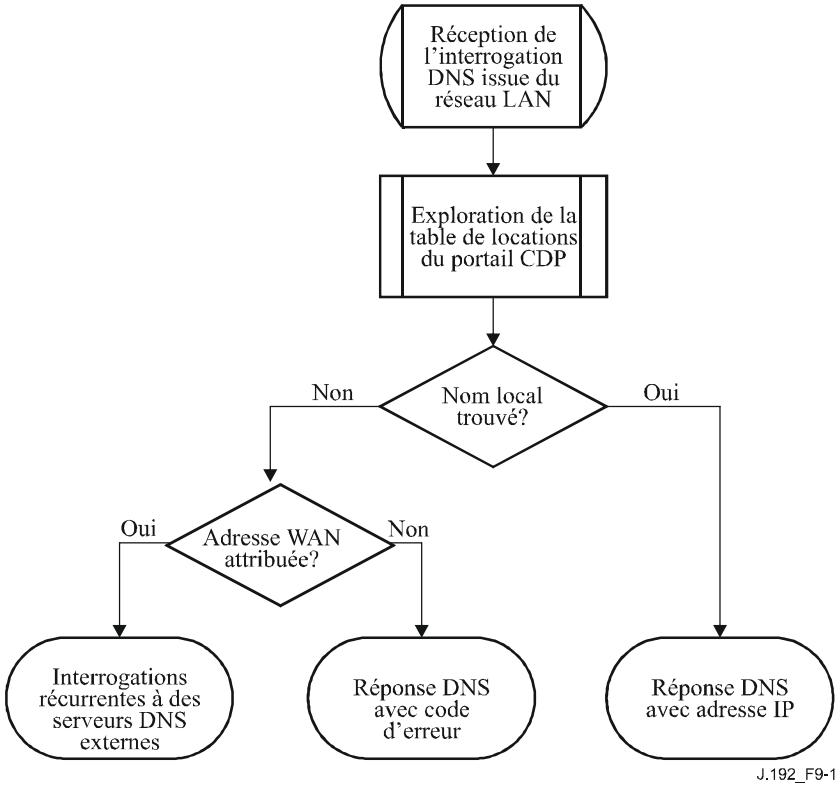


Figure 9-1/J.192 – Traitement de paquet au portail CNP

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 LAN actifs. Aussi longtemps qu'un dispositif IP de réseau LAN 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).

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 du document [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], [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 adressées à l'objet cabhCdpServerDnsAddress.

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 LAN, 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 LAN.

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 LAN 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.

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 le document [RFC 1035].

Le portail CNP DOIT répondre aux interrogations DNS de type QCLASS = IN et du type QTYPE = A, NS, SOA ou PTR.

Les réponses du portail CNP aux interrogations DNS DOIVENT être conforme à la section 3.3 du document [RFC 1035], avec le bit de réponse d'autorisation réglé à '1' dans la section d'en-tête (voir section 4.1.1 du document [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 du document [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 LAN.

10 Qualité de service

10.1 Introduction

Le présent paragraphe décrit l'environnement IPCable2Home afin de permettre aux applications de réseau domestique d'utiliser des ressources de qualité de service (QS). Ces ressources offrent 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.

La présente Recommandation définit les exigences de qualité de service d'élément et de sous-élément PS et BP qui sont nécessaires afin de permettre aux applications d'établir différents niveaux de QS dans le réseau domestique et de permettre aux opérateurs de communiquer le traitement de priorité souhaité aux applications activées par le modèle IPCable2Home dans le réseau domestique.

10.1.1 Objectifs

Les objectifs de la qualité de service IPCable2Home sont les suivants:

- permettre aux applications de réseau domestique d'établir une transmission de données priorisée entre serveurs ainsi qu'entre les serveurs et la passerelle résidentielle au moyen d'une messagerie conforme;
- permettre aux applications de réseau domestique d'établir des priorités dans les sessions de transmission de données entre le système CMTS et le dispositif de passerelle résidentielle au moyen d'une messagerie conforme au modèle IPCablecom.

10.1.2 Hypothèses

Les hypothèses ci-après ont été faites pour la qualité de service IPCable2Home:

- afin d'éviter des problèmes avec les fonctions de conversion NAT dans l'élément de portail CAP, Les applications conformes à l'environnement IPCablecom 1.0 utiliseront l'adressage dans le secteur LAN-Pass du modèle IPCable2Home comme défini dans les § 7 et 9;
- les applications qui pourraient bénéficier de la qualité de service pourront être intégrées dans des dispositifs de serveur local IPCable2Home connectés par une technique de création de réseau domestique;
- les applications de serveur local IPCable2Home pourront comprendre des services IPCablecom.

NOTE – Tout dispositif susceptible de recevoir des messages QS pour des services d'opérateur devra être conforme à la présente Recommandation et le système d'exploitation du dispositif ainsi que la pile du réseau 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 (PS et BP) et de sous-éléments fonctionnels du modèle IPCable2Home situés dans le dispositif PS et dans les points BP. Les développeurs d'équipements de mise en réseau dans le modèle 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 ensembles minimaux de capacités spécifiés sont tenus de participer au domaine de la qualité de service. Les éléments de base de la qualité CqoS sont présentés dans le § 10.2.2.

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 un mécanisme qui commande l'accès de transmission au moyen de priorités d'accès à des supports partagés pour les éléments logiques PS et BP. 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 et qui doivent être retransmis/réexpédiés par des interfaces avec un réseau LAN.
QS 3	Gestion des caractéristiques de la QS: IPCable2Home spécifiera un mécanisme de signalisation et de gestion pour la communication de caractéristiques de qualité de service entre le dispositif PS et les points BP recherchant la QS dans un réseau domestique. Ce mécanisme sera intégré et géré dans le dispositif PS.

10.2.2 Qualité de service IPCable2Home: description du système

L'architecture de qualité CqoS se compose des entités suivantes:

- domaine de la qualité de service;
- élément de services PS (PS);
- élément de point extrême (point BP);
- sous-élément du portail de qualité de service IPCable2Home (CQP);

- sous-élément de point extrême de qualité de service IPCable2Home (QBP).

L'équipement du réseau de données par câble gère les fonctions de qualité de service IPCable2Home mais n'est pas dans le domaine de la qualité de service.

10.2.2.1 Sous-élément de portail CQP

L'élément de services PS comprend un sous-élément de portail de qualité de service IPCable2Home (CQP). Le portail CQP agit comme un portail de qualité CqoS pour les applications conformes à l'environnement IPCable2Home. Sa fonction primaire est d'offrir une qualité de service fondée sur des priorités aux dispositifs situés dans le réseau domestique. Elle 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 passant par le service portail. Elle est également chargée de la communication de caractéristiques de qualité de service à divers dispositifs domestiques.

Le portail CQP prend également en charge la livraison de messages de qualité de service dans le réseau en hybride HFC pour les applications conformes au modèle IPCablecom. La messagerie conforme au modèle IPCablecom comprend la messagerie de qualité de service et d'autres messages associés aux aspects d'un service spécifique comme les décisions de politique et d'application de modèles de réservation en deux phases. (d'après CH 1.0.)

10.2.2.2 Sous-élément de portail QBP

L'élément de point BP comprend un sous-élément de point extrême de qualité de service IPCable2Home (QBP). Il effectue un accès au support d'après des priorités pour le trafic provenant du point extrême. Il est également chargé de la réception de caractéristiques de qualité de service à partir du dispositif PS.

10.2.2.3 Fonctionnalité de qualité de service dans le portail CQP et le point QBP

Les sous-éléments de portail CQP et de point QBP comportent une ou plusieurs des fonctionnalités ci-après:

- **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 et l'accès au support partagé en fonction de priorités dans le dispositif PS. Cette fonctionnalité ne fait partie que du dispositif PS;
- **serveur (distant) de caractéristiques de qualité de service (QCS)**: cette fonctionnalité est chargée de conserver un répertoire de caractéristiques de qualité de service pour divers dispositifs et applications contenues dans le réseau domestique et également de communiquer ces caractéristiques à ces dispositifs et applications. Cette fonctionnalité ne fait partie que du dispositif PS;
- **client des caractéristiques de qualité de service (QCC)**: cette fonctionnalité, avec l'aide du serveur QCS, détermine les caractéristiques de qualité de service qu'une application ou un dispositif particulier a besoin d'utiliser. Elle ne réside que dans le point BP.

10.2.2.4 Domaine de la qualité de service

Le domaine de la qualité de service définit la sphère d'influence directe de la fonctionnalité de qualité CQoS. Le domaine de la qualité de service existe au niveau de chaque résidence et est indépendant des secteurs d'adressage. Les résidences individuelles sont distinctes et ont des domaines de qualité de service indépendants. Les éléments de portail CQP et de point BPQ limitent le domaine de la qualité de service dans une résidence donnée.

10.2.2.5 Classes de dispositifs physiques et éléments fonctionnels de qualité CqoS

Un exemple de la relation entre les dispositifs IPCable2Home et les éléments fonctionnels de qualité CqoS est présenté dans la Figure 10-1.

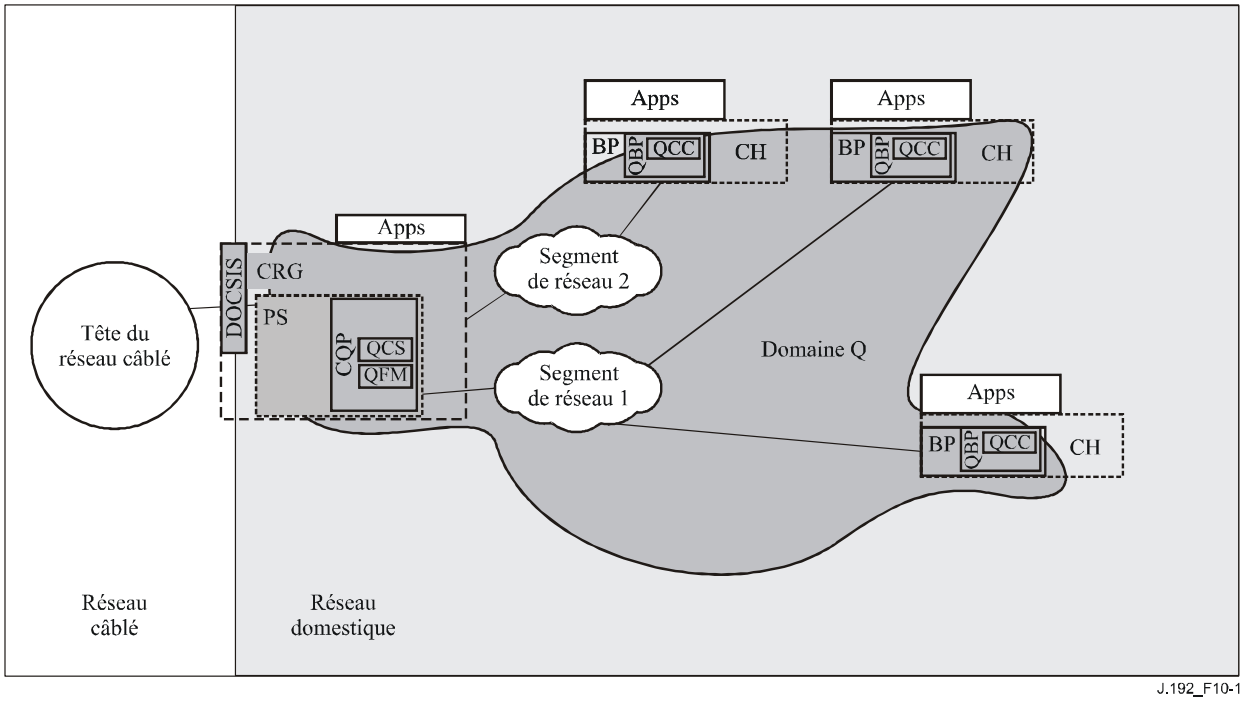


Figure 10-1/J.192 – Exemple d'éléments fonctionnels de qualité CqoS

10.2.2.6 Priorités IPCable2Home et leurs mappages

10.2.2.6.1 Priorités IPCable2Home

La présente Recommandation définit trois priorités de qualité de service différentes, qui sont les suivantes:

- priorités IPCable2Home génériques;
- priorités IPCable2Home de mise en file d'attente;
- priorités IPCable2Home d'accès au support.

10.2.2.6.1.1 Priorités IPCable2Home génériques

La présente Recommandation définit huit niveaux de priorité générique IPCable2Home, de 0 à 7, le 7^{e} étant le plus élevé et 0 étant le moins élevé. Les câblo-opérateurs peuvent attribuer une seule de ces huit priorités à une application. Sur les trois types de priorité définis, seule la valeur de priorité générique IPCable2Home pour une application peut être réglée par un câblo-opérateur. Les deux autres priorités: les priorités IPCable2Home de mise en file d'attente et les priorités IPCable2Home d'accès au support, sont déduites de cette priorité générique IPCable2Home selon les capacités du matériel et du logiciel dans le dispositif. Plus élevée est la priorité générique IPCable2Home attribuée à une application, plus élevée est la préférence accordée aux paquets de cette application dans les fonctionnalités de réexpédition de paquet et d'accès au support.

10.2.2.6.1.2 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. Donc, chaque interface a besoin d'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 a besoin d'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 de la priorité générique IPCable2Home attribuée à l'application qui a émis le paquet, au moyen du nombre de files d'attente prises en charge par une interface dans le dispositif PS. Ce mappage est spécifié dans le § 10.2.2.6.2.

10.2.2.6.1.3 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 est priorisé en fonction de la priorité attribuée aux paquets. Ainsi, une technique de partage de support a besoin d'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. la technique HomePNA prend en charge huit priorités d'accès au support, la technique HomePlug prend en charge quatre priorités d'accès au support). La priorité IPCable2Home d'accès au support d'un paquet est déduite de sa priorité générique IPCable2Home, fondée 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 défini dans le § 10.2.2.6.3. Les valeurs des priorités IPCable2Home d'accès au support sont des niveaux logiques relatifs qui représentent un niveau de préférence qu'un paquet applicatif devrait obtenir pour accéder au support. Le mappage des priorités IPCable2Home d'accès au support est séparé et distinct des mappages initiaux de priorité d'accès au support définis par les techniques de partage de support dans la couche 2, afin de conserver l'indépendance des mappages de priorités IPCable2Home d'accès au support par rapport aux techniques de couche 2.

10.2.2.6.2 Mappage des priorités IPCable2Home génériques sur les priorités IPCable2Home de mise en file d'attente

Comme décrit dans le § 10.2.2.6.1.2, le dispositif PS effectue une mise en file d'attente priorisée pour chacune de ses interfaces. Il y a huit priorités IPCable2Home génériques définies, donc un scénario idéal serait qu'une interface ait huit files d'attente et que chaque file reçoive une priorité comprise entre 0 et 7. Cependant, le nombre de files d'attente déployées à une interface du dispositif PS varie en fonction de l'implémentation. Le nombre de files d'attente prises en charge par une interface sera mémorisé dans la base de données PS et sera lisible par un objet de base MIB cabhPriorityQosPsIfAttribIfNumQueues. Si une interface implémente N ($1 \leq N \leq 8$) files d'attente, les diverses files d'attente d'une interface seront désignées avec des priorités IPCable2Home de mise en file d'attente comprises entre 0 (la plus basse) et N – 1 (la plus haute). Quand un paquet entre dans le dispositif PS, la priorité IPCable2Home de mise en file d'attente de ce paquet a besoin d'être déterminée sur la base de sa priorité générique de façon que ce paquet puisse être placé dans une file appropriée. Ce mappage entre les deux priorités est spécifié dans le Tableau 10-2.

Dans le Tableau 10-2, huit priorités génériques figurent dans la première colonne. Dans les colonnes adjacentes du tableau, le nombre de files d'attente prises en charge par l'interface est présenté comme une étendue comprise entre 8 et 1. Les entrées du tableau représentent les priorités IPCable2Home de mise en file d'attente allant de 0 à N – 1 pour les paquets.

Une fois que la priorité IPCable2Home de mise en file d'attente d'un paquet est déterminée à partir de sa priorité générique au moyen du Tableau 10-2, un paquet est placé dans une file d'attente qui est désignée pour cette priorité IPCable2Home de mise en file d'attente spécifique.

Tableau 10-2/J.192 – Mappages de priorité IPCable2Home de mise en file d'attente

Priorité IPCable2Home générique	Nombre de files prises en charge par l'interface (N)							
	8	7	6	5	4	3	2	1
7	7	6	5	4	3	2	1	0
6	6	5	4	3	3	2	1	0
5	5	4	3	2	2	1	1	0
4	4	3	2	2	2	1	1	0
3	3	2	1	1	1	1	0	0
2	2	1	1	1	1	0	0	0
1	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

NOTE – L'alinéa ci-après décrit comment le mappage des priorités IPCable2Home de mise en file d'attente devrait être utilisé:

Si un paquet de données entrantes a une priorité générique de 7 et est destiné à une interface sortante qui ne prend en charge que trois files d'attente (N = 3), alors la priorité IPCable2Home de mise en file d'attente pour ce paquet sera égale à 2. Trois files d'attente pour cette interface particulière seront désignées avec des priorités de '0' (la plus basse), '1' et '2' (la plus haute). Ce paquet particulier sera placé dans la file d'attente ayant la désignation de priorité 2 pour cette interface.

10.2.2.6.3 Mappage des priorités IPCable2Home génériques sur les priorités IPCable2Home d'accès au support

Comme exposé dans le § 10.2.2.6.1.3, diverses techniques de couche 2 prennent en charge un nombre variable de priorités d'accès au support. Donc, huit priorités IPCable2Home génériques, définies pour des applications, doivent être mappées sur un nombre approprié de priorités IPCable2Home d'accès au support, fondé sur le nombre de priorités d'accès au support ($1 \leq M \leq 8$) prises en charge par une interface à technique de couche 2. Le nombre initial de priorités d'accès au support (M) prises en charge par la technique particulière de partage de support dans la couche 2 de chaque interface dans les dispositifs PS et BP a été mémorisé dans le dispositif PS ou BP, selon le cas. Le nombre de priorités d'accès au support prises en charge par les interfaces avec le dispositif PS est disponible dans l'objet de base MIB cabhPriorityQosPsIfAttribIfNumPriorities du dispositif PS. Le nombre de priorités d'accès au support prises en charge par l'interface avec le point BP est disponible dans le dispositif PS par l'intermédiaire de l'objet de base MIB cabhPsDevBpNumberInterfacesPriorities. Le mappage entre ces deux priorités est défini dans le Tableau 10-3.

Le Tableau 10-3 est très semblable au Tableau 10-2, sauf que le mappage des valeurs de priorité générique IPCable2Home est effectué au moyen du nombre de priorités d'accès au support(M) prises en charge par une technique particulière de partage de support dans la couche 2. Les entrées dans le tableau représentent les priorités IPCable2Home d'accès au support. Ainsi, si une technique de couche 2 prend en charge M priorités d'accès au support, alors les priorités IPCable2Home d'accès au support pour cette technique iront de 0 (la plus basse) à M – 1 (la plus haute). Ces valeurs de priorité IPCable2Home d'accès au support représentent des niveaux logiques relatifs. Plus élevée est la valeur de priorité IPCable2Home d'accès au support pour le paquet, plus élevée est la préférence qu'il devrait recevoir afin d'accéder aux supports partagés. Les réalisateurs de la présente Recommandation devraient s'assurer que les paquets reçoivent un niveau préférentiel relatif d'accès préférentiel aux supports partagés, comme décrit par le mappage des priorités IPCable2Home d'accès au support.

NOTE – L'alinéa ci-après décrit comment le mappage des priorités IPCable2Home d'accès au support devrait être utilisé:

Si une valeur de priorité générique IPCable2Home pour un paquet applicatif est 7 (la plus haute) et que la technique de couche 2 dans laquelle le paquet est actuellement transmis prenne en charge 4 priorités d'accès au support alors, sur la base du Tableau 10-3, la valeur de priorité IPCable2Home d'accès au support du paquet sera 3 (la plus haute). Cependant, si une valeur de priorité générique pour un paquet est 2, la valeur de priorité IPCable2Home d'accès au support pour la technique précédente sera 1 (avant-dernière en importance). Compte tenu de ce qui précède, le mappage IPCable2Home requis peut être différent des mappages initialement utilisés par les techniques de partage de support.

Voir à l'Appendice I des exemples de différences entre les mappages de priorité IPCable2Home d'accès au support et les mappages initiaux par technique de couche 2**.**

Tableau 10-3/J.192 – Mappages des priorités IPCable2Home d'accès au support

Priorité générique IPCable2Home	**# Priorités d'accès au support prises en charge (N) dans le réseau LAN**							
	8	7	6	5	4	3	2	1
7	7	6	5	4	3	2	1	0
6	6	5	4	3	3	2	1	0
5	5	4	3	2	2	1	1	0
4	4	3	2	2	2	1	1	0
3	3	2	1	1	1	1	0	0
2	2	1	1	1	1	0	0	0
1	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

10.3 Sous-élément logique des services portail CQP

Le portail CQP contient les fonctionnalités de réexpédition QFM et de serveur QCS comme représenté dans la Figure 10-1. La fonctionnalité de réexpédition QFM est décrite dans le § 10.3.1. La fonctionnalité de serveur QCS est décrite dans le § 10.3.2.

10.3.1 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 LAN 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 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 LAN/PS et les réexpédier vers une interface avec le réseau LAN de destination en fonction de leurs priorités et des capacités de mise en file d'attente dans les interfaces avec un réseau LAN;
- offrir un accès priorisé aux supports partagés pendant la transmission des paquets en fonction de la priorité des paquets et des capacités de partage de support pour un accès priorisé.

10.3.1.2 Réexpédition et accès au support de la qualité de service: directives de conception

Tableau 10-4/J.192 – QFM: directives de conception du système

Numéro	Directives
QFM.1	La fonction QFM devrait fonctionner sur les paquets à destination et en provenance des secteurs d'adresses LAN-Trans et LAN-Pass.
QFM.2	La fonction QFM déterminera la priorité des paquets au moyen des informations disponibles dans la base MIB du dispositif PS conservée par le serveur QCS.
QFM.3	La fonction QFM ordonnera les paquets entrants de façon qu'ils ressortent par les interfaces avec un réseau LAN 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	La fonction QFM offrira un accès priorisé aux supports partagés à chaque interface, selon la priorité des paquets.
QFM.6	La fonction QFM devrait mapper la priorité générique IPCable2Home du paquet sur la priorité IPCable2Home d'accès au support conformément au mappage défini.
QFM.7	La fonction QFM devrait être en mesure de fonctionner avec des interfaces qui prennent en charge différents nombres de priorités d'accès au support.

10.3.1.3 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.

10.3.1.4 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 à la sortie du dispositif PS vers un serveur local LAN 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 dans le réseau LAN domestique reçoivent un accès priorisé aux interfaces de transmission avec le serveur local et aux supports partagés par le réseau LAN. Tout paquet sortant du dispositif PS à une interface avec un réseau LAN devrait être traité par la fonction QFM sans tenir compte de son origine.

Dès que la fonction QFM reçoit un paquet destiné à une interface particulière avec un réseau LAN, cette fonction effectue les trois actions suivantes avant que le paquet soit transmis à l'interface avec le réseau LAN de destination:

1) processus de classification afin d'identifier la priorité générique du paquet;
2) mise en file d'attente priorisée;
3) accès priorisé au support.

10.3.1.4.1 Classification du paquet afin d'identifier la priorité générique IPCable2Home

Quand le dispositif PS a besoin de transmettre un paquet par l'interface avec un réseau LAN, il examine ce paquet afin d'identifier pour lui une priorité générique IPCable2Home. Le dispositif PS lit l'adresse IP de destination et le point d'accès de destination du paquet. La base de données PS mémorise une table classificatrice (objet cabhPriorityQosDestPriorityListTable) qui fait appel à des valeurs d'adresse IP de destination et de point d'accès de destination permettant de déterminer la

priorité générique du paquet. Le remplacement par des structures génériques (0) est autorisé pour le champ de point d'accès de destination mais non pour le champ d'adresse IP de destination. Donc, le dispositif PS essaye d'abord de trouver une entrée spécifique qui corresponde à l'adresse IP de destination et au point d'accès de destination du paquet, permettant de déterminer sa priorité. Si une entrée spécifique n'est pas trouvée, le dispositif PS essaye de déterminer la priorité au moyen de la seule adresse IP de destination. Si aucune entrée n'est trouvée dans la table classificatrice pour l'adresse IP de destination et le point d'accès de destination du paquet, alors le dispositif PS attribue une valeur de priorité générique de 0 au paquet. Le dispositif PS fait appel à la valeur attribuée de priorité générique IPCable2Home permettant de déterminer la priorité IPCable2Home de mise en file d'attente du paquet et sa priorité IPCable2Home d'accès au support.

10.3.1.4.2 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 valeurs de priorité générique IPCable2Home définies par la présente Recommandation. Donc, le dispositif PS applique la valeur de priorité générique IPCable2Home du paquet à une valeur de priorité IPCable2Home de mise en file d'attente comme défini dans le § 10.2.2.6.1.2. 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 IPCable2Home de mise en file d'attente.

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*.

10.3.1.4.3 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 LAN avec une priorité appropriée. Donc, la fonction QFM applique la valeur de priorité générique IPCable2Home du paquet aux valeurs de priorité IPCable2Home d'accès au support comme décrit dans le § 10.2.2.6.3, au moyen du Tableau 10-3. 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 LAN.

10.3.1.4.4 Prise en charge des applications IPCablecom

Etant donné que l'objectif de la qualité QS est de n'être fournie que dans le réseau domestique, la présente Recommandation ne prête pas une attention particulière à la qualité QS du réseau d'accès. Cependant, un dispositif IP de réseau LAN peut héberger une application IPCablecom [J.161], [J.163], auquel cas le dispositif PS peut être configuré pour le traitement de paquet en mode de traversée de façon à dériver la messagerie QS entre l'application IPCablecom située dans le réseau domestique et le système CMTS.

Etant donné que le dispositif PS va simplement réexpédier la messagerie de qualité de service IPCablecom lors du mode de traversée, il ne dépend pas du système NMS pour remplir cette fonction. Cette fonction de portail CQP reste donc la même pour les deux modes d'approvisionnement: DHCP et SNMP (voir § 5.5).

10.3.1.5 Réexpédition et accès au support de la qualité de service: exigences

10.3.1.5.1 Classification de paquet: exigences

Quand le dispositif PS a besoin de transmettre un paquet sur une interface avec un réseau LAN, le dispositif PS DOIT déterminer la priorité générique IPCable2Home pour ce paquet à partir des valeurs de son adresse IP de destination et de son point d'accès de destination au moyen de la table classificatrice du dispositif PS (objet cabhPriorityQosBpDestTable) mémorisées dans la base de données PS (voir § E.7). Le dispositif PS DOIT toujours essayer de trouver une entrée spécifique dans la base de données PS qui corresponde aussi bien à l'adresse IP de destination qu'au point d'accès de destination du paquet, afin de déterminer sa priorité. Si une entrée spécifique n'est pas trouvée, alors le dispositif PS DOIT essayer de trouver une entrée qui corresponde seulement à l'adresse IP de destination du paquet. S'il n'y a aucune entrée dans la base de données PS qui corresponde à l'adresse IP de destination du paquet, alors le dispositif PS DOIT attribuer à ce paquet la valeur 0 de priorité générique IPCable2Home.

10.3.1.5.2 Mise en file d'attente priorisée: exigences

Le dispositif PS DOIT mémoriser le nombre de files d'attente implémentées par chacune de ses interfaces dans la base de données PS, pouvant être obtenu par une valeur d'objet cabhPriorityQosPsIfAttribIfNumQueues de base MIB (voir § E.7).

Le dispositif PS DOIT mapper la valeur de priorité générique IPCable2Home du paquet identifié pendant le processus de classification, à la valeur de priorité IPCable2Home de mise en file d'attente définie dans le § 10.2.2.6.1.2 au moyen du nombre de files d'attente (objet cabhPriorityQosPsIfAttribIfNumQueues) implémentées 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 LAN, 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, le dispositif PS 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.

10.3.1.5.3 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 cabhPriorityQosPsIfAttribIfNumPriorities (voir § E.7).

Après que le paquet a été extrait des files d'attente d'une interface particulière, le dispositif PS DOIT appliquer la priorité générique du paquet à la priorité IPCable2Home d'accès au support, comme défini dans le § 10.2.2.6.1.3, au moyen du nombre de priorités d'accès au support prises en charge (objet cabhPriorityQosPsIfAttribIfNumPriorities) 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.

10.3.1.5.4 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 [J.161], [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 d'approvisionnement: DHCP et SNMP (voir § 5.5).

10.3.2 Serveur (distant) de caractéristiques de qualité des services portail (QCS)

La fonctionnalité de serveur (distant) de caractéristiques de qualité de service (QCS) est chargée, dans le dispositif PS, de la gestion des priorités applicatives dans le réseau domestique pour le compte d'un câblo-opérateur. Le présent paragraphe fournit la description de la fonctionnalité de serveur QCS et des exigences PS associées.

10.3.2.1 Serveur (distant) de caractéristiques de qualité de service: objectifs

- Etablir un ensemble de critères permettant aux applications et aux piles du réseau d'attribuer et d'utiliser des caractéristiques de qualité de service pour le trafic dans le réseau domestique.
- Assurer un mécanisme permettant à la tête de réseau de communiquer les caractéristiques de qualité de service recherchées aux services portail puis à des serveurs locaux IPCable2Home (points BP). Plus précisément, l'attribution de caractéristiques de qualité de service est associée à la priorité des informations selon chaque type d'application.

10.3.2.2 Serveur (distant) de caractéristiques de qualité de service: directives de conception

Tableau 10-5/J.192 – Directives de conception du serveur QCS

Numéro	Directives de conception du système
QCS.1	Le serveur QCS recevra des informations sur les priorités pour chaque application à partir du serveur (distant) de gestion de réseau (NMS) situé dans la tête de réseau.
QCS.2	Les priorités des informations fournies au serveur QCS seront régies par les câblo-opérateurs (commande individuelle ou collective de mise à jour du PS).
QCS.3	Les priorités des informations fournies au serveur QCS pourront être mises à jour par la tête de réseau et les points BP (clients QCC) vont acquérir ces informations mises à jour à partir du serveur QCS.
QCS.4	Le serveur QCS utilisera un protocole de contenu de message (XML) et un protocole de transport de message (SOAP) définis pour la distribution des informations de priorité aux points BP.
QCS.5	Le serveur QCS utilisera une interface définie avec le contenu des messages (MIB) afin de fournir des informations sur les priorités de diverses applications de réseau LAN domestique au serveur (distant) de gestion de réseau (NMS) situé dans la tête de réseau.
QCS.6	Le serveur QCS facilite la fonctionnalité de réexpédition et d'accès au support de la qualité de service (QFM) afin de déterminer une priorité du paquet applicatif.

10.3.2.3 Serveur (distant) de caractéristiques de qualité de service: hypothèses

- IPCable2Home définit un format permettant d'échanger des messages entre PS et BP.
- IPCable2Home définit un protocole permettant d'échanger des informations entre PS et BP.
- Les serveurs locaux IPCable2Home peuvent avoir plusieurs services/applications.

10.3.2.4 Serveur (distant) de caractéristiques de qualité de service: description du système

Le serveur QCS conserve une "base de données" des informations contenues dans la base de données PS comme décrit dans le § 5.4. Le serveur QCS reçoit des informations de priorité relatives aux applications à partir de la tête de réseau, par configuration initiale du dispositif PS ou par une interface avec une base MIB dans le portail CMP. Le serveur QCS recueille également les informations relatives aux applications à partir de divers points BP du réseau LAN domestique et leur attribue des priorités. Le serveur QCS communique ces informations de priorité applicative aux points extrêmes (clients QCC) à utiliser pour l'accès prioritaire au support par les points BP. Ces informations, conservées par le serveur QCS, sont utilisées par la fonctionnalité de réexpédition QFM dans le dispositif PS pour la réexpédition priorisée et l'accès prioritaire au support des paquets qui le traversent.

Le reste du § 10.3.2.4 est consacré à la description de l'échange d'informations qui se produit entre la tête de réseau et le dispositif PS situé dans le réseau WAN et entre le dispositif PS et les points BP situés dans le réseau LAN.

10.3.2.4.1 Echange d'informations du côté WAN

Du côté WAN, la tête de réseau du câblo-opérateur fournit au dispositif PS un mappage des différentes applications et les priorités qu'elles devraient utiliser dans un fichier de configuration ou qu'elles devraient obtenir au moyen de commandes SET (mise à jour) du protocole SNMP. Le système NMS, en tête de réseau, peut lire et mettre à jour (ajouter/modifier/supprimer) ces priorités applicatives dans la base de données PS au moyen du protocole SNMP, par une interface avec une base MIB.

10.3.2.4.1.1 Mappages d'identificateurs d'application à la priorité générique IPCable2Home à partir de la tête de réseau vers le dispositif PS

La tête de réseau offre au dispositif PS une liste d'identificateurs d'application avec leurs priorités IPCable2Home génériques qu'un câblo-opérateur souhaite voir utilisées par ces applications. Ces informations sont fournies aux services 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 une table de base MIB, cabhPriorityQosMasterTable (voir § E.7) que le dispositif PS utilise comme table de référence des priorités afin d'identifier celles-ci pour diverses applications fonctionnant aux points extrêmes du réseau LAN domestique.

Le dispositif PS peut également recevoir des demandes issues du système NMS afin de mettre à jour (ajouter/modifier/supprimer) ces priorités IPCable2Home génériques pour les applications contenues dans sa table de référence, au moyen du protocole SNMP. En réponse à ces requêtes, le dispositif PS met à jour (ajouter/modifier/supprimer) la table de référence des priorités (objet cabhPriorityQosMasterTable). De telles mises à jour des priorités applicatives sont communiquées aux points extrêmes pendant les échanges ultérieurs d'informations du côté LAN, ce qui est décrit dans le § 10.3.2.4.2.

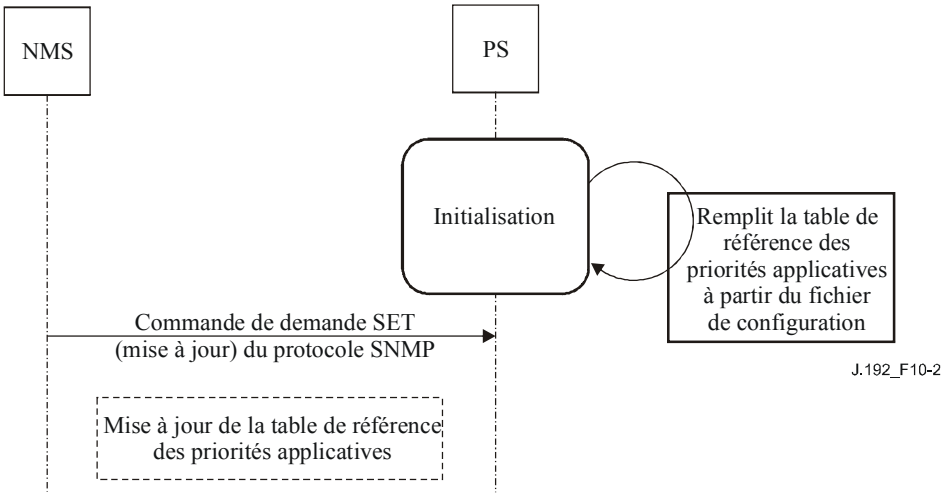


Figure 10-2/J.192 – Echange et traitement d'informations de réseau WAN dans le dispositif PS

10.3.2.4.2 Echange d'informations du côté LAN

Du côté LAN, un dispositif de point BP communique aux services portail ses informations relatives aux applications et aux sessions (adresses IP de destination et points d'accès) afin d'obtenir leurs priorités. Une fois que le dispositif PS reçoit ces informations, il détermine les priorités appropriées en les recherchant par exploration dans la table de référence des priorités et les réachemine jusqu'au point extrême. Ces informations sont échangées entre dispositifs PS et BP au moyen du schéma XML d'objet QoSProfile (décrit ci-dessous dans le § 10.3.2.4.2.1) et de la messagerie lancée par point extrême en protocole SOAP (Opération BP_Init) comme décrit dans le § 6.3.3.4.3.2.

10.3.2.4.2.1 Schéma XML d'objet QoSProfile

Le schéma XML d'objet QoSProfile contient deux séquences complexes en langage XML: QoSApplicationList et DesPriorityList. L'objet QoSApplicationList contient quatre éléments: BpIpAddress, ApplicationId, DefaultCHPriority et une séquence de DestPriorityList. Le type complexe DestPriorityList, qui est considéré comme une séquence secondaire dans l'objet QoSApplicationList, contient trois éléments: DestIp, DestPort et IpPortPriority. Chaque élément a un type défini comme indiqué dans le Tableau 10-6. Les types définis sont des références extraites des définitions de schéma XML établies par le groupe W3C [XML].

L'élément ApplicationId est le numéro de point d'accès du serveur applicatif pour chaque application de point BP attribuée par l'autorité IANA [IANAPort]. Bien que les applications soient identifiées par le numéro de point d'accès IANA, une communication peut également intervenir à d'autres numéros de point d'accès. Le point BP communique au dispositif PS une liste d'identificateurs d'application pour toutes les applications installées à ce point, par le message BP_Init (décrit dans le § 10.4.1.4.1.1).

L'élément DefaultCHPriority est la priorité par défaut IPCable2Home pour une application. Le point BP peut offrir une valeur pour cet élément dans l'objet QoSProfile. Cette valeur sera remplacée en surécriture par la valeur fournie par le dispositif PS dans le message BP_Init_Response (décrit ci-dessous dans le § 10.3.2.4.2.3), après consultation de la table de référence des priorités d'application dans la base de données PS (objet cabhPriorityQosMasterTable).

Le point BP comprend une ou plusieurs séquence(s) DestPriorityListEntry dans l'objet QoSProfile pour une session d'application avec un autre dispositif. La ou les séquences DestPriorityListEntry sont associées à l'élément ApplicationId dans le schéma XML d'objet QoSProfile. Les éléments DestIP et DestPort correspondent respectivement à l'adresse IP de destination et au numéro de point

d'accès de destination de la session d'application (connexion d'accès par numéro logique) qui est établie par le point extrême. Ces entrées servent à déterminer la priorité (IpPortPriority) du trafic traversant le dispositif PS, sur la base de l'adresse IP de destination et du numéro de point d'accès spécifiquement indiqués dans l'entrée. Le remplacement par des structures génériques (0) n'est autorisé que pour l'élément DestPort, mais non pour l'élément DestIP. Le point BP peut offrir une valeur pour l'élément IpPortPriority dans l'objet QoSProfile. Le dispositif PS remplace par surécriture cette valeur par l'élément DefaultCHPriority fourni dans le message BP_Init_Response, après consultation de la table de référence des priorités d'application dans la base de données PS (objet cabhPriorityQosMasterTable).

Un point BP est toujours tenu de transmettre l'entier schéma XML d'objet QoSProfile au dispositif PS chaque fois qu'il envoie le message BP_Init.

Tableau 10-6/J.192 – Schéma XML du profil de qualité de service

```
<xs:complexType name= "ch:QoSProfile"/>
      <xs:element name ="ch:QoSApplicationList"   type="ch:QoSApplicationListEntry minOccurs="1"
maxOccurs="4"/>"
</xs:complexType>


<xs:complexType name= "ch:QoSApplicationListEntry>
   <xs:sequence>
        <xs:element name="ch:BpIpAddress"              type="xs:string"/>
        <xs:element name="ch:ApplicationId"             type="xs:int"/>
        <xs:element name="ch:DefaultCHPriority"       type="xs:int"/>
        <xs:element name="ch:DestPriorityList"   type="ch:DestPriorityListEntry minOccurs="0"
maxOccurs="4"/>"
    </xs:sequence>
</xs:complexType>


<xs:complexType name= "ch:DestPriorityListEntry>
   <xs:sequence>
         <xs:element name="ch:DestIp"           type="xs:string"/>
         <xs:element name="ch:DestPort"         type="xs:int"/>
         <xs:element name="ch:IpPortPriority"   type="xs:int"/>
    </xs:sequence>
</xs:complexType>
```

10.3.2.4.2.2 Transfert des informations de point BP au dispositif PS au moyen du message BP_Init

Un point BP est tenu d'envoyer au dispositif PS ses informations relatives aux applications et aux sessions, dans le format du schéma XML d'objet QoSProfile, au moyen du message BP_Init comme décrit dans le § 6.3.3.4.3.2.1, dans les trois occasions suivantes:

- acquisition ou renouvellement de location DHCP;
- mise à jour d'application (addition ou suppression) dans un dispositif de point BP;
- établissement et terminaison de session d'application avec un autre dispositif, au moyen d'un point BP.

Voir au § 10.4.1.4.1.1.1 une description détaillée de l'échange d'informations par point BP dans chacune des trois occasions précédentes.

10.3.2.4.2.3 Informations de priorité de PS à BP au moyen du message BP_Init_Response

Le traitement du schéma XML d'objet QoSProfile par le dispositif PS est exactement le même dans les trois occasions différentes (susmentionnés dans le § 10.3.2.4.2.2), quand le dispositif PS reçoit le message BP_Init. Le traitement du schéma XML d'objet QoSProfile est décrit ci-dessous:

dès réception du schéma XML d'objet QoSProfile à partir du point extrême dans le message BP_Init, le dispositif PS détermine les valeurs des éléments DefaultCHPriority (faisant partie de QoSApplicationListEntry) et IpPortPriority (faisant partie de DestPriorityListEntry) pour toutes les applications contenues dans l'objet QoSProfile par exploration de la table de référence des priorités dans la base de données PS (objet cabhPriorityQosMasterTable). Le dispositif PS met à jour l'élément QosProfile du point BP avec ces priorités par la surécriture des valeurs que le point BP peut avoir fournies dans son élément original QoSProfile.

Le dispositif PS mémorise alors ces informations de priorité d'application au point BP, représentées par l'élément mis à jour QoSProfile, dans la base de données PS qui est accessible par les tables de base MIB cabhPriorityQosBpTable et cabhPriorityQosBpDestTable (voir § E.7). Le dispositif PS remplace complètement les anciennes informations BP de priorité relatives aux applications qui peuvent avoir été mémorisées dans sa base de données par les nouvelles informations représentées par l'élément mis à jour QoSProfile. Un tel remplacement complet des anciennes informations BP de priorité relatives aux applications vise le traitement de l'addition comme de la suppression d'une nouvelle application ou session dans le point BP et maintient à un niveau minimal la complexité de traitement dans le dispositif PS.

La table cabhPriorityQosBpTable représente des informations sur diverses applications et leurs priorités à un certain point extrême du réseau LAN domestique. L'objet cabhPriorityQosBpDestTable représente les priorités spécifiques d'adresse IP de destination et de point d'accès pour différentes sessions d'application au point BP. La fonctionnalité de réexpédition QFM contenue dans le dispositif PS utilise ces informations représentées par l'objet cabhPriorityQosBpDestTable pour sa mise en file d'attente priorisée et son accès prioritaire au support dans le dispositif PS.

Après mise à jour de la base de données avec les informations de priorité d'application au point BP, le dispositif PS envoie au point extrême le profil BP QoSProfile mis à jour avec les informations de priorité, au moyen du message BP_Init_Response comme décrit dans le § 6.3.3.4.3.2.2. Cet élément mis à jour QoSProfile achemine au point extrême les informations appropriées de priorité qu'il est tenu d'utiliser pour ses applications.

10.3.2.5 Exigences relatives au serveur (distant) de caractéristiques de qualité de service

10.3.2.5.1 Exigences relatives à l'échange d'informations du côté WAN

Le dispositif PS DOIT mémoriser une liste d'identificateurs d'applications avec leurs priorités IPCable2Home génériques, offerte par un câblo-opérateur, dans la base de données PS qui est accessible (voir § E.7). Le dispositif PS DOIT prendre en charge la mise à jour (ajouter/modifier/supprimer) de cette table de référence des priorités (objet cabhPriorityQosMasterTable) par 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 à l'échange d'informations du côté LAN

Le traitement du schéma XML d'objet QoSProfile par le dispositif PS est identique dans les trois occasions différentes (susmentionnées dans le § 10.3.2.4.2.2) quand il reçoit le message BP_Init.

Le dispositif PS DOIT être capable de traiter le schéma XML d'objet QoSProfile de point BP (comme décrit dans le § 10.3.2.4.2.1) contenant ses informations d'applications et de sessions (adresse IP et point d'accès de destination) reçues dans le message BP_Init (comme décrit dans

le § 6.3.3.4.3.2). Quand il reçoit le schéma XML d'objet QoSProfile à partir du point extrême (à l'une des trois occasions décrites dans le § 10.3.2.4.2.2) dans le message BP_Init, le dispositif PS DOIT déterminer les valeurs des éléments DefaultCHPriority (faisant partie de l'objet QoSApplicationListEntry) et IpPortPriority (faisant partie de DestPriorityListEntry) pour toutes les applications contenues dans l'objet QoSProfile par exploration de la table de référence des priorités contenue dans la base de données PS (objet cabhPriorityQosMasterTable). Le dispositif PS DOIT mettre à jour l'élément QosProfile du point BP avec ces valeurs de priorité par surécriture des valeurs que le point BP peut avoir offertes dans son élément original QoSProfile.

Le dispositif PS alors DOIT mémoriser ces informations de priorité d'application au point BP, représentées par l'élément mis à jour QoSProfile, dans la base de données PS qui est accessible par les tables de base MIB cabhPriorityQosBpTable et cabhPriorityQosBpDestTable (voir § E.7). Le dispositif PS DOIT remplacer complètement les anciennes informations BP de priorité relatives aux applications, qui peuvent avoir été mémorisées dans sa base de données, par les nouvelles informations représentées par l'élément mis à jour QoSProfile.

Après mise à jour de la base de données PS avec les informations de priorité d'application au point BP, le dispositif PS DOIT envoyer au point extrême l'élément entier BP QoSProfile, mis à jour avec les informations de priorité, au moyen du message BP_Init_Response, comme décrit dans le § 6.3.3.4.3.2.2.

10.4 Sous-élément logique de point extrême QBP

10.4.1 Client des caractéristiques de qualité de service (QCC)

10.4.1.1 Client des caractéristiques de qualité de service: objectifs

- Offrir un mécanisme permettant à un serveur local IPCable2Home de recevoir les caractéristiques de qualité de service recherchées à partir du dispositif PS. Ces caractéristiques de qualité de service sont communiquées au dispositif PS à partir de la tête de réseau.
- Etablir un ensemble de critères dans un serveur local IPCable2Home permettant à ses applications et piles de réseau d'attribuer et d'utiliser les caractéristiques de qualité de service pour son trafic applicatif.

10.4.1.2 Client des caractéristiques de qualité de service: hypothèse de conception

Un serveur local conforme à l'environnement IPCable2Home (point BP) peut comporter plusieurs services/applications.

10.4.1.3 Client des caractéristiques de qualité de service: directives de conception du système

Tableau 10-7/J.192 – Directives de conception du client QCC

Numéro	Directives
QCC.1	Le client QCC recevra les informations relatives aux priorités applicatives à partir du serveur QCS.
QCC.2	Les priorités régies par le serveur QCS seront mises à jour dynamiquement et le client QCC demandera des informations mises à jour de priorité à partir du serveur QCS.
QCC.3	Le client QCC utilisera un protocole défini de contenu de message (XML) et un protocole défini de transport de message (SOAP) pour communiquer les informations de priorité au dispositif PS.
QCC.4	Le client QCC offrira un accès priorisé aux supports partagés de son interface avec un réseau LAN selon la priorité des paquets.

10.4.1.4 Client des caractéristiques de qualité de service: description du système

Le présent paragraphe offre un aperçu général des principaux concepts du client de caractéristiques de qualité de service (QCC) au point extrême.

La messagerie du client QCC est étroitement associée à celle du serveur QCS décrit dans le § 10.3.2.4.2. Le client QCC au point BP est un homologue du serveur QCS dans le dispositif PS. Le client QCC effectue tous les échanges de messages de profil QoSProfile avec le dispositif PS (comme décrit dans le § 10.3.2.4.2) pour le compte du point extrême, au moyen de la messagerie lancée par le point extrême en protocole SOAP (§ 6.3.3.4.3.2). Donc, le client QCC obtient des informations de priorité pour diverses applications et sessions applicatives au point extrême. Le client QCC conserve une base de données interne afin de mémoriser les informations de priorité relatives aux applications qu'il reçoit du serveur QCS et fait appel à ces informations afin de prioriser son flux applicatif.

Le client QCC est également chargé du mappage de la priorité générique IPCable2Home du paquet applicatif sur les priorités IPCable2Home d'accès au support, au moyen du nombre de priorités d'accès au support prises en charge par l'interface avec le point BP, comme spécifié dans le § 10.2.2.6.3.

Le client QCC est chargé des deux principales fonctions suivantes dans le point extrême:

- échange d'informations du côté LAN;
- accès prioritaire au support pour les applications de point BP.

NOTE – Le reste du § 10.4.1.4 est consacré à la description de ces deux fonctions principales du client QCC.

10.4.1.4.1 Echange d'informations du côté LAN

Comme décrit dans le § 10.3.2.4.2, un dispositif de point BP est tenu de communiquer au dispositif PS ses informations relatives aux applications et sessions (adresse IP et point d'accès de destination) afin d'obtenir leurs priorités. Après avoir envoyé les informations de priorité au point extrême, le dispositif PS mémorise ces informations dans sa base de données et y fait appel pour l'accès priorisé au support. Ce point BP est tenu d'envoyer ses informations au dispositif PS au moyen du schéma XML d'objet QoSProfile (décrit ci-dessous dans le § 10.3.2.4.2.1) et de la messagerie lancée par point extrême en protocole SOAP (opération BP_Init), comme décrit dans le § 6.3.3.4.3.2.

10.4.1.4.1.1 Transfert des informations de point BP au dispositif PS au moyen du message BP_Init

Un point BP est toujours tenu d'acheminer ses informations au dispositif PS dans le format du schéma XML d'objet QoSProfile (Tableau 10-6) au moyen du message BP_Init, comme décrit dans le § 6.3.3.4.3.2.1. Un dispositif de point BP envoie toujours son schéma QoSProfile entier au dispositif PS. Comme décrit dans le § 10.3.2.4.2.2, un dispositif de point BP est tenu d'envoyer le message BP_Init avec son schéma QoSProfile entier au dispositif PS dans les trois occasions suivantes:

- acquisition ou renouvellement de location DHCP;
- mise à jour d'application (addition ou suppression) dans un dispositif de point BP;
- ouverture ou fermeture – par un dispositif de point BP – de session d'application avec un autre dispositif.

10.4.1.4.1.1.1 Informations sur les applications et sur le dispositif BP envoyées au dispositif PS lors d'une acquisition ou d'un renouvellement de location DHCP à un point BP

Après avoir reçu le message ACK du protocole DHCP [RFC 2131] adressé à lui-même au moment de l'acquisition ou du renouvellement d'une location DHCP, un dispositif de point BP est tenu d'envoyer au dispositif PS ses informations de priorité de dispositif et d'application au moyen du

message BP_Init. Les informations relatives au dispositif de point BP sont envoyées au moyen du schéma XML de profil de dispositif (défini dans le § 6.5.3.1.4) et les informations de priorité relatives aux applications sont envoyées au moyen du schéma XML d'objet QoSProfile.

Le profil du dispositif de point extrême envoyé au dispositif PS contient un certain nombre de priorités d'accès au support (élément XML: numberMediaAccessPriorities) prises en charge par une interface dans un dispositif de point BP. Cet échange et ce traitement d'informations sont décrits dans le § 6.5.3.3, "Fonction de découverte de point MBP". Au moyen de ces informations, le dispositif PS remplit l'objet cabhPsDevBpNumberInterfacePriorities (voir § E.4) de base MIB, qui fait partie de l'objet cabhPsDevBpProfileTable (voir § E.4) de base MIB.

L'élément QosProfile du point BP envoyé au dispositif PS, après acquisition ou renouvellement de location DHCP au point BP, contient une liste d'applications fonctionnant au point BP (QoSApplicationListEntry). Il peut également (facultativement) contenir des entrées d'adresse IP de destination et de point d'accès spécifiques (DestPriorityListEntry) associées à une application. Ces informations sont formatées conformément au schéma XML d'objet QoSProfile comme décrit dans le Tableau 10-6. Le point BP peut (facultativement) offrir les valeurs des éléments XML DefaultCHPriority et IpPortPriority.

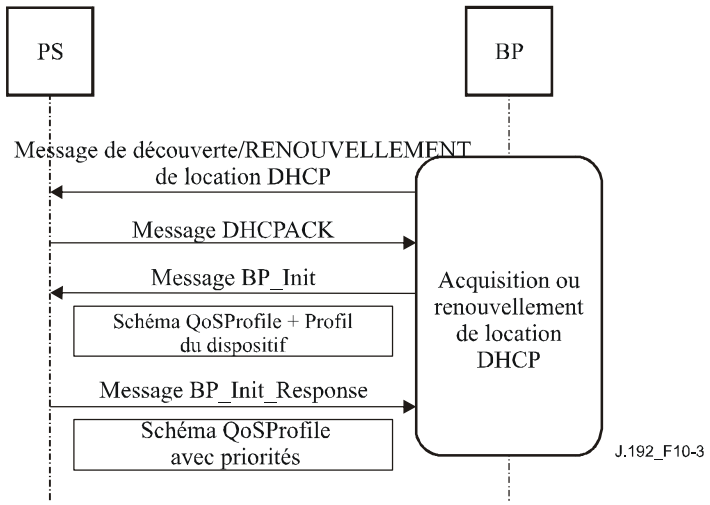


Figure 10-3/J.192 – Echange d'informations sur l'acquisition ou le renouvellement de location à un point extrême

10.4.1.4.1.1.2 Informations relatives aux applications de point BP envoyées au dispositif PS lors d'une mise à jour d'application dans le point extrême

Quand une nouvelle application est ajoutée au point BP, celui-ci ajoute une entrée pour cette application (QoSApplicationListEntry) dans son schéma XML existant d'objet QoSProfile. Le point BP peut également (facultativement) remplir l'élément DefaultCHPriority associé à cet identificateur d'application dans l'objet QoSProfile. Il peut également inclure la séquence DestPriorityListEntry pour cet identificateur d'application. Le point BP est alors tenu d'envoyer ce nouveau schéma XML d'objet QoSProfile au dispositif PS au moyen du message BP_Init.

Quand une application est supprimée à partir du point extrême, le point BP est tenu de supprimer toutes les entrées (QoSApplicationListEntry ainsi que DestPriorityListEntry) associées à cette application particulière à partir de son schéma QoSProfile. Le point BP est alors tenu d'envoyer ce schéma modifié QoSProfile au dispositif PS au moyen du message BP_Init.

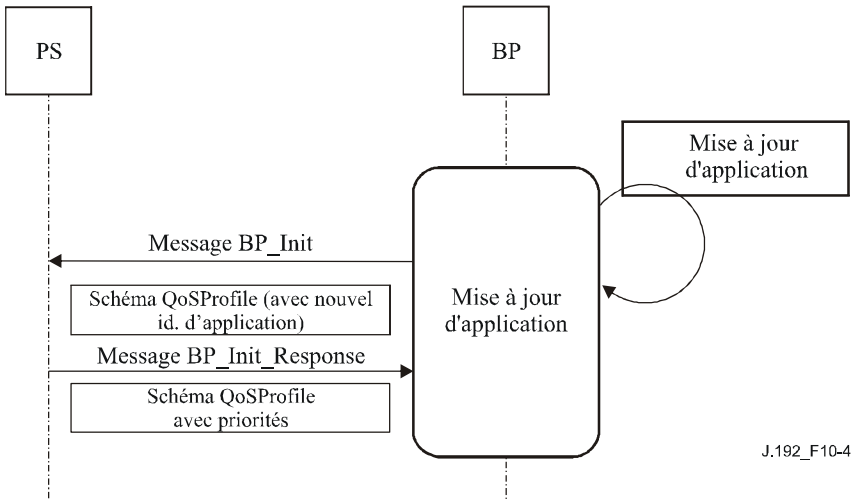


Figure 10-4/J.192 – Echange d'informations sur la mise à jour d'application à un point extrême

10.4.1.4.1.1.3 Informations relatives aux applications de point BP envoyées au dispositif PS lors d'une ouverture ou fermeture de session d'application

Après qu'une application a ouvert dans un dispositif de point BP une session avec un autre dispositif, le point BP ajoute les informations d'adresse IP de destination et de point d'accès de destination de la session (DestPriorityListEntry) associées à cette application (identificateurs d'application) dans son schéma XML d'objet QoSProfile (Tableau 10-6). Le point BP peut (facultativement) remplir l'élément IpPortPriority contenu dans l'objet DestPriorityListEntry. Le point BP envoie alors ce schéma XML d'objet QoSProfile au dispositif PS au moyen du message BP_Init de façon que le dispositif PS puisse créer des entrées dans sa table classificatrice (objet cabhPriorityQosBpDestTable) après avoir identifié une priorité (IpPortPriority) pour l'entrée au moyen de la table de référence des priorités. Ces entrées de classificateur sont utilisées par la fonctionnalité de réexpédition QFM dans le dispositif PS afin de déterminer les priorités des paquets en examinant leur adresse IP de destination et leur point d'accès (s'ils se trouvent en traversée du dispositif PS). Au moyen de ces entrées dans la table classificatrice, la fonction QFM effectue la mise en file d'attente priorisée et l'accès prioritaire au support comme décrit dans le § 10.3.1.4.

Une fois que le point BP a fermé une session, le point BP supprime l'entrée spécifiquement correspondante d'adresse IP et de point d'accès de destination, DestPriorityListEntry, de son schéma XML d'objet QoSProfile et envoie au dispositif PS cet élément QoSProfile mis à jour au moyen du message BP_Init de façon que le dispositif PS puisse supprimer les entrées dans sa table classificatrice.

Ces entrées spécifiques d'adresse IP et de point d'accès de destination dans la table classificatrice du dispositif PS (objet cabhPriorityQosBpDestTable) peuvent servir à effectuer une réexpédition priorisée de paquet et un accès prioritaire au support pour le trafic allant du dispositif PS à un dispositif uniquement destinataire et non conforme.

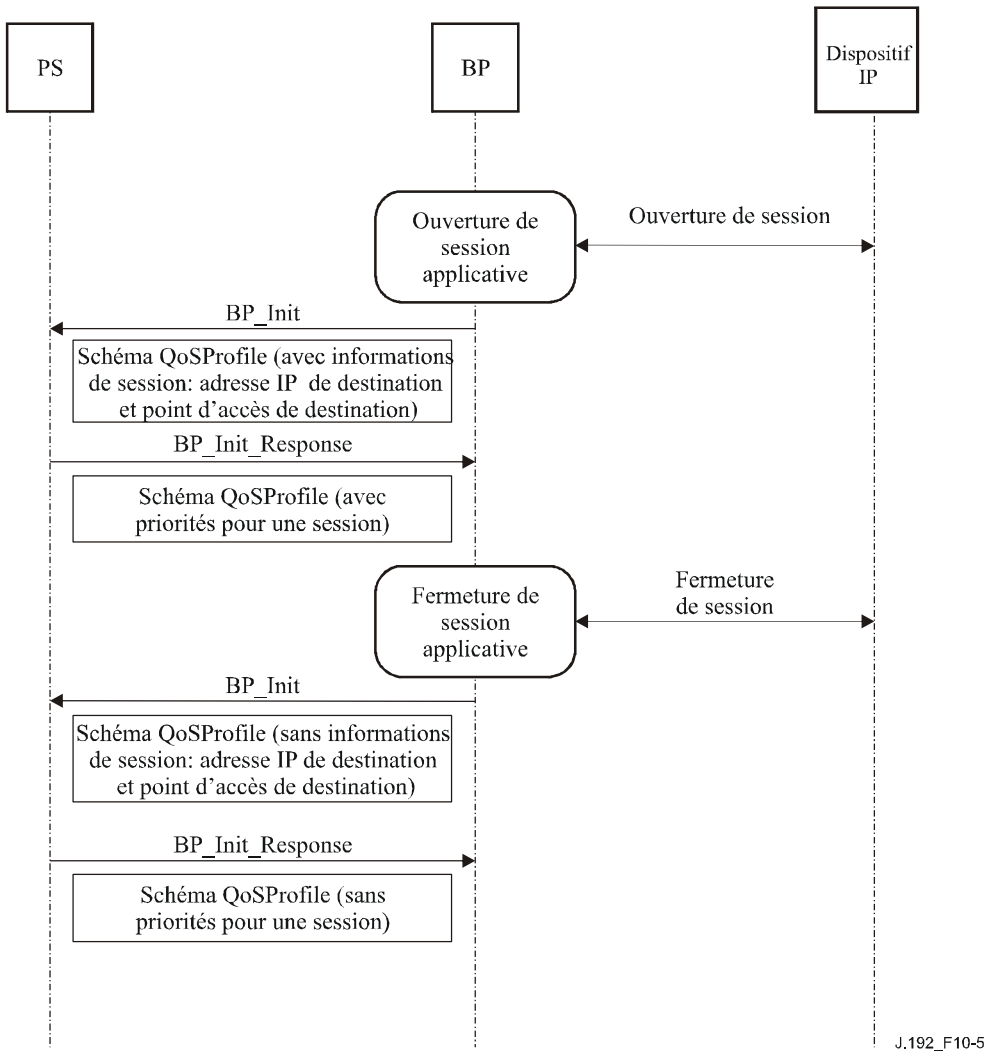


Figure 10-5/J.192 – Echange d'informations sur l'ouverture et la fermeture d'une session de point extrême

10.4.1.4.1.2 Réception d'informations sur les priorités à partir du dispositif PS dans le message BP_Init_Response

Un point BP reçoit des informations sur les priorités pour ses applications (élément DefaultCHPriority) et pour ses sessions applicatives (élément IpPortPriority) dans le message BP_Init_Response envoyé par le dispositif PS dans le format du schéma XML d'objet QoSProfile. Du point de vue d'un point BP, le processus de réception et de traitement du schéma XML d'objet QoSProfile, après réception du message BP_Init_Response à partir du dispositif PS, est exactement le même pour chacune des trois occasions (comme indiqué ci-dessus dans le § 10.4.1.4.1.1), quand il envoie le message BP_Init.

Dès réception de ces informations, le point BP remplace complètement, dans sa base de données, son schéma déjà mémorisé XML d'objet QoSProfile par le schéma nouvellement reçu QoSProfile. Le point BP fait appel aux informations de priorité fournies dans ce schéma XML d'objet QoSProfile afin de déterminer des priorités pour ses applications (identificateurs d'application) et ses sessions applicatives (identifiées par leur adresse IP de destination et leur point d'accès de destination).

10.4.1.4.2 Accès priorisé au support

Le point BP fait appel à des informations de priorité relatives aux applications qu'il reçoit du dispositif PS dans le schéma XML d'objet QoSProfile (Tableau 10-6) afin d'identifier une priorité

générique IPCable2Home pour tous les paquets à transmettre sur son interface avec un réseau LAN. Si l'adresse IP de destination et le numéro de point d'accès pour un paquet applicatif correspondent aux éléments DestIP et DestPort de toutes les séquences de l'élément DestPriorityListEntry dans le schéma XML d'objet QoSProfile, le point BP fait appel à une valeur de priorité spécifiée par l'élément IpPortPriority de cette séquence DestPriorityListEntry, en tant que priorité générique IPCable2Home pour ce paquet. Sinon, le point BP fait appel à l'élément DefaultCHPriority correspondant à l'élément CHApplicationId, en tant que priorité générique IPCable2Home pour le paquet. Le point BP applique cette priorité générique IPCable2Home du paquet à une priorité IPCable2Home d'accès au support comme spécifié dans le § 10.2.2.6.3, au moyen de l'élément numberMediaAccessPriorities du schéma XML de profil de dispositif de point extrême (§ 6.5.3.1). Le point BP émet alors le paquet par sa technique de partage de support de telle façon que l'accès préférentiel relatif du paquet aux supports partagés soit conservé comme requis par la valeur de la priorité IPCable2Home d'accès au support.

10.4.1.5 Exigences relatives au client des caractéristiques de qualité de service

10.4.1.5.1 Exigences relatives à l'échange d'informations du côté LAN

Le présent paragraphe spécifie les exigences du point BP relatives à l'échange d'informations qu'il a besoin d'exécuter afin d'obtenir des informations sur les priorités à partir du dispositif PS pour ses applications et sessions.

10.4.1.5.1.1 Transfert des informations de point BP au dispositif PS au moyen du message BP_Init

Un dispositif de point BP DOIT communiquer au dispositif PS ses informations sur les applications et sessions afin de recevoir les informations de priorité (adresse IP et point d'accès de destination) qui les concernent, dans le format du schéma XML d'objet QoSProfile (Tableau 10-6), au moyen du message BP_Init comme décrit dans le § 6.3.3.4.3.2.1. Un dispositif de point BP DOIT envoyer le message BP_Init avec son schéma QoSProfile entier au dispositif PS dans les trois occasions suivantes:

- acquisition ou renouvellement de location DHCP;
- mise à jour d'application (addition ou suppression) dans un dispositif de point BP;
- ouverture ou fermeture – par un dispositif de point BP – d'une session d'application avec un autre dispositif.

10.4.1.5.1.1.1 Informations sur les applications et sur le dispositif BP envoyées au dispositif PS lors d'une acquisition/d'un renouvellement de location DHCP au point BP

Après avoir reçu un message ACK du protocole DHCP [RFC 2131] adressé à lui-même au moment de l'acquisition ou du renouvellement d'une location DHCP, le point BP est tenu d'envoyer ses informations de priorité de dispositif et d'application au dispositif PS au moyen du message BP_Init comme spécifié dans le § 6.5.3.3.4.

Le point BP DOIT inclure sa liste d'applications (QoSApplicationListEntry) dans l'objet QoSProfile envoyé au dispositif PS après son acquisition ou renouvellement de location DHCP. Le point BP peut inclure dans ce schéma QoSProfile les entrées spécifiques d'adresse IP de destination et de point d'accès (DestPriorityListEntry) associées à une application. Le point BP peut également offrir dans ce schéma QoSProfile les valeurs des éléments DefaultCHPriority et IpPortPriority en langage XML.

10.4.1.5.1.1.2 Informations relatives aux applications de point BP envoyées au dispositif PS lors d'une mise à jour d'application dans le point extrême

Quand une nouvelle application est ajoutée au point BP, celui-ci DOIT ajouter dans son schéma existant XML d'objet QoSProfile une entrée pour cette application (QoSApplicationListEntry). Le

point BP peut (facultativement) remplir dans l'objet QoSProfile l'élément DefaultCHPriority associé à cet identificateur d'application. Le point BP peut également inclure la séquence DestPriorityListEntry pour cet identificateur d'application.

Quand une application est supprimée du point extrême, le point BP DOIT supprimer de son schéma QoSProfile toutes les entrées (QoSApplicationListEntry ainsi que DestPriorityListEntry) associées à cette application particulière.

Après une telle mise à jour du schéma XML d'objet QoSProfile, le point BP est tenu d'envoyer ce nouveau schéma XML d'objet QoSProfile au dispositif PS au moyen du message BP_Init.

10.4.1.5.1.1.3 Informations relatives aux applications de point BP envoyées au dispositif PS lors d'une ouverture ou fermeture de session d'application

Quand une application située dans un dispositif de point BP ouvre une session avec un autre dispositif, le point BP DOIT ajouter – dans son schéma XML d'objet QoSProfile (Tableau 10-6) – les informations d'adresse IP de destination et de point d'accès de destination (DestPriorityListEntry) de la session qui sont associées à cette application (identificateurs d'application). Le point BP peut "remplacer par une structure générique" (0) l'élément DestPort. Le point BP NE DOIT PAS "remplacer par une structure générique" l'élément DestIP. Le point BP peut (facultativement) remplir l'élément IpPortPriority dans la séquence DestPriorityListEntry.

Quand une application sur un dispositif de point BP ferme une session, le point BP DOIT supprimer – de son schéma XML d'objet QoSProfile – l'entrée spécifique correspondante d'adresse IP de destination et de point d'accès, DestPriorityListEntry.

Après une telle mise à jour du schéma XML d'objet QoSProfile, le point BP est tenu d'envoyer ce nouveau schéma XML d'objet QoSProfile au dispositif PS au moyen du message BP_Init de façon que le dispositif PS puisse mettre à jour (addition/suppression) les entrées de sa table classificatrice (objet cabhPriorityQosBpDestTable).

Ces entrées spécifiques d'adresse IP de destination et de point d'accès dans la table classificatrice du dispositif PS (objet cabhPriorityQosBpDestTable) PEUVENT servir à fournir une réexpédition priorisée de paquet et un accès prioritaire de paquet au support pour le trafic allant du dispositif PS à un dispositif uniquement destinataire et non conforme.

10.4.1.5.1.2 Informations sur les priorités envoyées par le dispositif PS à un point extrême dans le message BP_Init_Response

Un point BP DOIT être capable de traiter des informations sur les priorités de ses applications (DefaultCHPriority) et de ses sessions applicatives (IpPortPriority), qu'il reçoit du dispositif PS dans le format du schéma XML d'objet QoSProfile (Tableau 10-6) au moyen du message BP_Init_Response. Dès réception de ces informations, le point BP DOIT remplacer complètement son schéma XML déjà mémorisé d'objet QoSProfile, par le schéma XML d'objet QoSProfile nouvellement reçu.

10.4.1.5.2 Exigences relatives à l'accès prioritaire au support

Le point BP DOIT utiliser les informations de priorité d'application (DefaultCHPriority ou IpPortPriority) qu'il reçoit du dispositif PS dans le schéma XML d'objet QoSProfile (Tableau 10-6) afin d'identifier une priorité générique IPCable2Home pour tous les paquets à transmettre sur son interface avec un réseau LAN. Si l'adresse IP de destination et le numéro de point d'accès d'un paquet applicatif correspondent aux éléments DestIP et DestPort de l'une quelconque des séquences DestPriorityListEntry dans le schéma XML d'objet QoSProfile, alors le point BP DOIT utiliser une valeur de priorité spécifiée par l'élément IpPortPriority de cette séquence DestPriorityListEntry en tant que priorité générique IPCable2Home pour ce paquet. Sinon, le point BP DOIT utiliser l'élément DefaultCHPriority correspondant à l'identificateur CHApplicationId en tant que priorité générique IPCable2Home pour le paquet. Le point BP DOIT appliquer cette priorité générique

IPCable2Home du paquet à une priorité IPCable2Home d'accès au support comme spécifié dans le § 10.2.2.6.3, au moyen de l'élément numberMediaAccessPriorities du schéma XML de profil de dispositif de point extrême (§ 6.5.3.1). Le point BP DOIT ensuite transmettre le paquet par sa technique de partage de support de telle façon que l'accès préférentiel relatif du paquet aux supports partagés, tel que requis par la valeur de priorité IPCable2Home d'accès au support, soit conservé.

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 LAN 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 LAN 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 [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 LAN, 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 portail (PS) qui comprend des fonctions de gestion, d'approvisionnement, 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), serveur de protocole de configuration dynamique du serveur local (DHCP) [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) dans le réseau câblé.

L'architecture de sécurité se concentre sur la sécurisation du réseau LAN 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
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 points d'accès, les adresses IP et l'heure actuelle
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.

Tableau 11-1/J.192 – Sécurité: directives de conception du système

Référence	Directives
SEC11	Le pare-feu protégera les réseaux LAN et WAN 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 PS.
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 portail" – Configuration globale des services 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 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 PS 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.

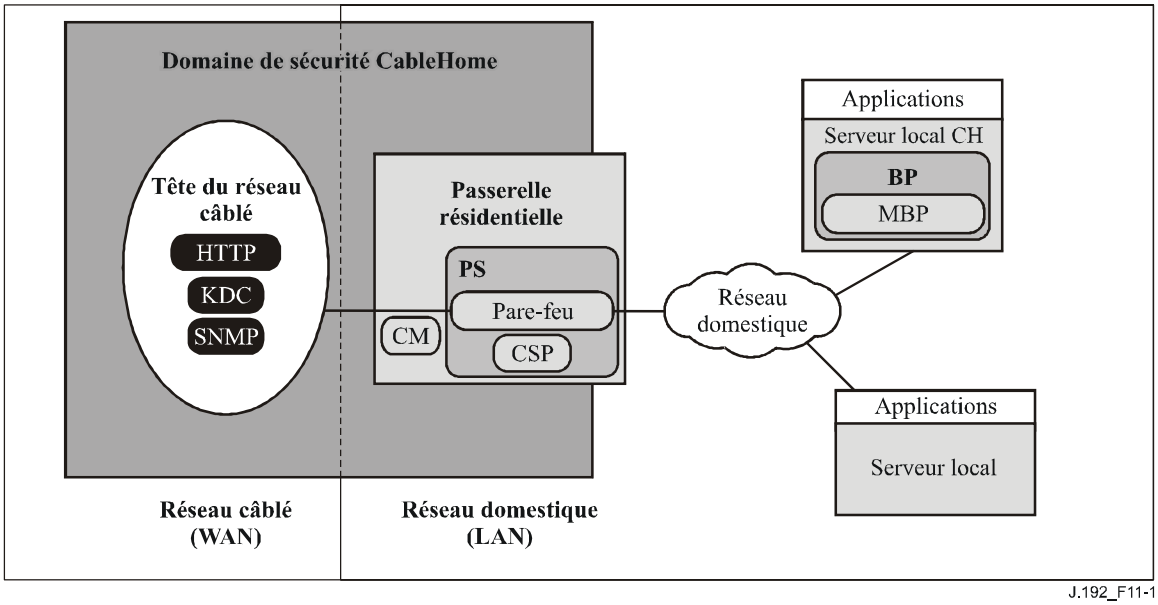


Figure 11-1/J.192 – Eléments de sécurité IPCable2Home

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 PS 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 PS est entièrement dans le domaine de sécurité, à l'exception de la fonctionnalité de commutation USFS du côté LAN. 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 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 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 d'approvisionnement 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 PS 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

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 PS 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 PS fournit l'identité de l'élément de services PS 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 PS. 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 approvisionne l'élément de services PS en mode d'approvisionnement 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 l'approvisionnement, 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 51 de l'option 177, 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 PS est approvisionné 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 d'approvisionnement SNMP, l'élément de services PS, 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 [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 d'approvisionnement* 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 PS 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 PS, la fonctionnalité de client qui est spécifiée pour l'adaptateur MTA. L'élément de services PS 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 PS (certificat d'élément de services PS) et les implémentations des éléments de services PS DOIVENT inclure le certificat d'élément de services PS.

Les paragraphes ci-après [J.170], concernant la fonctionnalité Kerberos, ne s'appliquent pas au modèle IPCable2Home:

- § 6.4.8.4, Préauthentificateur pour la localisation du serveur d'approvisionnement;
- § 6.4.7, Noms des mandants d'adaptateur MTA;
- § 6.4.8, Mappage d'adresse MAC d'adaptateur MTA sur un nom FQDN d'adaptateur MTA;
- § 6.4.10, Suivi des versions des clés de service;
- § 6.4.11, Opération transectorielle Kerberos;
- § 6.5.4, Messages de renouvellement de clé;
- § 6.5.6, Protocole IPsec cerbérisé;
- § 6.4.6, Conventions relatives aux emplacements et aux noms des serveurs Kerberos.

11.3.4.1.2 Variables d'authentification propres au modèle IPCable2Home

Le modèle IPCablecom spécifie pour Kerberos certains noms de variable dans l'architecture de réseau IPCablecom. 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 § 6.4.6.2/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 d'approvisionnement ou gestionnaire SNMP). L'élément de services PS a fourni au centre KDC l'adresse IP du serveur d'approvisionnement, dans le message de demande AS, en tant qu'informations nécessaires afin d'établir le contact approprié entre le centre KDC et le serveur d'approvisionnement.

Le nom de mandant de l'élément de services PS DOIT être de type NT-SRV-INST avec exactement deux composants, où le premier composant DOIT être la chaîne "PSElement" (non compris les guillemets) et où le deuxième composant DOIT être l'adresse MAC du réseau WAN-Man, soit:

PSElement/<Adresse MAC du réseau WAN-Man>

où <Adresse MAC du réseau WAN-Man> est l'adresse MAC de gestion de réseau WAN de l'élément de services PS. Le format du champ <Adresse MAC du réseau WAN-Man> 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/<Adresse d'entité SNMP>

où l'expression <Adresse d'entité SNMP> DOIT être l'adresse IP d'entité SNMP du fournisseur de services (sous-option 3 de l'option DHCP 177 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 spécification 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 [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) [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 11-2 à 11-13 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.

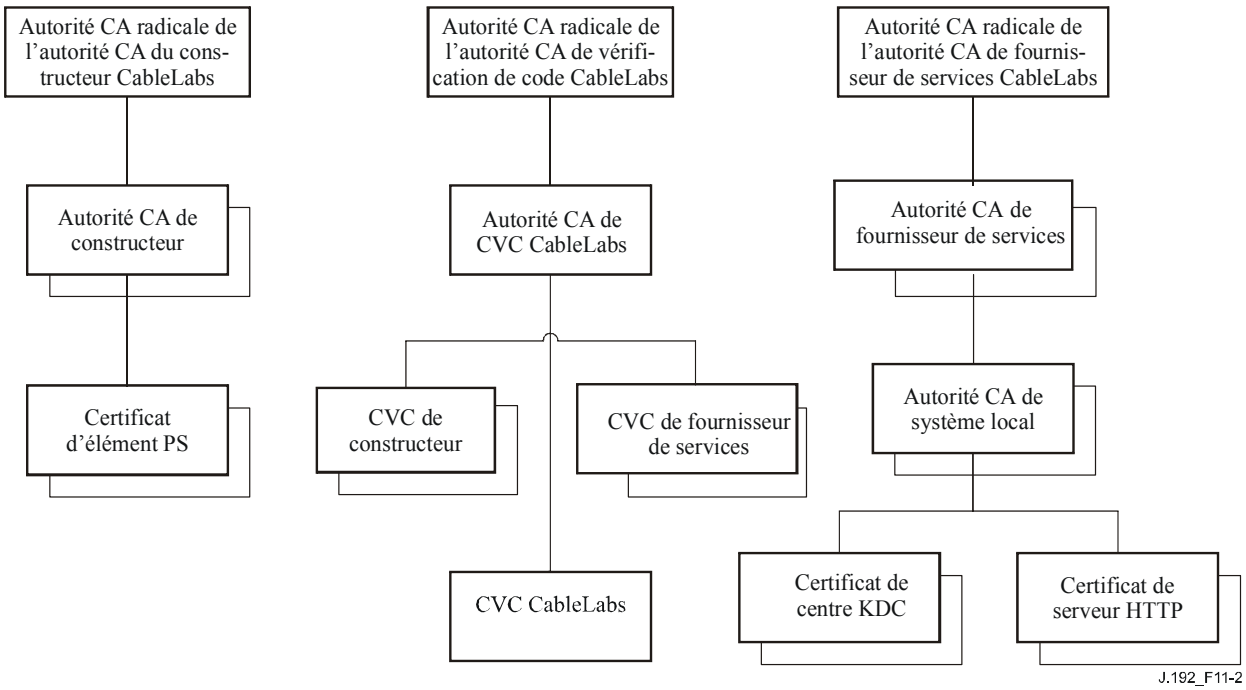


Figure 11-2/J.192 – Hiérarchie des certificats IPCable2Home

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 utilisent leur autorité CA afin d'envoyer des certificats individuels d'élément de services PS. 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 et 11-5. 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 PS.

Tableau 11-3/J.192 – Certificat d'autorité CA radicale de constructeur

Forme du nom du titulaire	C=<pays> O=<Nom de l'entreprise> CN=[Nom de l'entreprise] 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 ans au moins
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

Le certificat d'autorité CA de constructeur 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 PS.

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 PS 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 PS avec le nom du titulaire contenu dans le certificat d'autorité CA de constructeur. L'identificateur authorityKeyIdentifier du certificat d'élément de services PS DOIT être mis en correspondance avec l'identificateur subjectKeyIdentifier du certificat du constructeur comme décrit dans le document [RFC 3280].

Tableau 11-4/J.192 – Certificat d'autorité CA de constructeur

Forme du nom du titulaire	C=<pays> O=<Nom de l'entreprise> [ST=<état/région>] [L=<ville>] OU= <unité organisationnelle> [OU=<Usine du constructeur>] CN=<Nom de l'entreprise> 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 PS, 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 PS. Ce certificat produit des certificats d'élément de services PS. Ce certificat, de même que le certificat d'autorité CA radicale de constructeur et le certificat d'élément de services PS, sert à authentifier l'identité de l'élément de services PS. L'énumération facultative concernant l'usine du constructeur peut être le nom de l'usine et/ou son emplacement.

Tableau 11-4/J.192 – Certificat d'autorité CA de constructeur

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'élément de services PS

Le certificat d'élément de services PS 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 PS.

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 PS est installé en permanence, non renouvelable et non remplaçable. Donc, le certificat d'élément de services PS a une période de validité supérieure à la durée de vie opérationnelle attendue du dispositif spécifique.

Tableau 11-5/J.192 – Certificat d'élément de services PS

Forme du nom du titulaire	C=<pays> O=<Nom de l'entreprise> [ST=<état/région>] [L=<ville>] OU=<unité organisationnelle> [OU=<Nom de produit>] [OU=<Usine du constructeur>] CN=<Adresse MAC du réseau WAN-Man>
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 PS. Ce certificat sert à authentifier l'identité de l'élément de services PS.
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, dataEncipherment), anyExtendedKeyUsage[n,m] (id-kp-clientAuth), 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.

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 11-6, 11-7, 11-8, 11-9 et 11-10. 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.

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 11-6/J.192 – Certificat d'autorité CA radicale de vérification de code

Forme du nom du titulaire	C=<pays> O=<Nom de l'entreprise> CN= [Nom de l'entreprise] 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 ans au moins
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 11-7/J.192 – Certificat d'autorité CA de vérification de code

Forme du nom du titulaire	C=<pays> O=<Nom de l'entreprise> CN= [Nom de l'entreprise] 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 11-8/J.192 – Certificat de vérification de code de constructeur

Forme du nom du titulaire	C=<pays> O=<Nom de l'entreprise> [ST=<état/région>] [L=<ville>] CN=<Nom de l'entreprise> 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 11-9/J.192 – Certificat de vérification de code

Forme du nom du titulaire	C=<pays> O=<Nom de l'entreprise> CN=<Nom de l'entreprise>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 11-10/J.192 – Certificat de vérification de code du fournisseur de services

Forme du nom du titulaire	C=<pays> O=<Nom de l'entreprise> [ST=<état/région>] [L=<ville>] CN=<Nom de l'entreprise> 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 document [RFC 3280]. Ces valeurs spécifiques pour la hiérarchie des certificats de fournisseur de services DOIVENT être suivies selon les Tableaux 11-11 à 11-14. Si un champ requis n'est pas plus précisément énuméré dans les tableaux, les directives figurant dans le document [RFC 3280] DOIVENT être suivies. Les extensions génériques du modèle IPCable2Home DOIVENT également être incluses comme spécifié dans le § 11.3.4.2.

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 11-11/J.192 – Certificat d'autorité CA radicale de fournisseur de services

Forme du nom du titulaire	C=<pays> O=<Nom de l'entreprise> CN=<Nom de l'entreprise> 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 ans au moins
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 11-12/J.192 – Certificat d'autorité CA de fournisseur de services

Forme du nom du titulaire	C=<pays> O=<Nom de l'entreprise> CN=<Nom de l'entreprise> 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 PS 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.
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 11-13/J.192 – Certificat d'autorité CA de système local

Forme du nom du titulaire	C=<pays> O=<Nom de l'entreprise> OU=<Nom du système local> CN=<Nom de l'entreprise> Autorité CA de système local

Tableau 11-13/J.192 – Certificat d'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 § 8.2.4.1/J.170, "Certificat de centre de distribution de clés".

Tableau 11-14/J.192 – Certificat de centre KDC

Forme du nom du titulaire	C=<pays> O=<nom de l'entreprise> [OU=<Nom du système local>] OU=<Nom de l'entreprise> 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 PS 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= <valeur subjectKeyIdentifier extraite du certificat d'autorité CA>) 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 11-15/J.192 – Certificat de serveur HTTPS

Forme du nom du titulaire	C=<pays> O=<Nom de l'entreprise> [OU=<Nom du système local>] OU=<Nom de l'entreprise> 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 l'approvisionnement. Ce certificat est transmis à l'élément de services PS 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), anyExtendedKeyUsage[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 PS 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 [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 DOIT valider 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 le téléchargement sécurisé de logiciel au § 11.8.

11.3.4.2.3.3 Validation de la chaîne de fournisseur de services et vérification de la racine

L'élément de services PS 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 PS 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 d'approvisionnement de l'élément de services PS (voir § 5.5). Dans le modèle IPCable2Home, il y a trois modes d'approvisionnement: le mode d'approvisionnement DHCP, le mode d'approvisionnement SNMP et le mode inactif. Le mode d'approvisionnement 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 d'approvisionnement 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 d'approvisionnement de l'élément de services PS, 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 Objectifs de la messagerie de gestion sécurisée

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 2576] 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 d'approvisionnement DHCP

En mode d'approvisionnement DHCP, l'élément de services PS peut être configuré en mode d'accès NmAccess ou en mode de coexistence. En mode de coexistence, l'élément de services PS 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 PS est en mode d'approvisionnement DHCP et en mode d'accès NmAccess, la gestion de réseau par protocole SNMP dans l'élément de services PS 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 PS est en mode d'approvisionnement 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 PS 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 d'approvisionnement 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 2003] (remplacer les termes "CM" par "élément de services PS" 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 d'approvisionnement DHCP, l'élément de services PS DOIT également être capable de recevoir des éléments TLV de types 34, 34.1 et 34.2, comme défini dans la section 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 CHAdministrator fait appel à l'équation de Diffie-Helman afin de convertir Rm en un 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 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 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).

$$C = g \wedge xa \text{ MOD } p$$

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 implémentée 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 d'approvisionnement SNMP

Si l'élément de services PS est en mode d'approvisionnement SNMP, la gestion de réseau par protocole SNMP dans l'élément de services PS 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 d'approvisionnement 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 Kerberos approprié qui est indiqué dans le ticket [J.170], ce qui suit définit la règle à utiliser afin de produire l'automate SNMPv3:

- l'identificateur d'automate SNMPv3 suit 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];
- le cinquième octet contient la valeur 4 (quatre) afin d'indiquer que les octets suivants, jusqu'à 27, sont à considérer comme du texte. Jusqu'au 27^{e}, ces octets sont définis comme suit:
  - les 25 premiers caractères du nom de mandant Kerberos sont utilisés pour les octets d'identificateur d'automate à partir du 6^{e} octet;
- la séquence d'octets ci-dessus, indiquant le nom de mandant Kerberos, est suivie par un octet à considérer comme une valeur hexadécimale de 8 bits. Chaque valeur différente 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 se termine par un caractère vide.

Noter que 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 PS. D'autres utilisateurs peuvent également être définis. Dans le présent paragraphe, un utilisateur du modèle USM est défini précisément pour le processus d'approvisionnement. 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 d'approvisionnement (voir le Tableau 13-1, "Description des flux pour le processus d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement DHCP", étape CHPSWMD-11; le Tableau 13-2, "Description des flux pour le processus d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement SNMP",

étapes CHPSWMS-11 et CHPSWMS-13; et le § 13.4.3, "Messages INFORM d'enrôlement d'approvisionnement/d'approvisionnement terminé)".

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 PS 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 du dispositif de réseau WAN-Man
- usmUserSecurityName: CHAdministratorxx:xx:xx:xx:xx:xx, où xx:xx:xx:xx:xx:xx est l'adresse matérielle du dispositif de réseau WAN-Man
- 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 le document [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 LAN à réseau LAN. 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 QS des liaisons de réseau LAN à réseau LAN 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 PS sécurise les messages CqoS issus du côté WAN, 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 LAN 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 LAN de ce réseau contre le trafic indésirable de réseau WAN à réseau LAN.
- Protéger l'hybride HFC contre le trafic indésirable de réseau LAN à réseau WAN.
- 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 LAN conformément à la politique actuelle sans tenir compte du mode d'adressage: par conversion CAT ou par traversée (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 d'approvisionnement terminé, sans tenir compte du mode d'approvisionnement.

- 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 de politique commandent les actions de journalisation effectuées par le filtre de paquets du 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 11-16 ont guidé les spécifications de pare-feu IPCable2Home.

Tableau 11-16/J.192 – Sécurité IPCable2Home: directives de conception du système

Référence	Directives
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 points d'accès, 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 LAN et WAN 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 portail – Configuration globale des services 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), filtrage de paquets d'après l'état (SPF), passerelle de couche Application (ALG, *application level gateway*) et serveur applicatif mandataire (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 point d'accès 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 point d'accès 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 mandataire propre à l'application (ASP), qui est un autre pare-feu typique, peut, sur la base du protocole de couche Application, filtrer 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 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 implémenté 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 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.

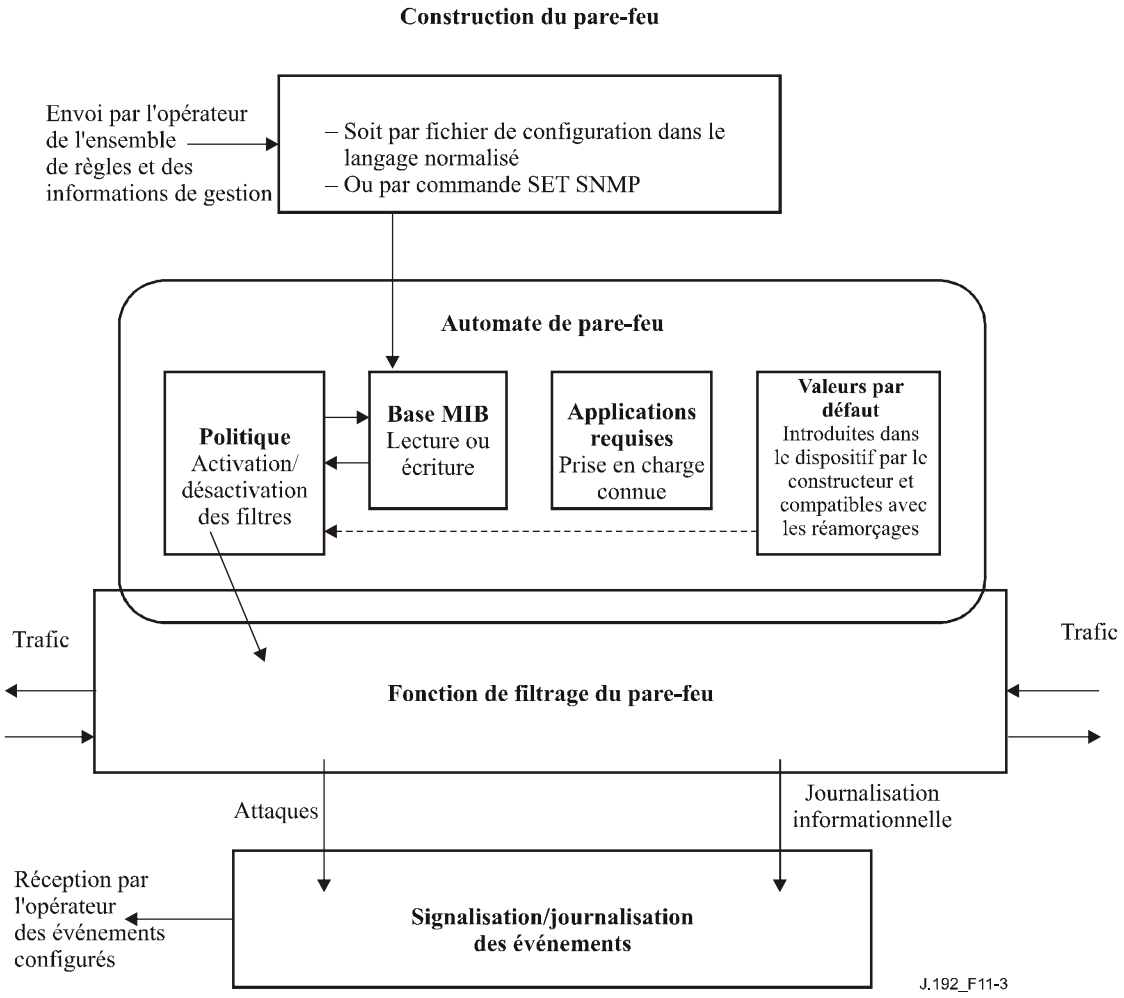


Figure 11-3/J.192 – Référence logique de pare-feu

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 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 PS ou le fichier de configuration du pare-feu. Non seulement le langage et le format du fichier de configuration contenant l'ensemble de règles applicable à un produit particulier de pare-feu sont définis, mais la façon dont ce fichier sera utilisé dans le pare-feu afin de configurer les composants SPF et ASP sera propre à l'implémentation.

Le dispositif PS DOIT être capable de recevoir et d'interpréter un fichier de configuration du pare-feu construit au moyen d'éléments TLV en notation ASN.1 avec codage en règles BER [ISO/CEI 8825-1]. 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 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 permet, mais n'exige pas la gestion à distance des fonctions de pare-feu par le câblo-opérateur. Le pare-feu DOIT accepter les ensembles de règles configurés en bloc, au moyen des fichiers spécifiés de configuration du PS ou du pare-feu. Quand un fichier de configuration contient des règles de filtrage de pare-feu, ces règles peuvent être traitées soit comme un ensemble de règles différentielles soit comme un ensemble complet de règles configurées, selon ce qui est établi par l'objet cabhSec2FwClearPreviousRuleset. Après téléchargement du fichier de configuration et achèvement du traitement, les règles de pare-feu extraites du fichier de configuration DOIVENT être immédiatement appliquées et disponibles pour utilisation dès que l'objet cabhPsDevProvState de base MIB a une valeur égale à pass(1), sans réamorçage du dispositif PS. Si l'objet cabhSec2FwPolicySelection est réglé à la valeur configuredRuleset, les nouvelles règles DOIVENT être immédiatement appliquées lors du traitement. Quand le dispositif PS traite un fichier de configuration avec des ensembles de règles de pare-feu, le dispositif PS NE DOIT PAS perdre les règles différentielles émises par demande SET (mise à jour) du protocole SNMP, ni les règles émises par de précédents fichiers de configuration, à moins que l'objet cabhSec2FwClearPreviousRuleset ne soit réglé à la valeur complete(2) ou incrementDefault(3). Concernant les règles établies par protocole SNMP, la règle ou la valeur d'objet de base MIB DOIT être activée (ou correctement disponible si l'activation n'est pas actuellement permise) immédiatement après traitement du message SET (mise à jour) du protocole SNMP sans réamorçage du dispositif PS. Par exemple, si un des filtres du pare-feu est mis à jour par commande SET du protocole SNMP, mais que l'objet cabhSec2FwPolicySelection soit actuellement réglé à la valeur factoryDefault, le dispositif PS mettra alors à jour l'ensemble de règles configurées avec la règle modifiée, mais fera actuellement fonctionner le dispositif PS au moyen de la politique par défaut à la construction jusqu'à ce que le câblo-opérateur modifie l'objet pour le mettre à la valeur configuredRuleset, qui comprendra donc la règle nouvellement configurée.

Le pare-feu DOIT vérifier et appliquer les règles configurées dans la table docsDevFilterIpTable comme décrit dans le document [RFC 2669], sauf indication contraire dans la présente Recommandation.

Si le dispositif PS ne peut pas traiter le fichier de configuration pour une raison ou une autre, le dispositif PS DOIT envoyer l'événement approprié d'échec de traitement et le pare-feu DOIT utiliser l'ensemble de règles choisi par l'objet cabhSec2FwPolicySelection et activé par l'objet cabhSec2FwEnable.

11.6.4.3 Politique de pare-feu

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 LAN. 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. S'il y a un conflit de règles dans la politique, le pare-feu DOIT résoudre ce conflit comme décrit pour les valeurs de l'objet docsDevFilterIpTable dans le document [RFC 2669], sauf indication contraire dans la présente Recommandation.

Le pare-feu est conçu afin de protéger le système informatique domestique à l'encontre d'attaques et de trafic indésirable. Le trafic est classé dans les catégories suivantes: trafic de réseau WAN, trafic de réseau LAN et trafic provenant du dispositif PS. Par défaut, s'il n'y a aucune règle pour le trafic lancé par des adresses IP de réseau autre que LAN (les adresses IP de réseau LAN sont définies comme des adresses de secteur LAN-Trans ou LAN-Pass), le pare-feu DOIT refuser ce trafic. Par défaut, s'il n'y a aucune règle configurée pour le trafic lancé à partir d'une adresse IP de réseau LAN à destination d'une adresse IP de réseau WAN, le pare-feu DOIT permettre ce trafic. Tous les

paquets non explicitement autorisés par une règle configurée DOIVENT être vérifiés afin de savoir s'ils DOIVENT être autorisés en raison de leur état.

On spécifie une façon normalisée de communiquer des politiques au pare-feu, une politique par défaut et la prise en charge du modèle IPCablecom. La politique par défaut sert de réglages par défaut normalisés à la construction; l'opérateur peut choisir de réinitialiser le bloc en fonction de ces réglages à tout moment. La politique par défaut à la construction permet la gestion du dispositif PS et active le dispositif PS pour l'essentiel du trafic lancé du réseau LAN au réseau WAN. Les câblo-opérateurs peuvent créer toute configuration requise afin de prendre en charge toute application sous pare-feu pour chaque client. La politique peut être réglée par le fichier de configuration du PS, par le fichier de configuration du pare-feu, ou par des messages SET (mise à jour) du protocole SNMP.

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 § 11.6.4.3.3, comporte la politique IPCable2Home par défaut à la construction plus les protocoles requis afin d'activer la messagerie IPCablecom à travers le pare-feu. L'Annexe D indique également quels points d'accès doivent être ouverts pour l'adaptateur MTA. La prise en charge du modèle IPCablecom permet l'approvisionnement, la gestion et les services à travers le pare-feu.

La politique par défaut à la construction, comme définie dans le Tableau 11-17, est tenue d'être installée au moment de la construction et d'être toujours disponible afin de réinitialiser le bloc à un niveau de filtrage de base. Tous les ensembles de règles configurées sont approvisionnés par le câblo-opérateur. La politique par défaut à la construction n'est pas étiquetée comme un "ensemble de règles" car elle n'est pas spécifiée dans le langage et dans le format requis du fichier de configuration. Au contraire, les exigences sont énumérées pour la politique par défaut et l'implémentation est propre au vendeur car elle est réalisée au moment de la construction.

Le modèle IPCable2Home spécifie actuellement une politique de pare-feu par défaut à la construction, intégrée dans le dispositif PS au moment de la fabrication, ainsi qu'une méthode permettant au câblo-opérateur de configurer les ensembles de règles dans le dispositif PS selon les besoins. Le présent paragraphe décrit le concept général de politique de pare-feu dans la mesure où il se rapporte aux secteurs d'adresses, à la politique par défaut à la construction, aux informations relatives à l'ensemble de règles IPCablecom et à l'ensemble de règles configurées par le câblo-opérateur.

11.6.4.3.1 Politique de pare-feu et secteurs d'adresses

La politique fondée sur les filtres du pare-feu utilise une configuration spécifique d'un ensemble de règles. S'il n'y a aucune configuration du pare-feu par un câblo-opérateur, le pare-feu est réglé à la politique par défaut à la construction. La politique comprend des règles de filtrage pour les adresses IP d'origine et de destination. Le concept de sens de transmission est déduit des termes *origine* et *destination* et n'est donc pas spécifié.

Le concept de secteurs d'adressage IP est défini dans la présente Recommandation pour les adresses IP de réseau WAN et de réseau LAN. Le dispositif PS est dans le réseau LAN, mais les paquets en provenance ou à destination du dispositif PS ne sont pas désignés par le terme de *trafic de réseau LAN* aux fins du filtrage par pare-feu. En revanche, c'est l'adresse IP spécifique du dispositif PS qui est appelée. 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 la politique par défaut à la construction. Les adresses IP de réseau LAN ne sont pas distinguées selon les modes d'adressage car le pare-feu ne filtre pas sur la base des modes d'adressage IP du modèle IPCable2Home. L'adresse IP d'interface PS/WAN-Data DOIT être

considérée comme faisant partie du secteur d'adresses IP de réseau LAN car l'adresse IP de réseau WAN-Data ne représente que les paquets dont les adresses IP ont été converties par la fonction CAT (par exemple des adresses IP dans le secteur LAN-Trans).

11.6.4.3.2 Politique par défaut à la construction

La politique par défaut à la construction offre la fonctionnalité normale du dispositif PS ainsi que l'essentiel du trafic lancé à partir de serveurs locaux. La politique par défaut à la construction DOIT être codée physiquement dans le dispositif PS au moment de la construction. Le dispositif PS DOIT toujours utiliser la politique par défaut à la construction quand l'objet cabhSec2FwPolicySelection est réglé à factoryDefault(1).

La politique par défaut à la construction DOIT prendre en charge les protocoles requis par IPCable2Home à l'exception du protocole ToD, qui n'est pas spécifié au-delà du processus d'approvisionnement et qui n'est donc pas inclus dans la politique par défaut à la construction, car le pare-feu ne devient pas actif avant que l'état d'approvisionnement ait été transmis. Si l'objet cabhSec2FwPolicySelection est réglé à factoryDefault pendant le processus d'approvisionnement (par exemple réamorçage), le dispositif PS DOIT activer la politique par défaut à la construction immédiatement après que l'objet cabhPsDevProvState de base MIB a pris une valeur égale à pass(1), sans réamorçage du dispositif PS. Si l'objet cabhSec2FwPolicySelection est réglé à factoryDefault par protocole SNMP, le dispositif PS DOIT activer la politique par défaut à la construction immédiatement, sans réamorçage du dispositif PS. La politique par défaut à la construction NE DOIT PAS inclure de restrictions sur l'heure actuelle ni de limites sur le nombre de sessions ou de connexions à prendre en charge simultanément, sauf spécification contraire dans l'Annexe D, "Applications par conversion CAT et pare-feu".

Le Tableau 11-17 spécifie la politique par défaut à la construction. Les deux secteurs d'adresses de réseau LAN, LAN-Trans et LAN-Pass, sont traités identiquement pour la politique par défaut à la construction et sont étiquetés comme adresses IP de réseau LAN. Le pare-feu DOIT être capable de rechercher des adresses dans la table de mappage CAT afin d'appliquer une politique sur la base de l'adresse IP réelle du dispositif de serveur local. Les adresses du dispositif PS NE DOIVENT PAS inclure d'adresses IP d'interface PS/WAN-Data. Les adresses IP d'interface PS/WAN-Data appartiennent au trafic IP de réseau LAN et, comme telles, sont traitées en tant qu'adresses IP de réseau LAN. Le tableau fonde ses informations sur l'ouverture de session et non sur le trafic autorisé. Donc, la politique de pare-feu par défaut à la construction DOIT être implémentée pour l'ouverture de session et non pour le trafic autorisé. Le trafic revenant sur requête du demandeur est interprété comme contenant des informations d'état pour une session. Le pare-feu vérifiera l'état de la session après la vérification des politiques afin de garantir qu'un paquet n'est pas refusé alors qu'il fait partie d'une session en cours. Le Tableau 11-17 DOIT être implémenté en tant que politique de pare-feu par défaut à la construction.

Tableau 11-17/J.192 – Politique de pare-feu IPCable2Home par défaut à la construction

En-têtes de colonne identifiant l'ouverture de session	Origine: adresse IP de réseau WAN Dest: adresse IP de l'interface PS/WAN-Man	Origine: adresse IP de réseau WAN Dest: adresse IP de réseau LAN	Origine: adresse IP de l'interface PS/WAN-Man Dest: adresse IP de réseau WAN	Origine: adresse IP de l'interface PS/WAN-Man Dest: adresse IP de réseau LAN	Origine: adresse IP de réseau LAN Dest: adresse IP du routeur-serveur PS	Origine: adresse IP de réseau LAN Dest: PS 192.168.0.1	Origine: adresse IP de réseau LAN Dest: adresse IP de l'interface PS/WAN-Man	Origine: adresse IP de réseau LAN Dest: adresse IP de réseau WAN	Scénarios relationnels requis
AOL IM	Refuser	Autoriser	Refuser	Refuser	Refuser	Refuser	Refuser	Autoriser	Tous
DHCP	Refuser	Refuser	Autoriser	Refuser	Autoriser	Autoriser	Refuser	Autoriser	Tous
DNS	Refuser	Refuser	Autoriser	Refuser	Autoriser	Autoriser	Refuser	Autoriser	Tous
FTP	Refuser	Refuser	Refuser	Refuser	Refuser	Refuser	Refuser	Autoriser	Tous
HTTP	Refuser	Refuser	Refuser	Refuser	Autoriser	Autoriser	Refuser	Autoriser	Tous
HTTPS (soit HTTP sur TLS)	Refuser	Refuser	Autoriser	Refuser	Autoriser	Autoriser	Refuser	Autoriser	Tous
ICMP: demandes d'écho et marqueur temporel (sondage par écho et suivi de chemine-ment)	Autoriser	Autoriser	Refuser	Autoriser	Autoriser	Autoriser	Refuser	Autoriser	Tous
IPSec	Refuser	Refuser	Refuser	Refuser	Refuser	Refuser	Refuser	Autoriser	Point à point, unique
Kerberos	Refuser	Refuser	Autoriser	Refuser	Refuser	Refuser	Refuser	Refuser	Tous
Messagerie Microsoft	Refuser	Autoriser	Refuser	Refuser	Refuser	Refuser	Refuser	Autoriser	Tous
Messagerie MSN	Refuser	Autoriser	Refuser	Refuser	Refuser	Refuser	Refuser	Autoriser	Tous
POP3	Refuser	Refuser	Refuser	Refuser	Refuser	Refuser	Refuser	Autoriser	Tous
SMTP	Refuser	Refuser	Refuser	Refuser	Refuser	Refuser	Refuser	Autoriser	Tous
SNMP	Autoriser	Refuser	Autoriser	Refuser	Autoriser	Autoriser	Refuser	Refuser	Tous
Message TRAP du SNMP	Refuser	Refuser	Autoriser	Refuser	Autoriser	Autoriser	Refuser	Refuser	Tous
Syslog	Refuser	Refuser	Autoriser	Refuser	Refuser	Refuser	Refuser	Refuser	Tous
Telnet	Refuser	Refuser	Refuser	Refuser	Autoriser	Autoriser	Refuser	Autoriser	Tous
TFTP	Refuser	Refuser	Autoriser	Refuser	Refuser	Refuser	Refuser	Autoriser	Tous
Messagerie Yahoo	Refuser	Autoriser	Refuser	Refuser	Refuser	Refuser	Refuser	Autoriser	Tous
Messagerie Windows	Refuser	Autoriser	Refuser	Refuser	Refuser	Refuser	Refuser	Autoriser	Point à point; point à multipoint

11.6.4.3.3 Ensemble de règles IPCablecom

Si le câblo-opérateur déploie 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 11-18 est une liste de spécifications qui exigent un point d'accès unique concernant la communication avec l'adaptateur MTA. Cependant, il ne s'agit pas d'une liste détaillée de toutes les spécifications IPCablecom.

Tableau 11-18/J.192 – Spécifications IPCablecom 1.x applicables au pare-feu IPCable2Home

Description	Spécification
Spécification des codecs audio/vidéo	[J.161]
Spécification de la qualité de service dynamique	[J.163]
Spécification du protocole de signalisation d'appel fourni par le réseau	[J.162]
Spécification de l'approvisionnement d'adaptateur MTA	[J.167]
Spécification de sécurité	[J.170]
Spécification du mécanisme d'événement de gestion	[J.164]
Spécification du protocole de serveur audio	[J.175]
Spécification de la signalisation du serveur (distant) de gestion d'appel	[J.178]

La liste des protocoles IPCablecom requis par l'adaptateur MTA a été extraite des spécifications indiquées. Les numéros de point d'accès attribués par l'autorité IANA afin d'ouvrir les points d'accès 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:

- approvisionnement: SNMPv3, DHCP, DNS, TFTP, SYSLOG
- flux média: RTP, RTCP
- qualité de service: RSVP
- sécurité: Kerberos, IPSec
- signalisation d'appel réseau: MGCP, SDP

  (NOTE – SDP n'exige aucun point d'accès spécifique.)

11.6.4.3.4 Ensemble de règles configurées et version actuelle

Le câblo-opérateur peut envoyer au dispositif PS tout ensemble de règles de pare-feu requis, au moyen d'un fichier de configuration ou d'une demande SET (mise à jour) du protocole SNMP. Quand un câblo-opérateur envoie des règles au dispositif PS, cela constitue l'ensemble de règles configurées ou la version actuelle. L'ensemble de règles configurées DOIT être conservé en mémoire non volatile (par exemple persistant après un réamorçage). Cette exigence garantit que le dispositif PS peut réactiver cet ensemble de règles si le pare-feu est activé et si la politique sélection est réglée à configuredRuleset. Les filtres de pare-feu définis sont réglés par l'ensemble de règles configurées. La plupart des objets de base MIB de filtrage par pare-feu sont spécifiés dans le document [RFC 2669], avec adjonction d'une table de planification supplémentaire dans la base MIB de sécurité. Les objets de base MIB sont regroupés dans une table de filtrage qui est l'ensemble des règles configurées.

Le traitement et l'application par le dispositif PS d'un ensemble de règles configurées émis par le câblo-opérateur dépendent du contenu du fichier de configuration et de la valeur de l'objet cabhSec2FwClearPreviousRuleset. L'ensemble de règles configurées peut être une augmentation de l'ensemble de règles configurées existant ou un remplacement complet. Une augmentation de la politique par défaut à la construction est également possible. Si le câblo-opérateur augmente les ensembles de règles de pare-feu en fonction de la politique par défaut à la construction, le dispositif PS DOIT remplir la table de filtrage avec les règles par défaut à la construction avant de remplir la table avec les règles configurées par le câblo-opérateur. Ce procédé offre une visibilité au câblo-opérateur, qui est ainsi capable de voir toutes les règles de filtrage. Les détails fonctionnels et les exigences relatives à cette caractéristique sont déclarés dans l'objet cabhSec2FwClearPreviousRuleset de base MIB, décrit dans le § 11.6.4.7.1.

11.6.4.4 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.

11.6.4.4.1 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 points d'accès, 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 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 point d'accès de l'application et ses limitations de trafic.

L'architecture du filtre de paquets dans le pare-feu spécifie des sens distincts pour le filtrage de paquets et pour le trafic du dispositif PS: le sens entrant (de réseau WAN à réseau LAN) et le sens sortant (de réseau LAN à réseau WAN). Le filtre des paquets entrants examine les paquets qui entrent dans l'interface PS/WAN. Le filtre des paquets sortants examine les paquets qui entrent dans l'interface PS/LAN. Des règles distinctes peuvent être appliquées aux filtres de paquets entrants et de paquets sortants. Les paquets destinés au dispositif PS à partir du réseau WAN ou LAN sont filtrés dans le pare-feu avant d'être réexpédiés vers l'un quelconque des composants du dispositif PS autres que le pare-feu (portails CAP, CDP, CNP, CSP, CQP et CPM).

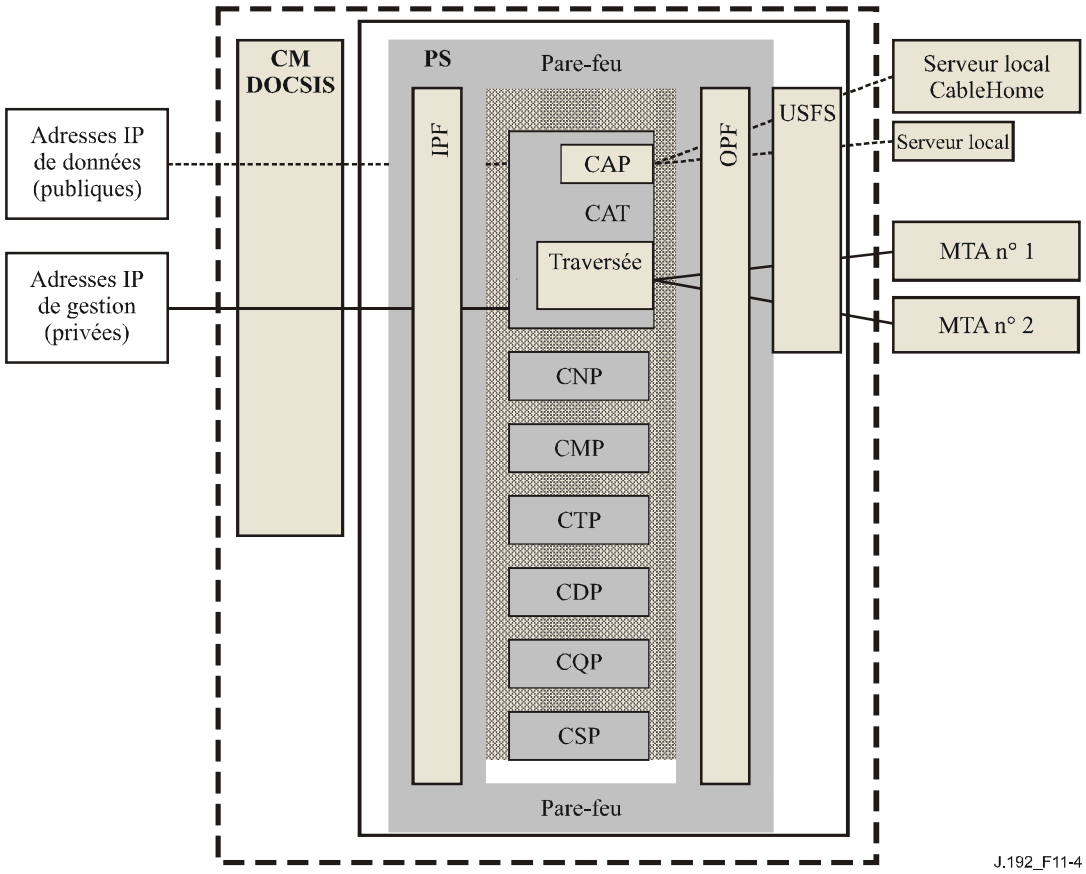


Figure 11-4/J.192 – Fonctionnalité de pare-feu à l'intérieur du dispositif PS

Les définitions de filtrage suivantes sont utilisées:

- AUTORISER signifie "laisser passer le paquet";
- REFUSER signifie "abandonner le paquet";
- les paquets de conversion NAT/NAPT (CH CAT) seront convertis à partir du réseau LAN, alors que les paquets revenant du réseau WAN vers le réseau LAN seront reconnus comme tels et subiront une conversion NAT/NAPT inverse. Les filtres du pare-feu seront appliqués en conjonction avec l'adresse correcte d'origine ou de destination dans le réseau LAN.

Les filtres de paquets entrants et de paquets sortants du pare-feu DOIVENT manifester le comportement suivant:

- le pare-feu DOIT refuser le trafic lancé avec une adresse IP extérieure au réseau LAN, à moins qu'il n'y ait une règle visant explicitement à permettre ce trafic. Des adresses IP autres que du réseau LAN sont des adresses qui ne sont pas dans la liste d'adresses du secteur LAN-Trans ou dans la liste d'adresses du secteur LAN-Pass;
- le pare-feu DOIT permettre tout le trafic lancé par des adresses IP de réseau LAN (sauf l'adresse IP d'interface PS/WAN-Man ou du routeur-serveur PS), à moins qu'il n'y ait une règle visant à refuser explicitement ce trafic;
- le pare-feu DOIT refuser les paquets réexécutés à partir du réseau LAN 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 dispositif PS NE DEVRAIT PAS permettre le trafic TCP sortant avant d'avoir établi une session en protocole TCP (c'est-à-dire avant d'avoir effectué un dialogue TCP à 3 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 points d'accès ou du réseau lancée à partir d'un réseau LAN 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 LAN, comme les messages BP_Init ou DISCOVER du protocole DHCP.

11.6.4.4.2 Critères de filtrage

Le comportement par défaut est de refuser le trafic lancé à partir d'adresses IP de réseau WAN, de l'adresse IP de l'interface PS/WAN-Man, ou de l'adresse IP de l'interface PS/routeur-serveur. Donc, les ensembles de règles et la politique par défaut sont 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 LAN 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;
- points d'accès 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.

11.6.4.4.3 Architecture de filtrage

Le filtre de paquets du pare-feu DOIT être capable de filtrer le trafic lorsque celui-ci entre dans le dispositif PS, à l'exception de l'utilisation de la fonction de commutation USFS à partir du réseau

LAN; et DOIT être capable d'offrir des filtres distincts de paquets entrants (de réseau WAN à réseau LAN), de paquets sortants (de réseau LAN à réseau WAN) et de paquets du dispositif PS. Ce pare-feu DOIT avoir les attributs suivants:

- filtrer les paquets reçus de l'interface PS/WAN, par exemple IfIndex = 1, (ce qui est désigné par le terme de *filtrage entrant*);
- paquets reçus de l'interface PS/LAN, par exemple IfIndex = 255, (ce qui est désigné par le terme de *filtrage sortant*);
- filtre les paquets provenant de l'intérieur du dispositif PS et allant vers le réseau LAN ou WAN;
- appliquer que des filtres déjà activés;
- le filtrage de paquets entrants et sortants précède la livraison des paquets à l'un quelconque des composants du dispositif PS extérieurs au pare-feu, à l'exception de la commutation USFS pour paquets provenant du réseau LAN;
- le filtrage de paquet sortant précède tout traitement par élément ASP/SPF.

Le filtre de paquets entrants du réseau WAN DOIT manifester le comportement suivant:

- refuser par défaut; c'est-à-dire que le comportement par défaut du pare-feu sur les paquets entrants, qui n'ont pas de règles de filtrage explicites afin de les autoriser, est de les abandonner;
- refuser tous les paquets dont l'adresse d'origine est dans les secteurs d'adresses LAN-Pass ou LAN-Trans et qui sont reçus de l'interface PS/WAN, par exemple IfIndex = 1;
- refuser tous les paquets avec adresse d'origine diffusée ou multidiffusée.

Le filtre de paquets sortants du réseau LAN DOIT manifester le comportement suivant:

- autoriser par défaut; c'est-à-dire que le comportement par défaut du pare-feu sur les paquets sortants, qui n'ont pas de règles de filtrage explicites afin de les refuser, est de les autoriser;
- ignorer tous les paquets avec adresse d'origine diffusée ou multidiffusée.

11.6.4.5 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) 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 demande 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.

11.6.4.5.1 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 PS 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 dépassé, 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 dépassé, 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 dépassé, le dispositif PS DOIT immédiatement envoyer l'événement 80010204;

TYPE 5: le type 5 DOIT journaliser les paquets autorisés entrant à partir du réseau WAN 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 WAN. Si ce type est activé et si le seuil est dépassé, le dispositif PS DOIT immédiatement envoyer l'événement 80010205;

TYPE 6: le type 6 DOIT journaliser les paquets autorisés sortant du réseau LAN 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 LAN domestique en traversant le réseau WAN. Si ce type est activé et si le seuil est dépassé, 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.

11.6.4.5.2 Journaux de pare-feu

Les informations de journalisation du pare-feu DOIVENT être mémorisées dans le dispositif PS pour chaque type de journal activé, comme spécifié dans le § 11.6.4.5.1. Le dispositif PS DOIT journaliser les informations spécifiées à moins que l'objet cabhSec2FwEventThreshold ne soit réglé à zéro, ou que l'objet cabhSec2FwEventEnable ne soit réglé à la valeur "désactiver", ou que l'objet cabhSec2FwEventInterval ne soit réglé à zéro, ou que le journal ne soit plein. Si l'objet cabhSec2FwEventThreshold n'est pas réglé à zéro, que l'objet cabhSec2FwEventEnable soit activé, que l'objet cabhSec2FwEventInterval ne soit pas réglé à zéro et que le journal ne soit pas plein, 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 en mémoire volatile de 1 koctet de données par journal, ce qui permettra de journaliser environ 40 occurrences sans compression. 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.

11.6.4.5.2.1 Données de journalisation

La journalisation peut poser différents problèmes si elle n'est pas correctement effectuée. La journalisation de tous les événements et paquets peut rendre le journal complexe, volumineux et difficile à comprendre. Il est malaisé de trier un grand nombre d'informations afin de rechercher un seul élément en particulier. Si la journalisation est limitée à quelques types d'événements seulement, elle ne fournira pas assez d'informations au câblo-opérateur pour déboguer les intrusions ou détecter les attaques. Noter que les journaux peuvent être "reniflés" s'ils ne sont pas chiffrés. Un pirate peut utiliser des informations journalisées afin d'obtenir un aperçu des divers services fonctionnant dans le dispositif PS ou dans les dispositifs de serveur local de réseau LAN.

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 d'approvisionnement.

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;

- point d'accès d'origine (TCP et UDP);
- point d'accès 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.

La table cabhSec2FwLogTable pour le type d'événement 3 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 mémorisé 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;
- adresse IP d'origine;
- 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:

- 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;
- 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;
- adresse IP d'origine;
- objet de base MIB dont la modification a été tentée;
- déclaration d'échec – Les événements de type 4 DOIVENT indiquer l'échec et sa raison.

11.6.4.6 Applications passant par 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. Ces applications sont permises mais la plupart d'entre elles ne le sont pas par défaut. En revanche, ces applications peuvent être activées par le câblo-opérateur. 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 LAN et WAN, ainsi qu'à destination et en provenance du dispositif PS lui-même.

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 WAN ou LAN. La politique est appliquée aux adresses IP d'origine et de destination, aux points d'accès et à l'heure actuelle. L'Annexe D énumère les exigences et fournit de plus amples détails.

11.6.4.7 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).

11.6.4.7.1 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 PS ou par une demande 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 que l'étiquette est établie, si les règles configurées sont changées, cet objet peut ne pas refléter

précisément la version des règles configurées fonctionnant sur le bloc. 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 que les fichiers de configuration PS ou du pare-feu contiennent un ensemble complet de règles de pare-feu configurées, ou une augmentation de l'ensemble de règles déjà configurées, selon son existence dans le fichier de configuration. Si le dispositif PS reçoit un fichier de configuration avec réglages de pare-feu, qui comprend une valeur d'objet cabhSec2FwClearPreviousRuleset marquée comme étant "increment(1)", ou si le réglage de cet objet n'est pas inclus dans un fichier de configuration qui contient des réglages de filtre pour le pare-feu, le dispositif PS DOIT traiter les réglages de filtre de pare-feu contenus dans le fichier de configuration comme une augmentation de l'ensemble de règles configurées. Si le dispositif PS reçoit un fichier de configuration avec réglages de pare-feu qui comprend un objet cabhSec2FwClearPreviousRuleset dont la valeur est marquée comme étant "incrementDefault(3)", le dispositif PS DOIT supprimer toutes les règles déjà configurées de l'ensemble de règles configurées, y compris les règles éventuellement contenues dans la table de planification du filtrage et DOIT incrémenter les règles nouvellement importées par téléchargement afin de les placer au-dessus de (c'est-à-dire à la suite de) la politique par défaut à la construction. Si le dispositif PS reçoit un fichier de configuration avec réglages de pare-feu qui comprend un objet cabhSec2FwClearPreviousRuleset dont la valeur est marquée comme étant "complete(2)", le dispositif PS DOIT supprimer toutes les règles déjà configurées de l'ensemble de règles configurées, y compris les règles éventuellement contenues dans la table de planification du filtrage, avant d'appliquer les réglages de filtre de pare-feu contenus dans le fichier de configuration.

Si l'objet cabhSec2FwClearPreviousRuleset est réglé à la valeur "increment(1)" au moyen du protocole SNMP, le dispositif PS DOIT traiter tous les réglages de filtre de pare-feu suivants au moyen du protocole SNMP comme une augmentation de l'ensemble des règles configurées. Si l'objet cabhSec2FwClearPreviousRuleset est réglé à incrementDefault(3) au moyen du protocole SNMP, le dispositif PS DOIT supprimer toutes les règles déjà configurées de l'ensemble de règles configurées, y compris les règles éventuellement contenues dans la table de planification du filtrage et DOIT traiter tous les réglages suivants de filtre de pare-feu, au moyen du protocole SNMP, comme une augmentation afin de les placer au-dessus de la politique par défaut à la construction. Si l'objet cabhSec2FwClearPreviousRuleset est mis à la valeur complete(2) au moyen du protocole SNMP, le dispositif PS DOIT supprimer toutes les règles de l'ensemble de règles configurées, y compris les règles éventuellement contenues dans la table de planification du filtrage. Dans ce scénario, le dispositif PS fonctionnera sans aucune règle configurée, (par exemple il n'y aura aucune règle de filtrage définie, mais le pare-feu continuera à offrir l'ensemble minimal de capacités et l'architecture, comme défini dans les § 11.6.4.4.1 et § 11.6.4.4.3). Valeur par défaut de cet objet = increment(1).

cabhSec2FwPolicySelection – cet objet permet la sélection de la politique de filtrage selon la valeur par défaut à la construction ou l'ensemble de règles configurées:

- factoryDefault (1) – cette valeur indique que le pare-feu utilise actuellement les réglages par défaut à la construction. Si cet objet est réglé à factoryDefault (1), le pare-feu DOIT filtrer conformément à la politique spécifiée par défaut à la construction;
- configuredRuleset (2) – cette valeur indique que le pare-feu utilise actuellement les ensembles de règles configurés par le câblo-opérateur. Si cet objet est réglé à configuredRuleset (2), le pare-feu DOIT utiliser le dernier ensemble connu de règles configurées.

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 "Vrai".

cabhSec2FwEventLastSetToFactory – cet objet signale la dernière fois que la table d'événements a été réinitialisée.

11.6.4.7.2 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 § 11.6.4.5.1.

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 de la présente Recommandation concernant les données de journal. 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 dépassé. 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 "Vrai" 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.

11.6.4.7.3 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 de 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 le document [RFC 2669]. Donc, le modèle IPCable2Home a adopté certains des objets de filtrage déjà définis dans le document [RFC 2669] et a ajouté dans la base MIB de sécurité certains objets de base MIB spécifiques du pare-feu.

Dans le document [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 points d'accès d'origine et de destination. C'est le cœur de la politique implémentée. C'est dans cette table de base MIB que la politique est définie et construite. Chaque paquet, entrant ou sortant, doit être comparé à la politique activée.

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 conformément aux réglages de filtre contenus dans les entrées de l'objet docsDevFilterIPTable. Cette table permet 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 WAN 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. Le pare-feu NE DOIT PAS associer de restrictions temporelles à une quelconque politique de filtrage, à moins qu'il n'y ait une règle explicite visant à définir les restrictions temporelles et que celles-ci soient clairement associées à des adresses IP connues.

La combinaison de filtres définie dans le document [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 point d'accès d'origine, de point d'accès de destination, d'heure actuelle 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 l'objet docsDevFilterIpTable, alors le dispositif PS DOIT appliquer l'ensemble minimal de capacités et l'architecture de pare-feu, comme défini dans les § 11.6.4.4.1 et 11.6.4.4.3. Le fanion docsDevFilterIpDefault défini dans le document [RFC 2669] DOIT être ignoré.

Les objets de base MIB suivants DOIVENT être implémentés à partir du document [RFC 2669] afin de créer la table FilterIpTable pour les règles de filtrage du pare-feu. Sauf indication contraire dans ce paragraphe, la fonctionnalité est comme spécifié dans le document [RFC 2669]:

– docsDevFilterIpTable >>DocsDevFilterIpEntry

  - **docsDevFilterIpIndex**

    conformément au document [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**
  - pour filtrer le trafic entrant en provenance du réseau WAN, docsDevFilterIpIfIndex; DOIT être réglé à 1;
  - pour filtrer le trafic entrant en provenance du réseau LAN, docsDevFilterIpIfIndex; DOIT être réglé à 255.
- **docsDevFilterIpDirection**

  Cette variable n'a aucune valeur pour le pare-feu. Donc, il ne devrait pas importer de savoir quelle valeur est fixée dans cet objet. Cependant, étant donné que la variable docsDevFilterIpDirection DOIT être réglée à une valeur égale à 1, 2 ou 3, il convient de régler cet objet de base MIB à "both(3)", car le document [RFC 2669] ne possède pas de valeur autorisée afin d'ignorer cet objet.
- **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**
- **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 "Vrai" 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 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** – instant de début des restrictions de trafic comme défini dans l'ensemble de règles;
- **cabhSec2FwFilterScheduleEndTime –** instant de fin des restrictions de trafic comme défini dans l'ensemble de règles;
- **cabhSec2FwFilterScheduleDOW –** jour de la semaine pendant lequel les restrictions de trafic seront appliquées.

Les règles de l'objet cabhSec2FwFilterScheduleTable concernant les restrictions d'heure et de jour sont associées à des politiques configurées dans l'objet docsDevFilterIPTable. Un paquet traité avec un marqueur d'horodatage situé dans le jour et dans l'heure interdits, comme spécifié par cette table, DOIT être refusé.

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 de la présente Recommandation. 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 CM 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;
- **clabMfgCVCCert** – Certificat de vérification de code de constructeur servant à mémoriser le certificat CVC 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 186-2] 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

Tableau 11-19/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 PS.

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) 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 demande 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 PS 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 demande 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 PS.

  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 PS DOIT demander le fichier spécifié par TFTP auprès du serveur de logiciel;
- l'élément de services PS DOIT vérifier que l'image logicielle téléchargée lui est appropriée. Si l'image logicielle téléchargée est appropriée, l'élément de services PS 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 PS n'est pas en mesure d'achever le transfert de fichiers pour une raison ou une autre, l'élément de services PS 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 PS 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 PS DOIT authentifier l'image logicielle téléchargée;
- l'élément de services PS 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 PS DOIT être capable de traiter une signature numérique PKCS # 7 et un certificat [X.509] comme défini dans les § 11.8.4.1.1 et 11.3.4.1.1, respectivement;
- (facultatif): l'élément de services PS DEVRAIT être capable de mettre à jour le certificat d'autorité CA radicale de certificat CVC mémorisé dans le dispositif;
- (facultatif): l'élément de services PS DEVRAIT être capable de remplacer le ou les certificats d'autorité CA de constructeur mémorisés dans le dispositif;
- (facultatif): l'élément de services PS DEVRAIT être capable de mettre à jour le certificat d'autorité CA de certificat CVC mémorisé dans le dispositif;
- (facultatif): l'élément de services PS DEVRAIT être capable de mettre à jour le certificat d'autorité CA radicale de fournisseur de services, mémorisé dans le dispositif.

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 PS, 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 PS 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 PS, comme entités distinctes ou intégrées selon la définition donnée dans le paragraphe relatif à l'architecture de la présente Recommandation.

- Si l'élément de services PS 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 PS est composé d'entités distinctes et autonomes, le téléchargement de logiciel pour les éléments IPCable2Home DOIT être effectué par l'élément de services PS, comme décrit ci-dessous dans la présente Recommandation.

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 document [RFC 2315] qui a été définie dans un format spécifique à utiliser avec des éléments de services PS. Le fichier de code DOIT être conforme au document [RFC 2315] et DOIT être codé selon les règles DER. Le fichier de code DOIT correspondre à la structure représentée dans le Tableau 11-20.

Quand des certificats sont téléchargés dans le cadre du fichier de code, ces certificats PEUVENT être contenus dans les champs spécifiés dans le Tableau 11-20 et être séparés de l'image de code réelle contenue dans le champ CodeImage.

Tableau 11-20/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 [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 11-21. Tout en conservant la conformité au document [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 PS DEVRAIT ignorer la signature [RFC 2315] si les données signées [RFC 2315] ne correspondent pas à la structure codée en règles DER.

Tableau 11-21/J.192 – Données signées PKCS # 7

Champ PKCS # 7	Description
Signed Data {	
version	version = 1
DigestAlgorithmIdentifiers	SHA-1
ContentInfo	
ContentType	Données (l'élément SignedContent est concaténé jusqu'à la fin de la structure PKCS # 7)
certificates {	(Certificat de vérification de code (CVC) de CableLabs)
mfgCVC	(REQUIS pour tous les fichiers de code)
co-signerCVC	(FACULTATIF; requis pour cosignatures)
} *fin des certificats*	
SignerInfo{	
MfgSignerInfo {	(REQUIS pour tous les fichiers de code)
version	version = 1
issuerAndSerialNumber	
issuerName	
CountryName	Etats-Unis d'Amérique
organizationName	CableLabs
CommonName	Autorité CA radicale de certificat CVC de CableLabs
certificateSerialNumber	<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 comme défini dans [PKCS # 7])
digestEncryptionAlgorithm	Chiffrement RSA
EncryptedDigest	
} *fin mfg signataire info*	
CoSignerInfo {	(FACULTATIF; requis pour les cosignatures)
version	version = 1

Tableau 11-21/J.192 – Données signées PKCS # 7

Champ PKCS # 7	Description
issuerAndSerialNumber	
issuerName	
CountryName	Etats-Unis d'Amérique
organizationName	CableLabs
CommonName	Autorité CA radicale de certificat CVC de CableLabs
certificateSerialNumber	<Numéro de série de certificat CVC de cosignataire>
digestAlgorithm	SHA-1
AuthenticatedAttributes	
contentType	Données (type de contenu de l'élément signedContent)
signingTime	Temps UTC (GMT), AAMMJJhhmmssZ
messageDigest	(condensé du contenu comme défini dans [PKCS # 7])
digestEncryptionAlgorithm	Chiffrement RSA
EncryptedDigest	
} *fin des infos d'opérateur mso signataire*	
} *fin des infos de signataire*	
} *fin des données signées*	

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 PS 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 PS 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 PS. Si le téléchargement et l'installation du code ont réussi, l'élément de services PS DOIT remplacer son certificat actuellement mémorisé par le nouveau certificat reçu dans le champ de contenu signé. 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 186-2]. L'élément de services PS 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 la 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 la Rec. UIT-T X.509. Ce certificat doit être utilisé par l'élément de services PS en mode d'approvisionnement 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 la 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
51	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 la 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 PS 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 correspondre exactement à la structure représentée dans le Tableau 11-22, à l'exception des éventuels changements d'ordre requis par le codage DER (par exemple l'ordre des attributs SET OF). L'élément de services PS DEVRAIT ignorer le certificat CVC s'il ne correspond pas à la structure codée en règles DER représentée dans le Tableau 11-22. Le codage DER DOIT satisfaire aux exigences du § 11.3.4.2, "Infrastructure de clé publique (PKI)".

Tableau 11-22/J.192 – Certificat de vérification de code conforme à la Rec. UIT-T X.509

Certificat X.509	Description
Certificate {	
version	2 (c'est-à-dire [UIT-T X.509] version 3)
serialNumber	entier, inférieur ou égal à 20 octets (c'est-à-dire nombre unique attribué par l'autorité CA radicale)
signature	codage RSA à hachage SHA-1, paramètres vides
issuer	
countryName	Etats-Unis d'Amérique
organizationName	
commonName	Autorité CA radicale de certificat CVC
validity	
notBefore	Temps utc (GMT), AAMMJJhhmmssZ (c'est-à-dire heure de production)
notAfter	Temps utc (GMT), AAMMJJhhmmssZ
subject	
countryName	<Nom de pays>
organizationName	<Nom de l'entreprise>
commonName	<Nom courant>
subjectPublicKeyInfo	
algorithm	Chiffrement RSA, paramètres vides
subjectPublicKey	module de 2048 bits
extensions	
KeyUsage	<utilisation de la clé>
authorityKeyIdentifier	<identificateur de la clé d'autorité>
signatureAlgorithm	codage RSA à hachage SHA-1, paramètres vides
signatureValue	<valeur de la signature>
} fin certificat	

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 PS 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 PS 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 PS.

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 PS 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 PS 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 PS 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 PS 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 PS 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 PS. 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 PS.

L'élément de services PS 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 PS 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 PS 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 PS 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 PS 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 PS comme objets codeAccessStart et cvcAccessStart.

L'élément de services PS 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 PS DOIT comparer précisément ces valeurs mémorisées aux valeurs de temps UTC délivrées à l'élément de services PS 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 PS 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 PS 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 PS.

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 PS:

- nom d'organisation du constructeur de l'élément de services PS;
- 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 PS DOIT toujours être présent dans le dispositif. Le nom d'organisation du constructeur de l'élément de services PS 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 PS.

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 PS.

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 PS.

11.8.4.4.2 Initialisation du réseau

Afin de prendre en charge la vérification de code, le fichier de configuration du 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 PS, l'élément de services PS 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 PS 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 PS, 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 PS. Un fichier de configuration PEUT contenir:

- aucun certificat CVC – l'élément de services PS NE DOIT PAS accepter de fichier de code;
- un seul certificat CVC de constructeur – l'élément de services PS 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 PS 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 PS 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 PS 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 PS 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 PS. Afin qu'un élément de services PS 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 PS 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 PS 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 PS ne contient pas de certificat CVC valide et que sa capacité de mise à jour des fichiers de code a été désactivée, l'élément de services PS DOIT ignorer toutes les informations contenues dans un certificat CVC délivré ultérieurement par protocole SNMP.

Le nom d'organisation du constructeur de l'élément de services PS et les valeurs de contrôles variables dans le temps du constructeur DOIVENT toujours être présents dans l'élément de services PS. 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 PS 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 PS 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 PS, l'ensemble de valeurs de certificat CVC du cosignataire DOIT être mémorisé dans la mémoire de l'élément de services PS. 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 PS, le certificat CVC est toujours dans le fichier de configuration. L'élément de services PS 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 PS 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 PS DOIT exécuter les étapes de validation et de procédure suivantes. Si l'un des essais de vérification suivants échoue, l'élément de services PS DOIT immédiatement arrêter le processus de vérification du certificat CVC et journaliser l'erreur si applicable. Si le fichier de configuration du PS n'inclut pas de certificat CVC correctement validé, l'élément de services PS NE DOIT PAS télécharger les fichiers de mise à jour de code, que ce téléchargement soit déclenché par le fichier de configuration du PS ou par protocole SNMP. En outre, si le fichier de configuration du PS ne contient pas de certificat CVC correctement validé, l'élément de services PS n'est pas tenu de traiter les certificats CVC délivrés ultérieurement et NE DOIT PAS accepter d'informations à partir d'un certificat CVC délivré ultérieurement par une commande SNMP de mise à jour (SET).

Dès réception du certificat CVC dans un fichier de configuration, l'élément de services PS DOIT:

1) vérifier que l'extension d'utilisation de clé étendue est contenue dans le certificat CVC comme défini dans le § 11.3.4.2.2.2;
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 PS 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 PS;
      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 PS, alors c'est le certificat CVC du cosignataire actuel et l'élément de services PS 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 PS;
      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 PS, 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;

iii) 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 PS;

iv) 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 PS. La vérification de la signature authentifiera l'origine et validera la confiance dans les paramètres du certificat CVC;

v) mettre à jour la valeur actuelle de l'objet cvcAccessStart de l'élément de services PS 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 PS, mettre à jour la valeur de l'objet codeAccessStart de l'élément de services PS avec la valeur d'instant de début de validité. L'élément de services PS 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 PS 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 PS DOIT exécuter les étapes de validation et de procédure suivantes:

NOTE – Si l'un quelconque des essais de vérification échoue, l'élément de services PS 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 PS DOIT:

1) vérifier que l'extension d'utilisation de clé étendue est contenue dans le certificat CVC, comme défini 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 PS 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 PS;

   b) si le nom d'organisation est identique à celui du cosignataire de code actuel de l'élément de services PS, 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 PS;

   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 PS 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 PS;

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 PS. 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 PS, mettre à jour la valeur de l'objet codeAccessStart de l'élément de services PS 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 § 11.8.4.1.7. L'autorité CA de certificat CVC du laboratoire CTL NE DOIT PAS signer de certificat CVC à moins qu'il ne soit identique au format spécifié dans le § 11.8.4.1.7. Avant de signer un certificat CVC, l'autorité CA de certificat CVC de laboratoire CTL DOIT vérifier que la demande de certificat est authentique.

L'autorité CA de certificat CVC de laboratoire CTL sera chargée de l'enregistrement des noms des souscripteurs de certificat CVC autorisés, qui comprennent les constructeurs d'élément de services PS et les câblo-opérateurs qui vont cosigner les images de code. Il appartient à l'autorité CA de certificat CVC de laboratoire CTL 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 des noms d'organisation aux cosignataires de fichier de code:

- le nom d'organisation servant à s'identifier soi-même comme agent cosignataire de code dans un certificat CVC DOIT être attribué par l'organisation qui a émis le certificat radical;
- le nom DOIT être un chaîne imprimable de 8 chiffres hexadécimaux qui distingue de façon univoque un agent de signature de code de tous les autres;
- chaque chiffre hexadécimal contenu dans le nom DOIT être choisi dans le jeu de caractères 0-9 (0x30-0x39) ou A-F (0x41-0x46);
- la chaîne composée de 8 chiffres 0 n'est pas autorisée et NE DOIT PAS être utilisée dans un 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 PS.

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 PS DOIT l'accepter.

11.8.4.6 Processus de déclenchement

Les téléchargements de code, sans tenir compte du mode d'approvisionnement, peuvent être lancés pendant le processus d'approvisionnement 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 PS 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 PS 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 PS.

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 PS subit une perte d'alimentation ou une réinitialisation pendant une mise à jour initialisée par SNMP, l'élément de services PS DOIT reprendre la mise à jour sans exiger d'intervention manuelle et, quand l'élément de services PS 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};
- docsDevSwCurrentVers DOIT être la version actuelle du logiciel qui doit fonctionner dans le dispositif.

Si l'élément de services PS 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 PS 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};
- docsDevSwCurrentVers DOIT être la version actuelle de logiciel qui doit fonctionner dans le dispositif.

Si un élément de services PS atteint le nombre maximal de réessais TFTP par l'envoi d'un total de 16 réessais consécutifs, l'élément de services PS 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};
- docsDevSwCurrentVers DOIT être la version actuelle de logiciel qui doit fonctionner dans le dispositif.

Après que l'élément de services PS a achevé la mise à jour logicielle sécurisée qui a été lancée par protocole SNMP, l'élément de services PS 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 PS 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 PS. 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 PS;
- docsDevSwServer PEUT être l'adresse du serveur TFTP contenant le logiciel qui fonctionne actuellement dans l'élément de services PS;
- docsDevSwOperStatus DOIT être à la valeur completeFromMgt{3};

- docsDevSwCurrentVers DOIT être la version actuelle du logiciel qui doit fonctionner dans l'élément de services PS.

Si l'élément de services PS 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};
- docsDevSwCurrentVers DOIT être la version actuelle de logiciel qui doit fonctionner dans le dispositif.

Si l'élément de services PS détermine que l'image téléchargée est endommagée ou corrompue, l'élément de services PS DOIT ignorer l'image nouvellement téléchargée. L'élément de services PS peut réessayer de télécharger si le nombre MAX de réessais de séquence TFTP n'a pas été atteint. Si l'élément de services PS choisit de ne pas réessayer et que le nombre MAX de réessais de séquence TFTP n'ait pas été atteint, l'élément de services PS 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};
- docsDevSwCurrentVers DOIT être la version actuelle de logiciel qui doit fonctionner dans le dispositif.

Si l'élément de services PS détermine que l'image est endommagée ou corrompue, l'élément de services PS DOIT ignorer l'image nouvellement téléchargée. L'élément de services PS 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 PS DOIT se replier sur la dernière image connue qui fonctionnait et passer à un état opérationnel. Dans ce cas, l'élément de services PS 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 PS a atteint l'état opérationnel, l'élément de services PS 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};
- docsDevSwCurrentVers 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 initialisé par fichier de configuration est déclenché par l'envoi du nom de fichier de mise à jour logicielle contenu dans le fichier de configuration de l'élément de services PS. Si le nom de fichier de mise à jour logicielle contenu dans le fichier de configuration de

l'élément de services PS ne correspond pas à l'image logicielle actuelle du dispositif, l'élément de services PS DOIT demander le fichier spécifié par TFTP à partir du serveur de logiciel.

NOTE – L'adresse IP du serveur de logiciels est un paramètre distinct. S'il est présent, l'élément de services PS DOIT essayer de télécharger le fichier spécifié à partir de ce serveur. S'il est absent, l'élément de services PS DOIT essayer de télécharger le fichier spécifié à partir du serveur de fichiers de configuration.

Si l'élément de services PS 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 PS 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};
- docsDevSwCurrentVers DOIT être la version actuelle de logiciel qui doit fonctionner dans le dispositif.

Si un élément de services PS atteint le nombre maximal de réessais TFTP par l'envoi d'un total de 16 réessais consécutifs, l'élément de services PS 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};
- docsDevSwCurrentVers DOIT être la version actuelle de logiciel qui doit fonctionner dans le dispositif.

Après que l'élément de services PS a achevé la mise à jour logicielle sécurisée qui a été initialisée par fichier de configuration, l'élément de services PS DOIT réamorcer et devenir opérationnel avec l'image logicielle correcte. Après que l'élément de services PS 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};
- docsDevSwCurrentVers 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 PS 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 PS 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 PS 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 PS;
   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 PS DOIT valider le certificat CVC de constructeur en vérifiant que:
   a) le nom d'organisation titulaire du certificat CVC est identique au nom du constructeur actuellement mémorisé dans la mémoire de l'élément de services PS;
   b) 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 PS;
   c) l'extension d'utilisation de clé étendue est contenue dans le certificat CVC comme défini dans le § 11.3.4.2.2.2;
3) l'élément de services PS 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 PS. 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 PS. 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 PS DOIT vérifier la signature du fichier de code du constructeur:
   a) l'élément de services PS 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 PS 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 PS 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 PS;
      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 PS 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 PS;

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 PS pour le nom d'organisation titulaire correspondant;

iii) l'extension d'utilisation de clé étendue est contenue dans le certificat CVC comme défini dans le § 11.3.4.2.2.2;

c) l'élément de services PS 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 PS. 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 PS. 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 PS DOIT vérifier la signature du fichier de code du cosignataire;

e) l'élément de services PS 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 PS 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 PS 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 PS 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 PS 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 PS;
   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 PS;
   c) la valeur signingTime [RFC 2315] du constructeur est inférieure à la valeur codeAccessStart actuellement contenue dans l'élément de services PS;
   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 PS;
   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 PS;
   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 PS;
   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 PS;
   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 PS;
   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 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 PS;
   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 PS;
   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 CableHome à son état antérieur exact.

Quand l'élément de services PS 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 PS 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 PS en mode d'approvisionnement 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

Tableau 11-23/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 d'approvisionnement 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 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 d'approvisionnement afin d'offrir une session sécurisée entre le serveur HTTPS et le dispositif PS aux fins de téléchargement du fichier de configuration du 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 d'approvisionnement 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 d'approvisionnement 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.

Tableau 11-24/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 le document [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 d'approvisionnement 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 d'approvisionnement DHCP avec le processus de téléchargement TFTP spécifié. Le diagramme de fluence d'approvisionnement 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, dans le fichier de configuration du PS, les informations nécessaires pour lancer un fichier distinct de configuration du pare-feu comme spécifié dans le § 6, le dispositif PS DOIT déterminer s'il a besoin de continuer la session de protocole TLS avec le serveur HTTPS qui a délivré le fichier de configuration du PS, ou d'établir une nouvelle session TLS avec un autre serveur HTTPS pour le téléchargement du fichier de configuration du pare-feu. Si le dispositif PS est chargé de télécharger un fichier de configuration du pare-feu vers un autre serveur HTTPS utilisé pour télécharger le fichier de configuration du PS, le dispositif PS DOIT établir une session de sécurité TLS comme spécifié par la présente Recommandation avant de demander le fichier de configuration du pare-feu.

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 point d'accès TCP #443 spécifié par les normes de l'autorité IANA afin de se connecter au serveur (distant) HTTP/TLS. Si la connexion TCP/IP ne peut pas être effectuée après cinq tentatives, avec 30 secondes autorisées pour chaque tentative, le dispositif PS DOIT envoyer l'événement 68002000.

11.9.4.3 Messages TLS

Sauf indication contraire, tous les messages sont conformes au document [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 cinq 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 le document [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 le document [RFC 2246].

11.9.4.3.3 Message ClientCertificate

Le dispositif PS DOIT envoyer son certificat d'élément de services PS au serveur HTTPS dans le message ClientCertificate. On suppose que le serveur HTTPS va valider et vérifier le certificat de client PS avant de procéder au dialogue initial. Si le certificat du dispositif PS n'est pas correctement authentifié par le serveur (distant), le dispositif PS client 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 du document [RFC 2246].

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 du document [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_NULL_WITH_NULL_NULL;
- 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 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 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 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 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 le document [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 le document [RFC 2246]. Les erreurs associées aux certificats DOIVENT être traitées comme étant fatales car le dispositif PS et le protocole HTTP reposent sur l'authentification du client et 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 cinq 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 le document [RFC 2616]. Le dispositif PS client DOIT envoyer au serveur une demande de fichier de configuration du PS ou de configuration de pare-feu selon la version HTTP 1.1. Le nom de fichier de configuration du PS utilisé dans la demande 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 demande 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 PS, ou qu'il a reçu par demande SET (mise à jour) du protocole SNMP.

Le dispositif PS client DOIT manipuler tous les messages de description d'état conformément au document [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 à partir du document [RFC 2616]. Si le téléchargement ne peut pas être achevé après cinq tentatives, avec 240 secondes autorisées pour chaque tentative, le dispositif PS DOIT échouer à la session et envoyer l'événement 68003100.

NOTE – Une longue temporisation est prévue afin d'inclure le téléchargement du fichier de configuration, qui parfois peut malheureusement être lent. 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" – Norme [FIPS 140-2]. 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 portail;
- accès à une base de données PS;
- reconfiguration:
  - téléchargement de logiciel des services portail;
  - téléchargement du fichier de configuration du 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 PS 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'essai 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 point d'accès 7 du dispositif IP de réseau LAN spécifié. Le point d'accès 7 est réservé au service d'écho;
5) le dispositif IP de réseau LAN 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 demande 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 demande GET (obtenir) du protocole SNMP jusqu'à ce que les résultats des essais indiquent que l'essai s'est achevé.

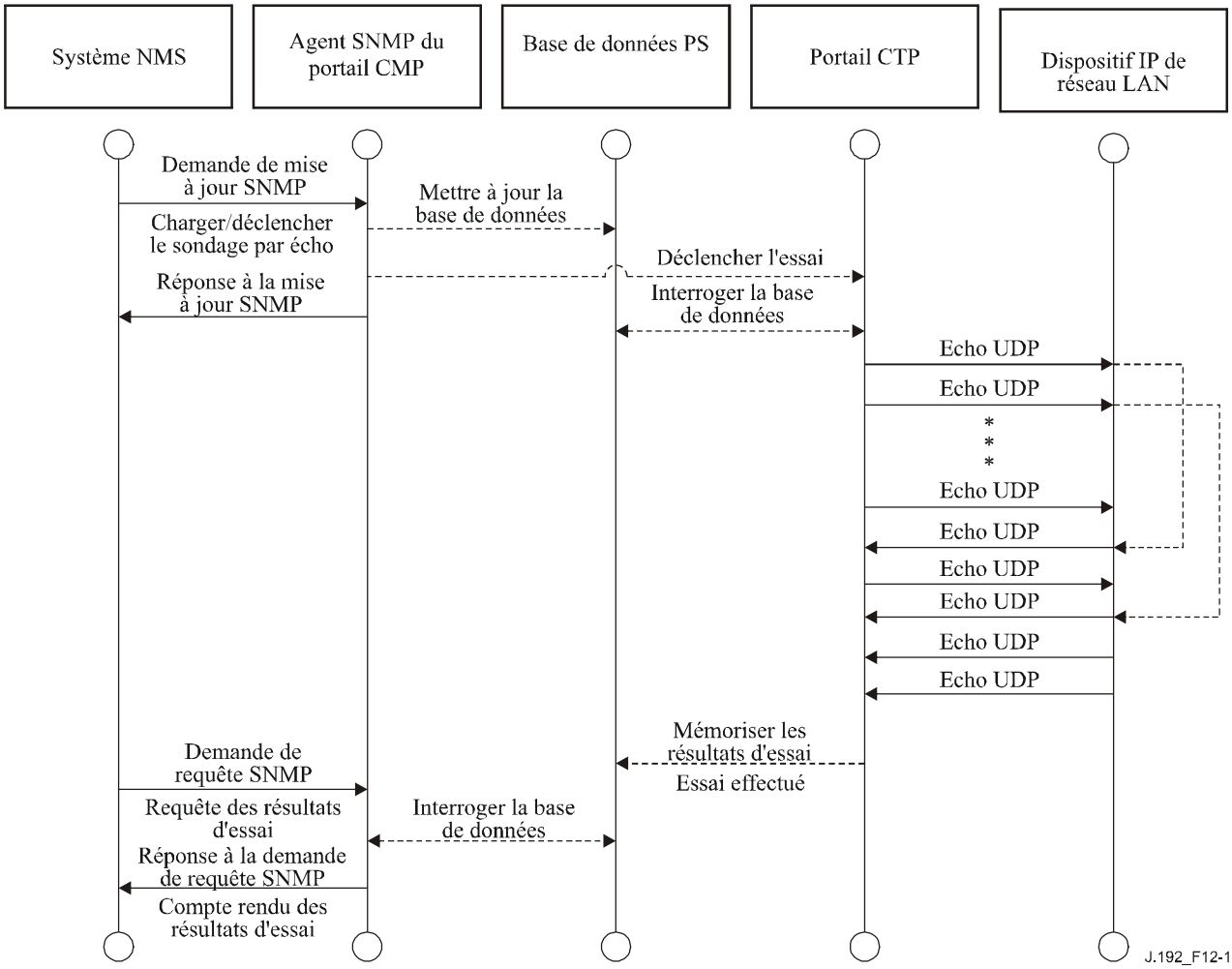


Figure 12-1/J.192 – Processus de l'utilitaire de vitesse de connexion – Diagramme séquentiel

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 demande 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 LAN spécifié;

5) le dispositif IP de réseau LAN 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 demande 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 demande GET (obtenir) du protocole SNMP jusqu'à ce que les résultats des essais indiquent que l'essai est achevé.

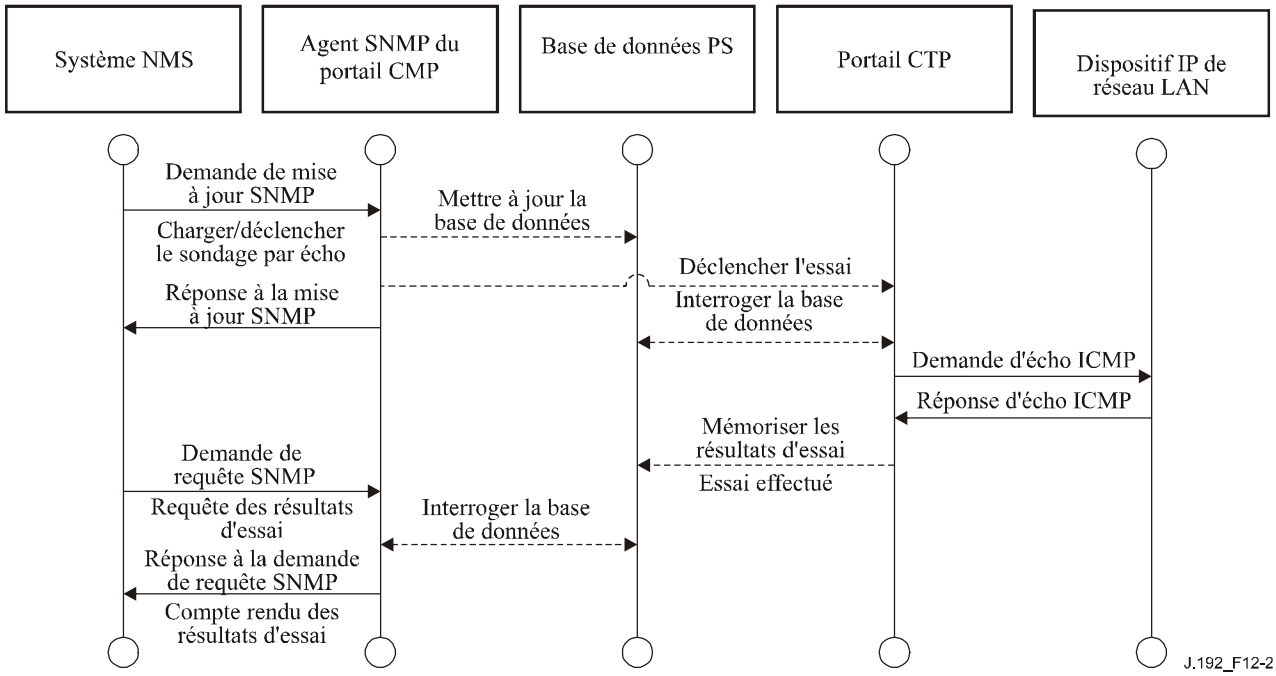


Figure 12-2/J.192 – Processus de l'utilitaire de sondage par écho – Diagramme séquentiel

12.3 Fonctionnement des services 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 GET-Request (demande de requête), GET-Next-Request (demande de 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 demande 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 demande "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.

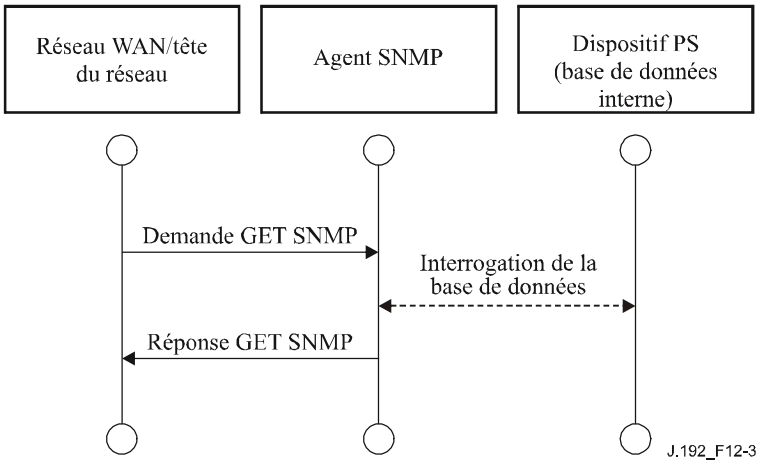


Figure 12-3/J.192 – Accès à une base de données PS à partir de l'interface PS/WAN-Man – Diagramme séquentiel

12.3.2 Reconfiguration

12.3.2.1 Téléchargement de logiciel des services portail

La Figure 12-4 décrit un processus de téléchargement de logiciel/micrologique pour un dispositif PS en mode d'approvisionnement 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 WAN peuvent avoir besoin d'être ré-approvisionnées (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.

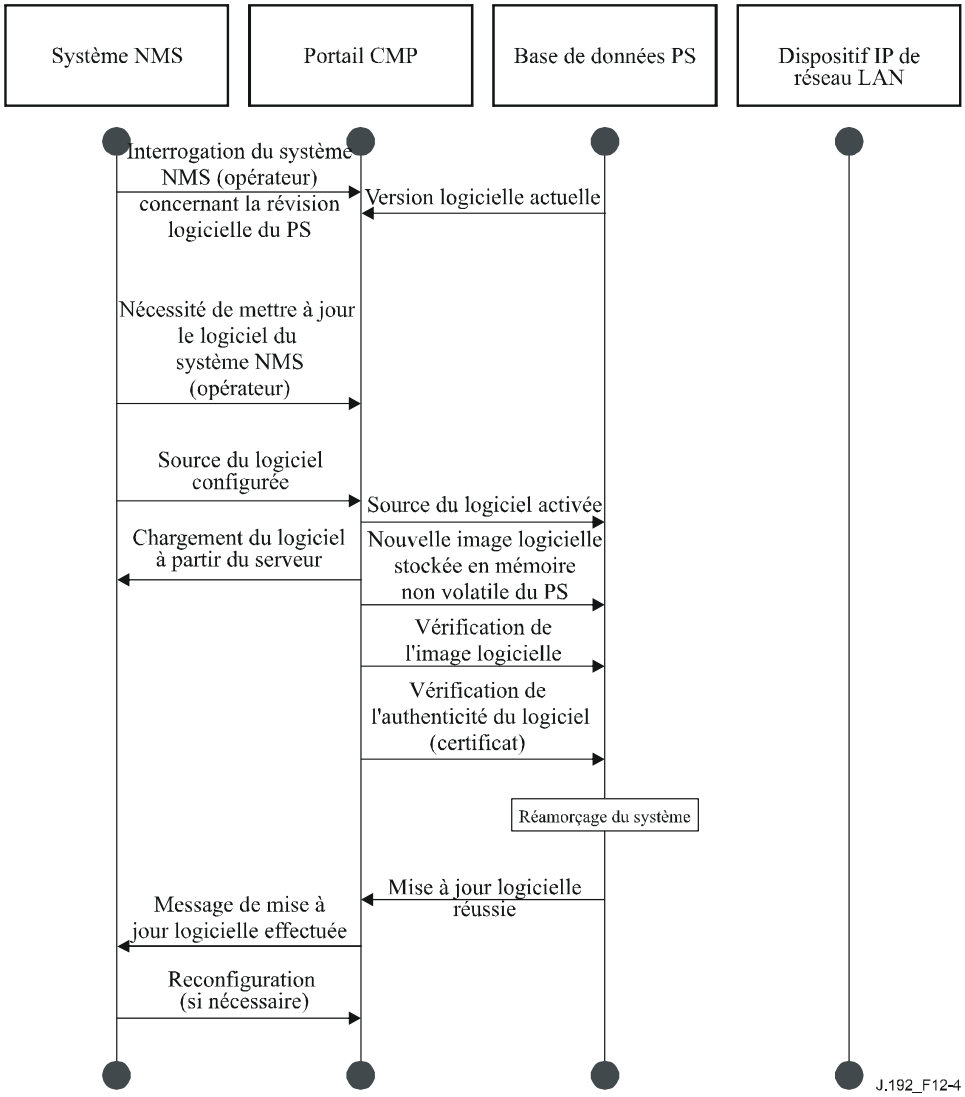


Figure 12-4/J.192 – Téléchargement de logiciel des services portail – Diagramme séquentiel

12.3.2.2 Téléchargement du fichier de configuration du PS

La Figure 12-5 décrit la reconfiguration d'un dispositif PS en mode d'approvisionnement SNMP par téléchargement du fichier de configuration. Ce processus est déclenché par le système NMS. Le fichier de configuration du 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.

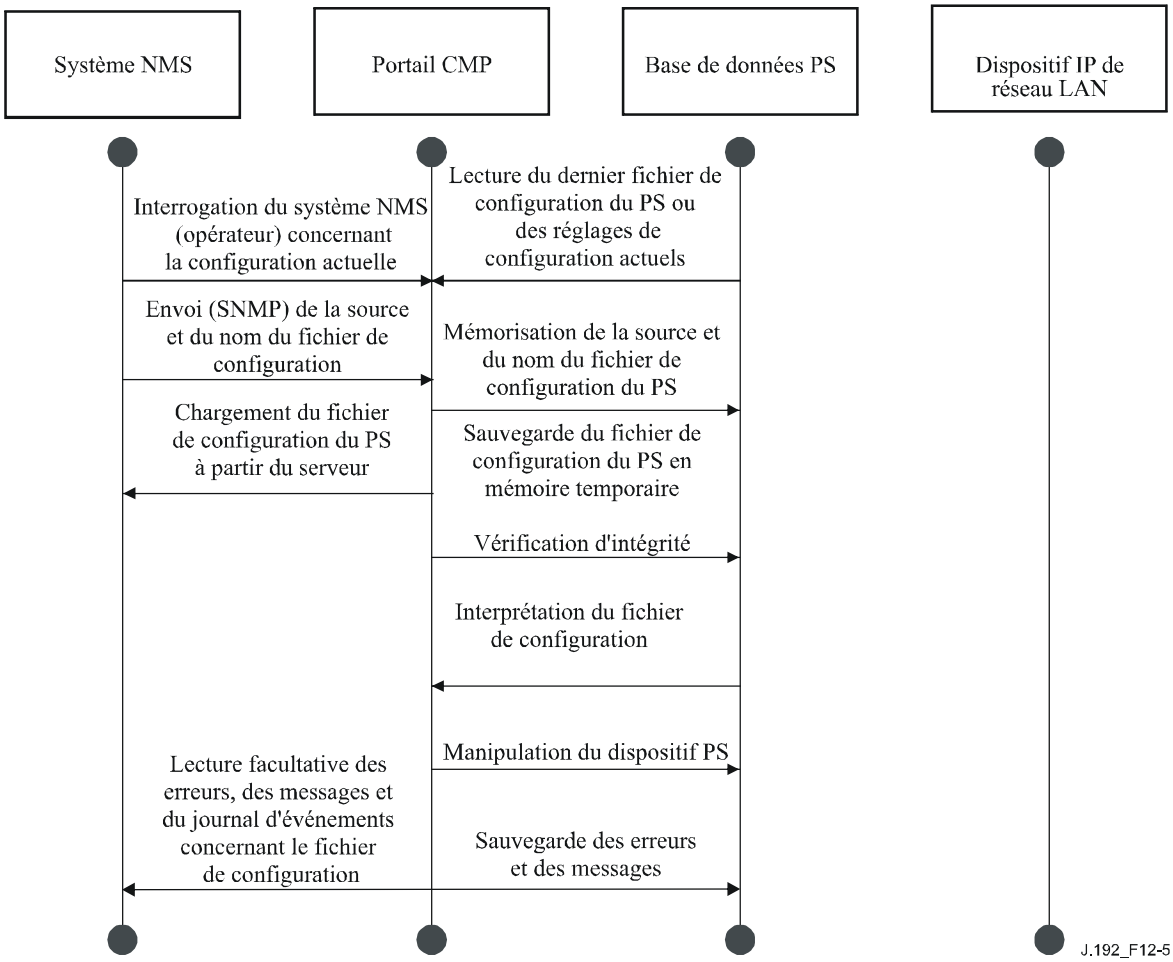


Figure 12-5/J.192 – Reconfiguration du dispositif PS (téléchargement du fichier de configuration) – Diagramme séquentiel

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.

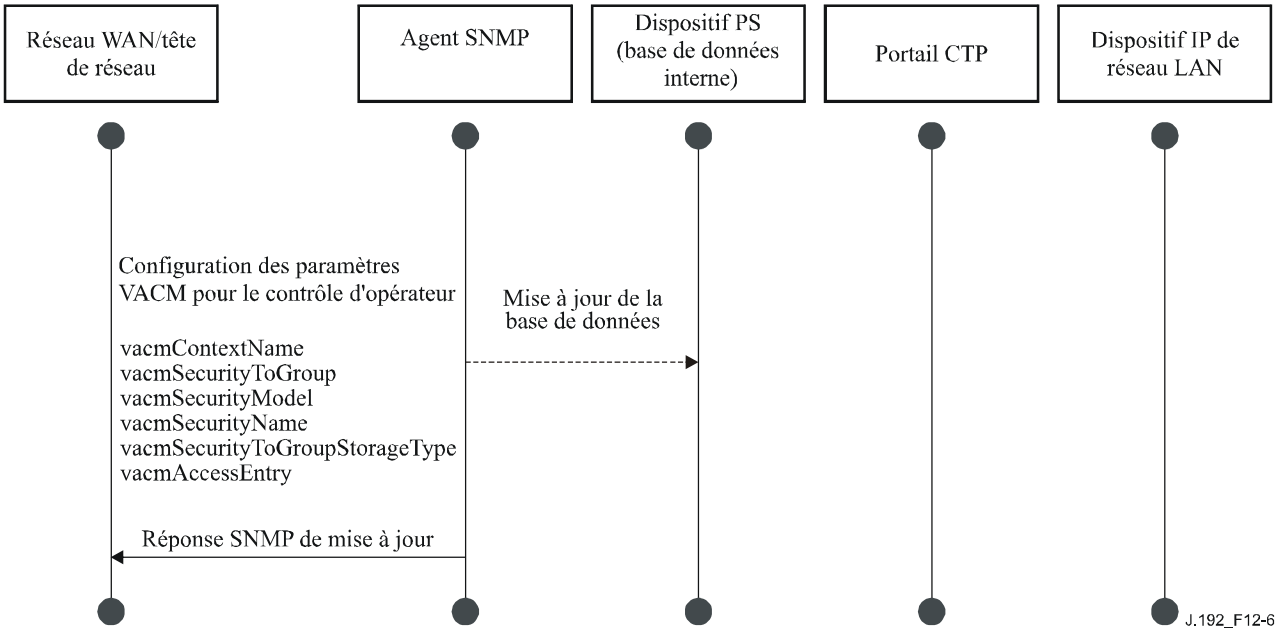


Figure 12-6/J.192 – Configuration des services portail (paramètres du modèle VACM) – Séquence

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 demande 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.

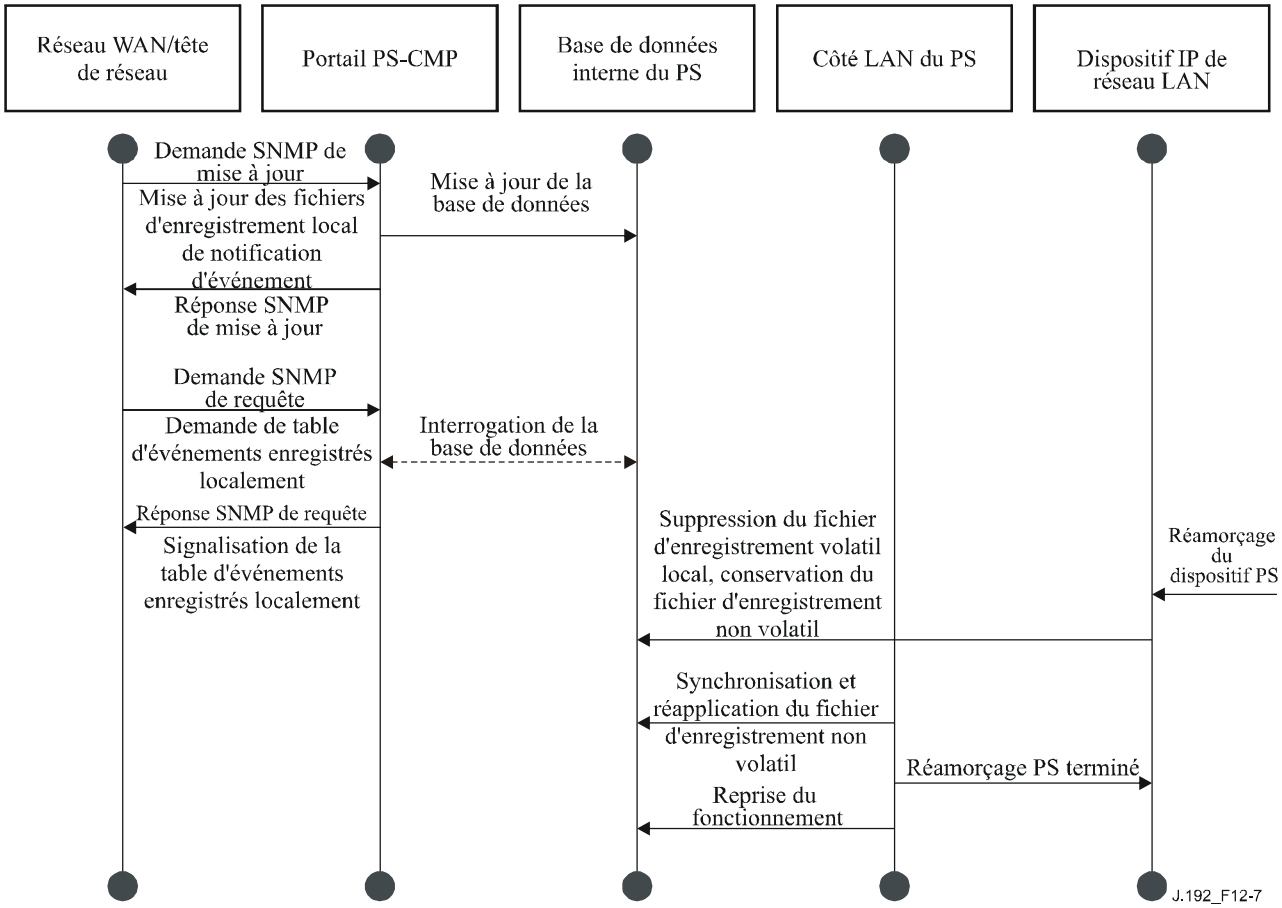


Figure 12-7/J.192 – Configuration des services portail (contrôle d'événement) – Séquence

La Figure 12-8 décrit le téléchargement d'un fichier de configuration pour un dispositif PS en mode d'approvisionnement SNMP. Ce processus est déclenché par une demande 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 transfert TRAP du protocole SNMP, l'adresse du serveur de transferts TRAP est récupérée à partir de la base de données PS et l'événement est envoyé à ce serveur de transferts TRAP.

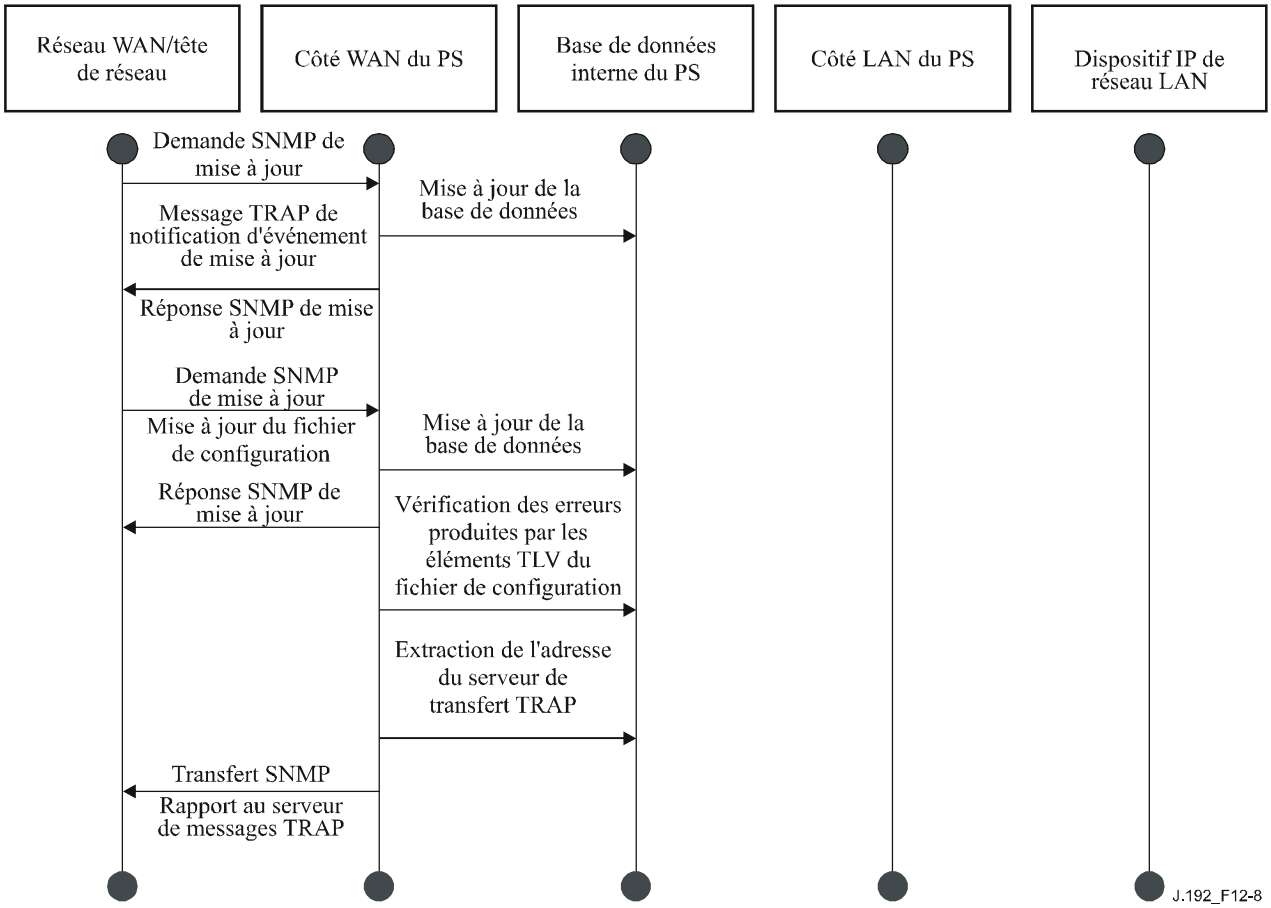


Figure 12-8/J.192 – Téléchargement du fichier de configuration du PS (avec éléments TLV non valides) – Séquence

La Figure 12-9 décrit le processus d'un dispositif IP de réseau LAN 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.

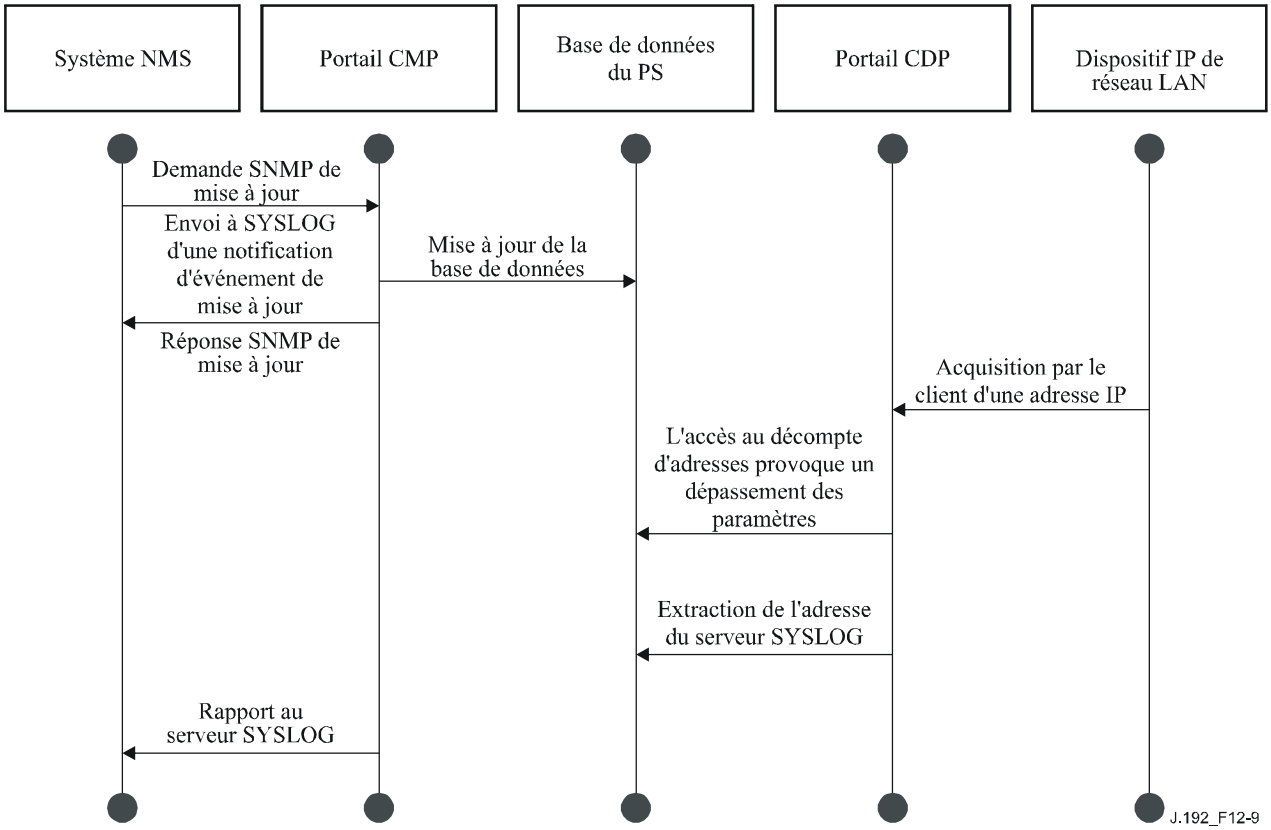


Figure 12-9/J.192 – Acquisition d'adresse (demande dépassant le compte approvisionné) – Séquence

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.

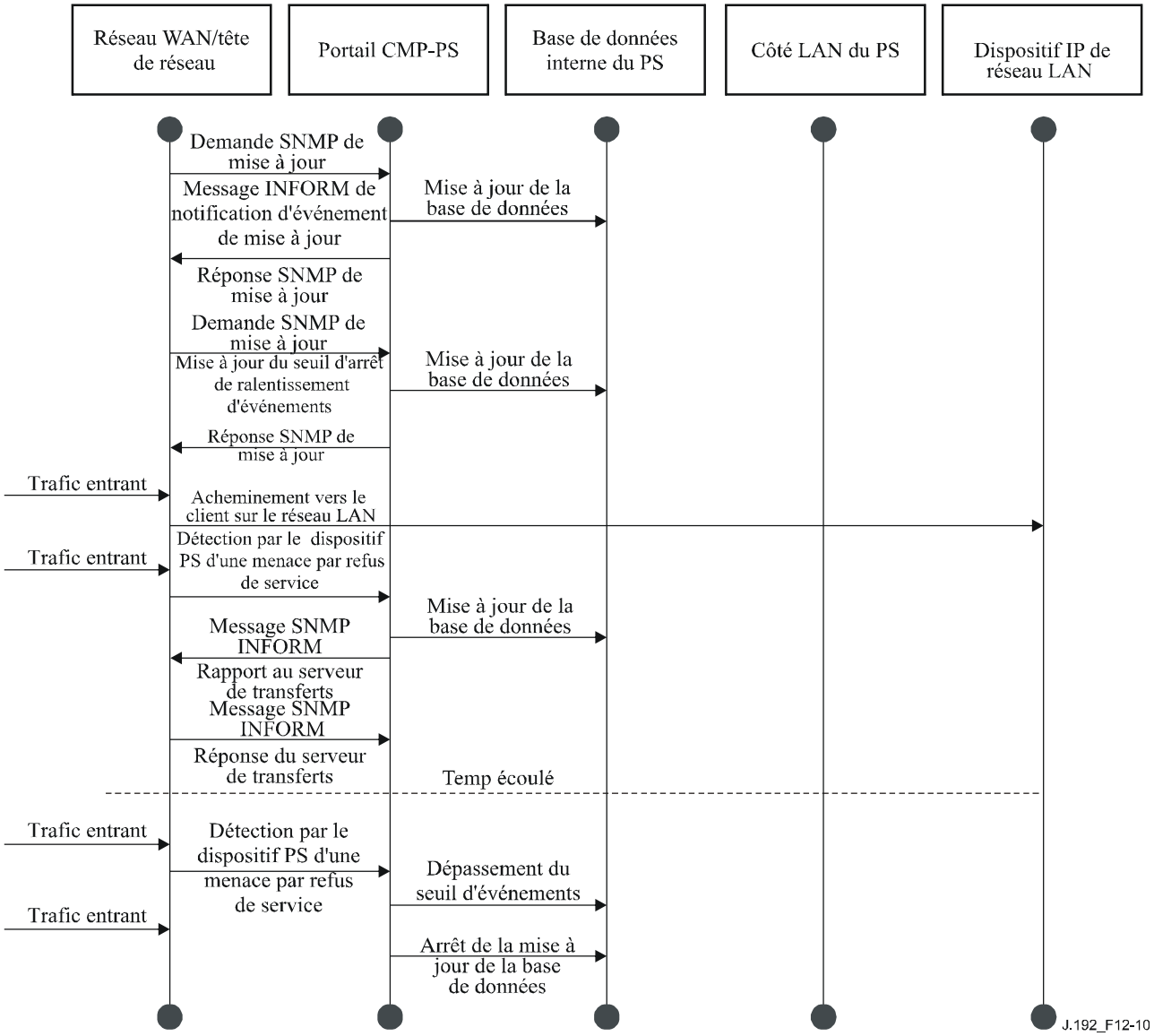


Figure 12-10/J.192 – Fonctionnement du ralentissement et de la limitation des événements au portail CMP

13 Processus d'approvisionnement

Le présent paragraphe décrit les processus impliqués lors de l'utilisation des utilitaires d'approvisionnement décrits dans le § 7, pour l'approvisionnement initial de dispositif IP de réseau LAN et de l'élément de services PS. Cet approvisionnement 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 PS.

Les processus d'approvisionnement sont décrits dans le présent paragraphe pour chacun des cas pertinents suivants:

- interface PS/WAN-Man – approvisionnement de la fonctionnalité de gestion fondée sur l'interface PS/WAN;
- interface PS/WAN-Data – approvisionnement d'adresses IP d'interface PS/WAN-Data à utiliser afin de créer des mappages de conversion CAT vers des dispositifs IP de réseau LAN situés dans le secteur d'adresses du réseau LAN-Trans;

- dispositif IP de réseau LAN situé dans le secteur LAN-Trans – approvisionnement d'un dispositif IP de réseau LAN avec une adresse IP convertie;
- dispositif IP de réseau LAN situé dans le secteur LAN-Pass – approvisionnement d'un dispositif IP de réseau LAN avec une adresse IP qui est transmise au réseau WAN.

L'approvisionnement de l'élément CM d'un dispositif PS intégré est séparé et distinct de l'approvisionnement 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 l'approvisionnement des câblo-modems.

Les éléments fonctionnels avec lesquels l'élément de services PS interagit pendant les processus d'approvisionnement 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 d'approvisionnement SNMP mais non en mode d'approvisionnement DHCP. Les autres éléments fonctionnels sont utilisés dans les deux modes d'approvisionnement.

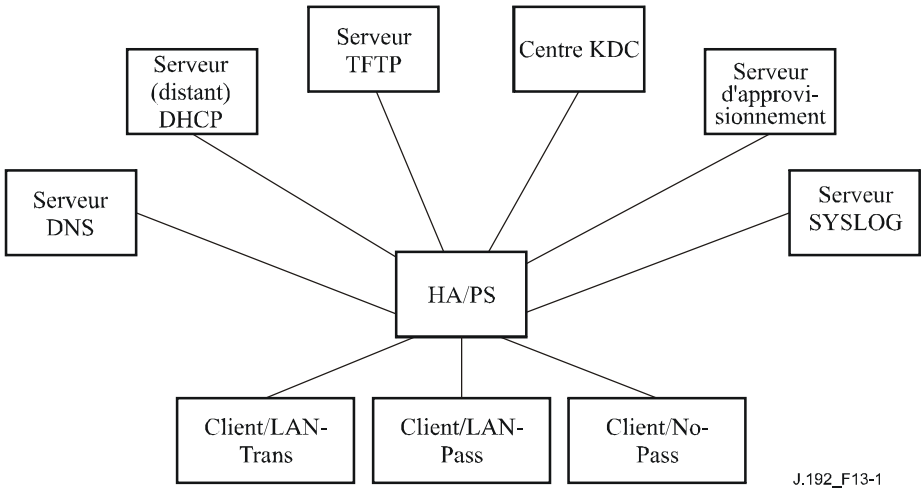


Figure 13-1/J.192 – Eléments Fonctionnels d'approvisionnement IPCable2Home

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 PS pour le dispositif PS et suit les règles décrites dans le document [RFC 1350]. Le serveur temporel (ToD) offre au dispositif PS les moyens d'acquérir l'heure actuelle en format UTC comme décrit dans le document [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 le document [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 le document [RFC 2576]. Le centre de distribution de clés (KDC) gère les clés d'autorisation et de chiffrement afin d'établir la confiance entre les éléments mis en réseau et implémente les règles définies dans le document [RFC 1949]. Le serveur de journalisation du système (SYSLOG) manipule les messages événementiels produits par le dispositif PS et par les dispositifs IP de réseau LAN 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 d'approvisionnement décrit dans le présent paragraphe afin d'accomplir les tâches énumérées au début du présent paragraphe.

13.1 Modes d'approvisionnement

Les paragraphes 5.5 et 7.2.1 présentent deux modes d'approvisionnement valides qui sont pris en charge par l'élément de services PS: le mode d'approvisionnement DHCP et le mode d'approvisionnement SNMP. Le dispositif PS fonctionne dans un troisième mode, le mode CableHome inactif, s'il n'est pas configuré de façon à fonctionner dans un des deux modes valides d'approvisionnement. Dans le présent paragraphe, les deux modes valides d'approvisionnement sont présentés plus en détail. La Figure 13-2 décrit un flux événementiel possible pour les deux modes d'approvisionnement et pour le mode CableHome 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 d'approvisionnement 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 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 d'approvisionnement 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 d'approvisionnement 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 d'approvisionnement 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 d'approvisionnement DHCP et en mode d'approvisionnement SNMP, ou s'il reçoit une combinaison non valide de ces champs et sous-options.

Toutes les conditions d'erreur ne sont pas représentées dans la Figure 13-2. Voir au § 7.2.2 une description du comportement du dispositif PS en cas de critères incorrects de décision relative au mode d'approvisionnement.

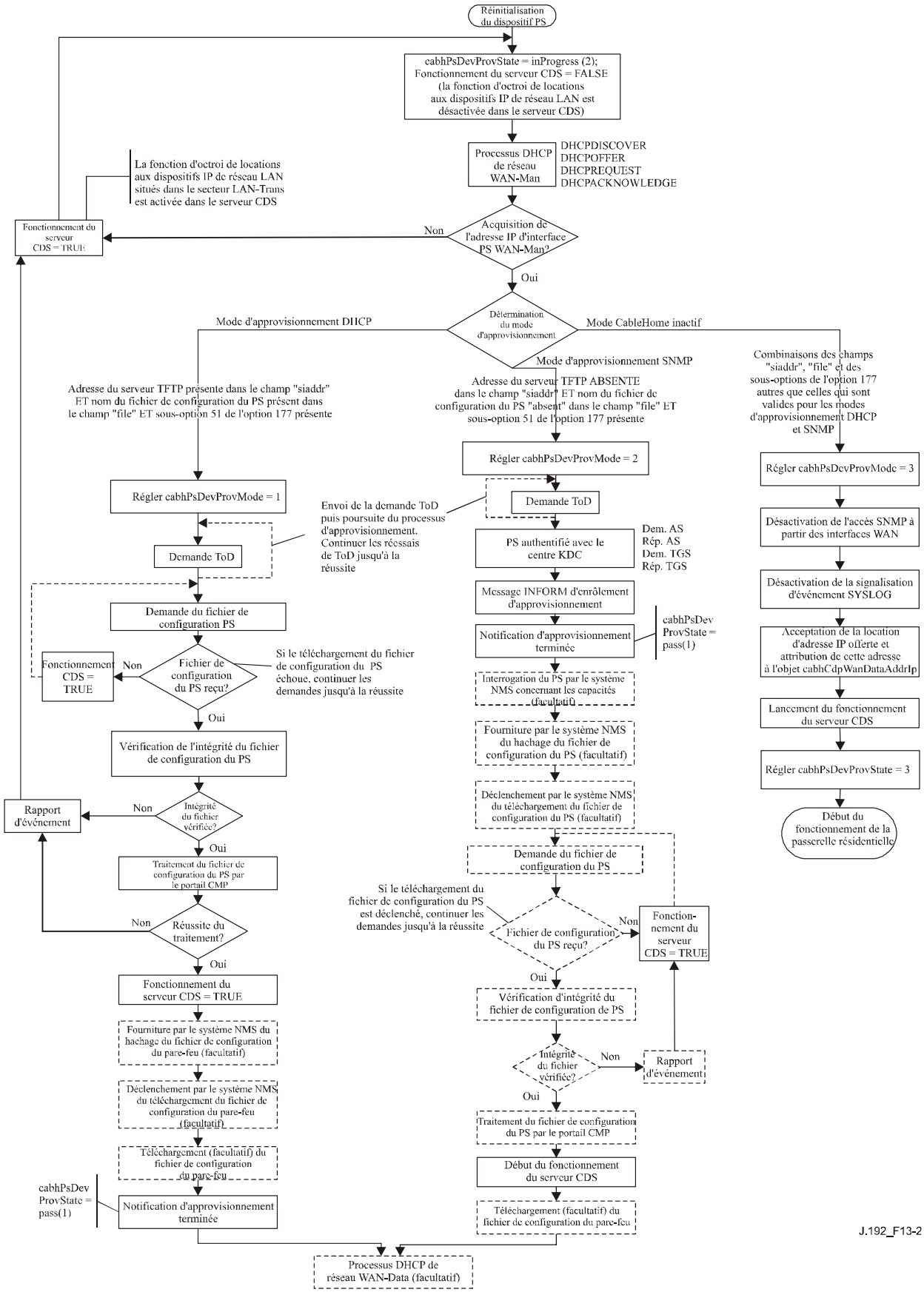


Figure 13-2/J.192 – Modes d'approvisionnement IPCable2Home

13.2 Processus d'approvisionnement des services portail pour la gestion: mode d'approvisionnement DHCP

Le dispositif PS demande au système d'approvisionnement 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 d'approvisionnement 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 WAN 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 d'approvisionnement DHCP, il utilise les informations du fichier de configuration du PS transmises dans le message DHCP comme déclencheur afin de télécharger le fichier de configuration du PS comme décrit dans le § 7.3. Le téléchargement du fichier de configuration du PS est nécessaire lorsque le dispositif PS fonctionne en mode d'approvisionnement DHCP, mais est facultatif lorsque le dispositif PS fonctionne en mode d'approvisionnement SNMP.

En mode d'approvisionnement 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.

Les Figures 13-3 et 13-1 décrivent la séquence des messages nécessaires pour initialiser un dispositif PS fonctionnant en mode d'approvisionnement DHCP. Le processus d'approvisionnement pour la gestion d'un dispositif PS fonctionnant en mode d'approvisionnement DHCP est le même pour le dispositif PS intégré avec un câblo-modem DOCSIS et pour le dispositif PS autonome. L'approvisionnement d'un dispositif PS intégré NE DOIT PAS intervenir avant le processus d'approvisionnement du câblo-modem. L'approvisionnement 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 13-3.

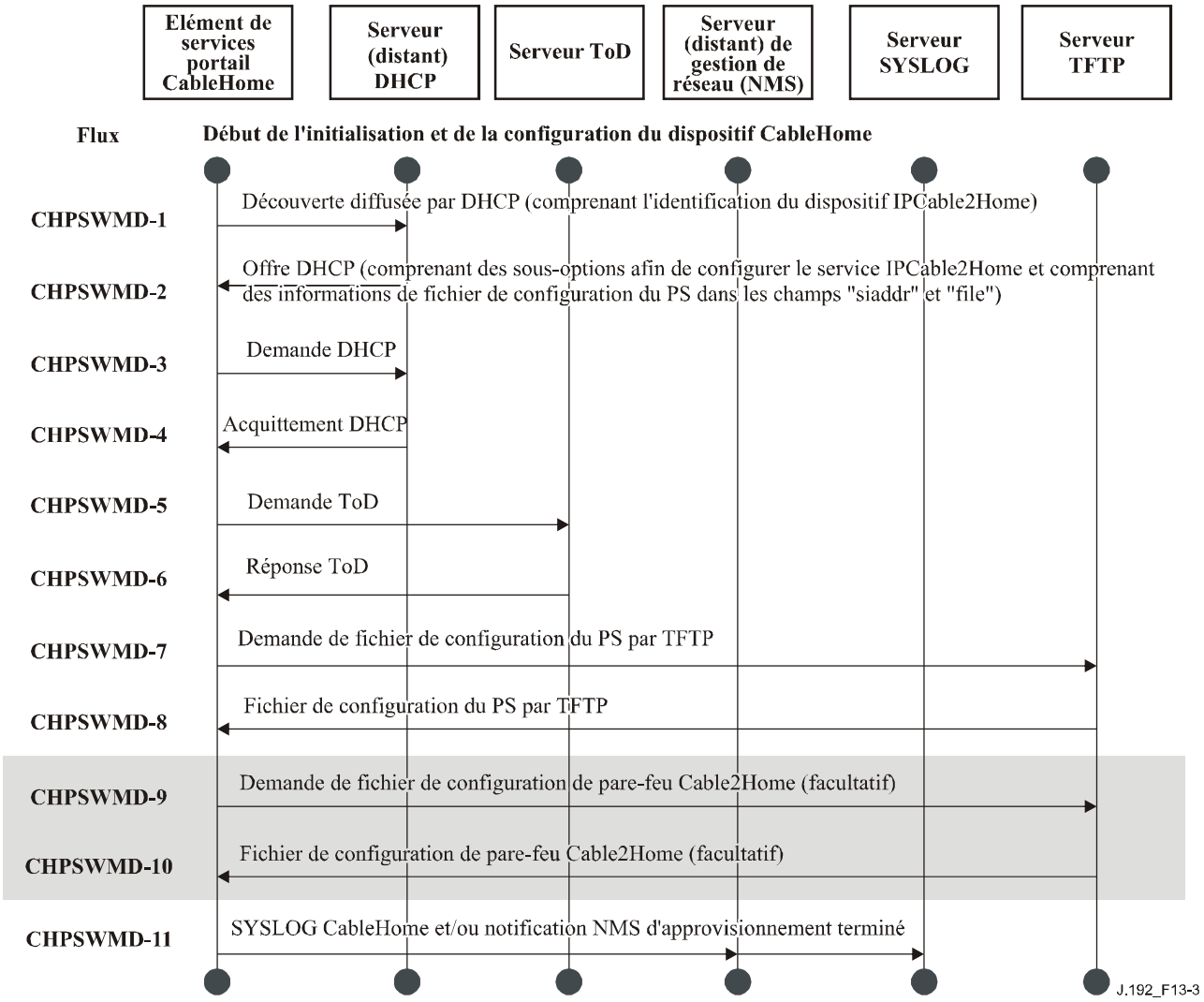


Figure 13-3/J.192 – Processus d'approvisionnement pour la gestion des services portail – Mode d'approvisionnement DHCP

Le Tableau 13-1 décrit les messages individuels CHPSWMD-1 – CHPSWMD-11 représentés dans la Figure 13-3.

Tableau 13-1/J.192 – Description des flux pour le processus d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement DHCP

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement 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 d'approvisionnement.	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 d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement DHCP

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
CHPSWMD-5	Demande d'heure actuelle (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 actuelle en format UTC.	CHPSWMD-6 DOIT survenir après achèvement de l'étape CHPSWMD-5.	Passer à l'étape CHPSWMD-7, signaler une erreur et revenir à CHPSWMD-5 (continuer à essayer ToD jusqu'à la réussite).
CHPSWMD-7	Demande de transfert TFTP Le dispositif PS fonctionnant en mode d'approvisionnement DHCP envoie au serveur TFTP une demande de 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.
CHPSWMD-8	L'envoi par le serveur TFTP du fichier de configuration du PS Après que le fichier de configuration du PS est reçu, le hachage est vérifié. Voir § 7.4.4.1. Le fichier de configuration du PS est alors traité. Voir au § 7.4.4 le contenu du fichier de configuration du 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 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, signaler une erreur et revenir à CHPSWMD-7 (continuer à essayer le téléchargement du fichier de configuration du PS). Si le traitement du fichier de configuration du PS produit une erreur, passer à l'étape CHPSWMD-9 et signaler l'erreur comme événement. Si le temporisateur d'approvisionnement arrive à expiration avant que le fichier de configuration du PS soit correctement téléchargé, le dispositif PS DOIT signaler une erreur et revenir à CHPSWMD-1.

Tableau 13-1/J.192 – Description des flux pour le processus d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement DHCP

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
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 PS, celui-ci envoie au serveur TFTP de configuration de pare-feu une demande de 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 PS, le processus d'approvisionnement du dispositif PS (mode d'approvisionnement 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 portail mais signaler une erreur et continuer à essayer CHPSWMD-9.
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 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 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.

Tableau 13-1/J.192 – Description des flux pour le processus d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement DHCP

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
CHPSWMD-11	Approvisionnement terminé Sur demande du système d'approvisionnement, le dispositif PS est tenu d'informer le système d'approvisionnement de l'état d'approvisionnement du dispositif PS. Le système d'approvisionnement 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 d'approvisionnement terminé au serveur SYSLOG avec l'état d'approvisionnement réglé à PASS. Si le dispositif PS achève correctement toutes les étapes d'approvisionnement 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 une notification d'approvisionnement terminé (objet cabhPsDevInitTrap) avec les paramètres appropriés au récepteur de notification. Si le temporisateur d'approvisionnement des services portail arrive à expiration avant que toutes les étapes requises de CHPSWMD-1 à CHPSWMD-10 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 d'approvisionnement terminé au serveur SYSLOG avec l'état d'approvisionnement réglé à FAIL.	CHPSWMD-11 DOIT survenir après achèvement de CHPSWMD-10.	Si le transfert SNMP échoue, le serveur d'approvisionnement ne peut pas savoir que le processus d'approvisionnement s'est achevé à moins qu'il n'interroge l'objet cabhPsProvState.

Tableau 13-1/J.192 – Description des flux pour le processus d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement DHCP

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
	Si le temporisateur d'approvisionnement des services portail arrive à expiration avant que toutes les étapes requises de CHPSWMD-1 à CHPSWMD-10 soient achevées et que le dispositif PS ait reçu des paramètres valides pour le récepteur de notification, le dispositif PS DOIT envoyer une notification d'approvisionnement échoué (objet cabhPsDevInitTrap) au récepteur de notification. Le dispositif PS DOIT mettre à jour la valeur de l'objet cabhPsDevProvState avec l'état 'pass' (1) quand les étapes de flux d'approvisionnement CHPSWMD-1 à CHPSWMD-11 ont été menées à bien. Le dispositif PS DOIT mettre à jour la valeur de l'objet cabhPsDevProvState avec l'état 'fail' (3) et signaler un événement indiquant l'échec du processus d'approvisionnement si le temporisateur d'approvisionnement des services portail arrive à expiration avant que la valeur de l'objet cabhPsDevProvState soit mise à jour avec l'état 'pass'.		

13.3 Processus d'approvisionnement des services portail pour la gestion: mode d'approvisionnement DHCP avec HTTP/TLS

Le dispositif PS demande au système d'approvisionnement 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 d'approvisionnement 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 WAN 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 d'approvisionnement DHCP, il utilisera les informations du fichier de configuration du PS transmises dans le message DHCP, comme déclencheur afin de télécharger le fichier de configuration du 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 d'approvisionnement 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 13-4 et le Tableau 13-2 décrivent la séquence de messages nécessaires pour initialiser un dispositif PS fonctionnant en mode d'approvisionnement DHCP avec HTTP/TLS. Le processus d'approvisionnement et la gestion du dispositif PS fonctionnant en mode d'approvisionnement DHCP sont les mêmes pour le dispositif PS intégré avec un câblo-modem DOCSIS et pour le dispositif PS autonome. L'approvisionnement du dispositif PS intégré NE DOIT PAS intervenir avant le processus d'approvisionnement du câblo-modem. L'approvisionnement 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.

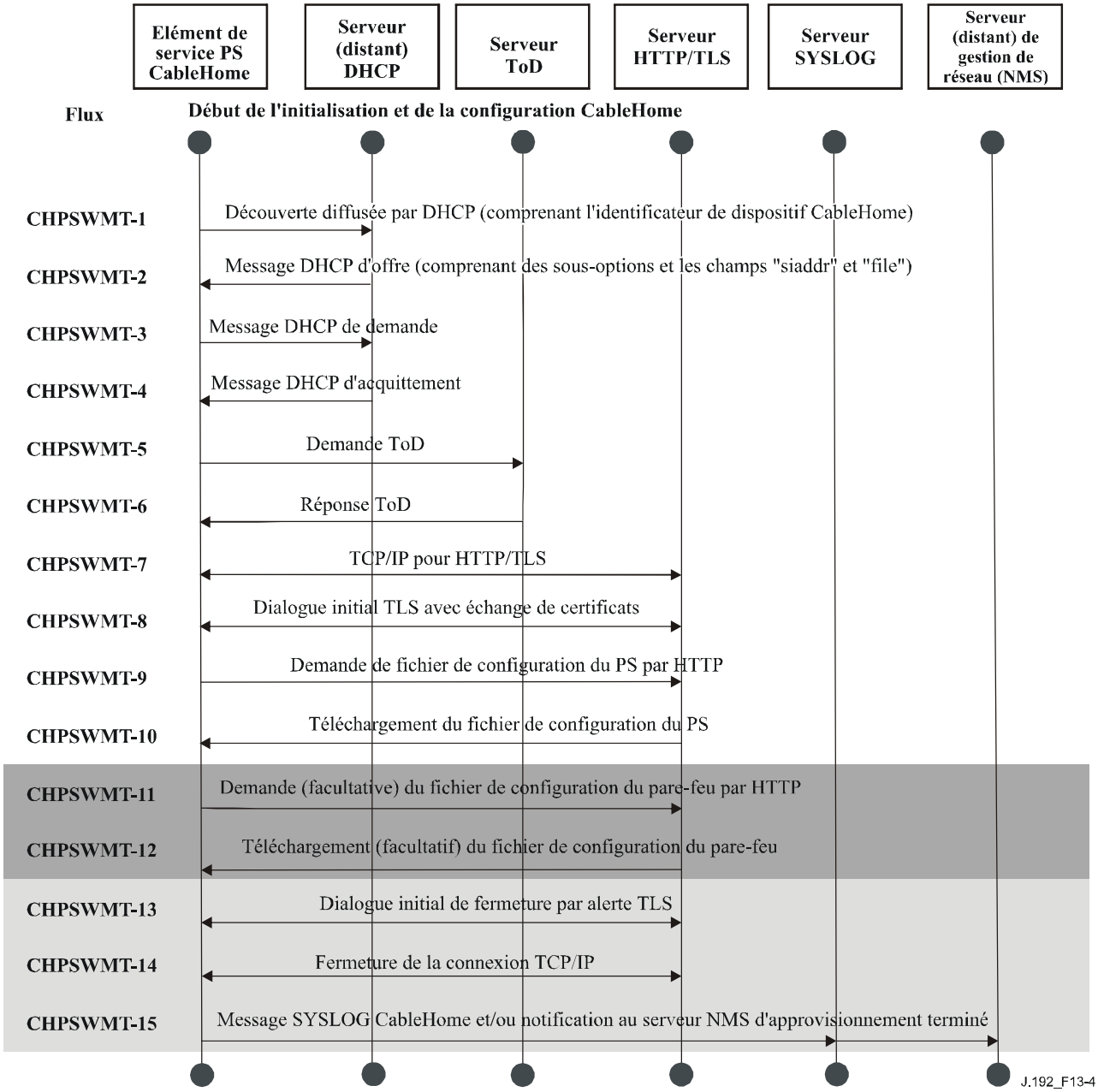


Figure 13-4/J.192 – Processus d'approvisionnement – Mode d'approvisionnement DHCP utilisant HTTP/TLS

Le Tableau 13-2 décrit les messages individuels CHPSWMT-1 – CHPSWMT-15 représentés dans la Figure 13-4. Pour plus d'informations, voir § 11.9, "Sécurité du fichier de configuration du PS en mode d'approvisionnement DHCP".

Tableau 13-2/J.192 – Description des flux en mode d'approvisionnement DHCP utilisant HTTP/TLS

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement 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 d'approvisionnement.	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 d'approvisionnement DHCP utilisant HTTP/TLS

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement 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 PS en mode d'approvisionnement 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 actuelle (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 actuelle: exigences".	CHPSWMT-5 DOIT survenir après achèvement de l'étape CHPSWMT-4.	Passer à l'étape CHPSWMT-6.
CHPSWMT-6	Réponse d'heure ToD Le serveur temporel ToD est censé répondre avec l'heure actuelle en format UTC.	CHPSWMT-6 DOIT survenir après achèvement de l'étape CHPSWMT-5.	Signaler une erreur et revenir à CHPSWMT-5 (continuer à essayer ToD jusqu'à la réussite).
CHPSWMT-7	Etablissement du protocole TCP/IP Le dispositif PS fonctionnant en mode d'approvisionnement DHCP établit une session TCP/IP afin d'échanger des messages HTTP avec le serveur HTTP dans le système d'approvisionnement 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.

Tableau 13-2/J.192 – Description des flux en mode d'approvisionnement DHCP utilisant HTTP/TLS

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
CHPSWMT-8	Dialogue initial du protocole TLS Le dispositif PS fonctionnant en mode d'approvisionnement 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.
CHPSWMT-9	Demande de fichier de configuration par HTTP Le dispositif PS fonctionnant en mode d'approvisionnement 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 PS Le fichier de configuration du PS est traité. Voir le § 7.4.4 concernant le contenu du fichier de configuration du 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 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 PS). Si le traitement du dispositif Fichier de configuration du PS produit une erreur, passer à l'étape CHPSWMT-13 et signaler l'erreur comme événement. Si le temporisateur d'approvisionnement arrive à expiration avant que le fichier de configuration du PS ait été correctement téléchargé, le dispositif PS DOIT signaler une erreur et revenir à CHPSWMT-1.

Tableau 13-2/J.192 – Description des flux en mode d'approvisionnement DHCP utilisant HTTP/TLS

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
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 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 PS, le processus d'approvisionnement du dispositif PS (mode d'approvisionnement 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 portail mais signaler une erreur et continuer à essayer CHPSWMT-13.
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 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 d'approvisionnement terminé.	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.

Tableau 13-2/J.192 – Description des flux en mode d'approvisionnement DHCP utilisant HTTP/TLS

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
CHPSWMT-15	Approvisionnement terminé Sur demande du système d'approvisionnement, le dispositif PS est tenu d'informer le système d'approvisionnement de l'état d'approvisionnement du dispositif PS. Le système d'approvisionnement 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 d'approvisionnement terminé au serveur SYSLOG avec l'état d'approvisionnement réglé à PASS. Si le dispositif PS achève correctement toutes les étapes d'approvisionnement 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 transfert (docsDevNmAccessIP) et configurant le message-transfert d'approvisionnement terminé (objet cabhPsDevInitTrap) avec la valeur 'lecture seulement avec transferts automatiques' (réglage de l'objet docsDevNmAccess à '4' voir [RFC 2669]), le dispositif PS DOIT envoyer un message-transfert d'approvisionnement terminé (objet cabhPsDevInitTrap) avec les paramètres appropriés, au récepteur de transferts. Si le temporisateur d'approvisionnement des services 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 d'approvisionnement terminé au serveur SYSLOG avec l'état d'approvisionnement réglé à FAIL.	CHPSWMT-15 DOIT survenir après achèvement de l'étape CHPSWMT-14.	Si le transfert SNMP échoue, le serveur d'approvisionnement ne peut pas savoir que le processus d'approvisionnement s'est achevé à moins qu'il n'interroge l'objet cabhPsDevProvState.

Tableau 13-2/J.192 – Description des flux en mode d'approvisionnement DHCP utilisant HTTP/TLS

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
	Si le temporisateur d'approvisionnement des services 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 transfert (docsDevNmAccessIP) et configurant le message-transfert d'approvisionnement terminé (objet cabhPsDevInitTrap) avec la valeur 'lecture seulement avec transferts automatiques' (mettre docsDevNmAccess à '4'. Voir [RFC 2669]), le dispositif PS DOIT envoyer un message-transfert d'échec d'approvisionnement (objet cabhPsDevInitRetryTrap), au récepteur de transferts. Le dispositif PS DOIT mettre à jour la valeur de l'objet cabhPsDevProvState avec l'état 'pass' (1) quand les étapes de flux d'approvisionnement CHPSWMT-1 à CHPSWMT-14 ont été menées à bien. Le dispositif PS DOIT mettre à jour la valeur de l'objet cabhPsDevProvState avec l'état 'fail' (3) et signaler un événement indiquant l'échec du processus d'approvisionnement si le temporisateur d'approvisionnement des services portail arrive à expiration avant que la valeur de l'objet cabhPsDevProvState soit mise à jour avec l'état 'pass'.		

13.4 Approvisionnement des services portail pour la gestion: mode d'approvisionnement 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 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 d'approvisionnement 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 d'approvisionnement SNMP, de télécharger un fichier de configuration du PS à partir du serveur TFTP. La notification de l'achèvement du processus d'approvisionnement 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 13-5 décrit les flux de message qui sont à utiliser afin d'accomplir l'approvisionnement du dispositif PS quand celui-ci fonctionne en mode d'approvisionnement SNMP. Le processus d'approvisionnement pour l'interface PS/WAN-Man est le même pour le dispositif PS intégré et pour le dispositif PS autonome. L'approvisionnement du dispositif PS autonome DEVRAIT intervenir immédiatement après mise sous tension/réinitialisation.

Le processus d'approvisionnement pour le réseau WAN-Man d'un dispositif PS fonctionnant en mode d'approvisionnement SNMP DOIT survenir par la séquence illustrée dans la Figure 13-5 et décrite en détail dans le Tableau 13-3. Les étapes facultatives sont représentées en grisé dans la Figure 13-5. Ces étapes facultatives peuvent être effectuées immédiatement après l'étape CHPSWMS-15, à un moment ultérieur, ou ne pas être effectuées du tout.

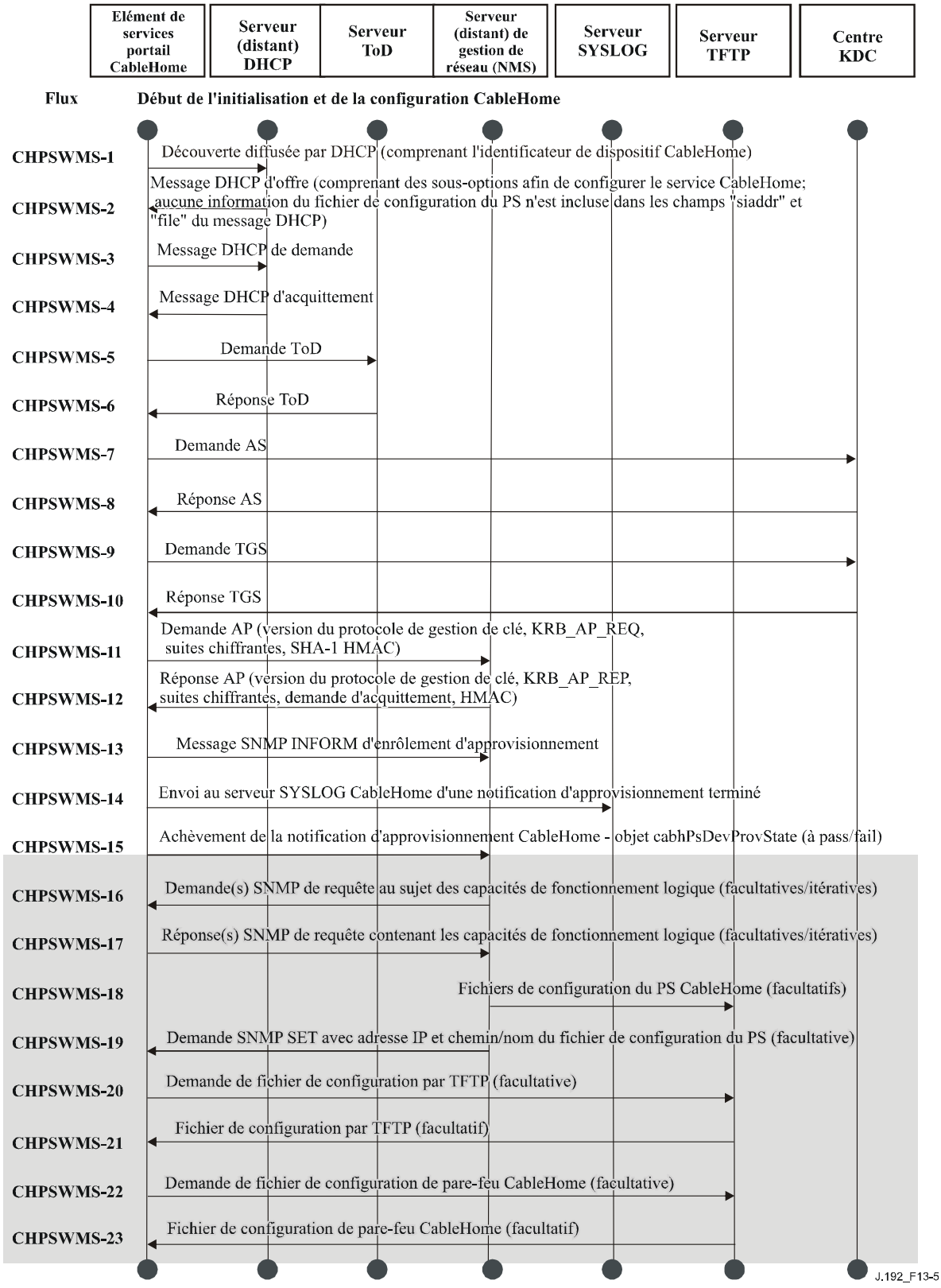


Figure 13-5/J.192 – Processus d'approvisionnement pour la gestion des services portail – Mode d'approvisionnement SNMP

Le Tableau 13-3 décrit les étapes individuelles du processus d'approvisionnement illustré dans la Figure 13-5.

Tableau 13-3/J.192 – Description des flux pour le processus d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement SNMP

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement 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 d'approvisionnement.	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.
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 177 avec les sous-options 3, 6, et 51 ET aucune information de fichier de configuration du 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 § 7.2.3.3). 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.

Tableau 13-3/J.192 – Description des flux pour le processus d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement SNMP

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-5	Demande d'heure actuelle (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 actuelle en format UTC.	CHPSWMS-6 DOIT survenir après achèvement de l'étape CHPSWMS-5.	Signaler une erreur et revenir à CHPSWMS-5 (continuer à essayer ToD jusqu'à la réussite).
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 offert dans l'option DHCP 177, sous-option 51, 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 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 51 de l'option DHCP 177.	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 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.

Tableau 13-3/J.192 – Description des flux pour le processus d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement SNMP

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-11	Demande de point d'accès AP Le dispositif PS envoie le message de demande de point d'accès 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.
CHPSWMS-12	Réponse de point d'accès 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 point d'accès 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	SNMP INFORM Après que le dispositif PS fonctionnant en mode d'approvisionnement SNMP a établi les clés SNMPv3, ce dispositif DOIT envoyer un message SNMPv3 INFORM (objet cabhPsDevProvEnrollTrap) demandant l'enrôlement dans l'entité SNMP dont l'adresse IP a été offerte dans l'option 177, sous-option 3, dans le message ACK du message DHCP.	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 d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement SNMP

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-14	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 "approvisionnement terminé". Cette notification comportera le résultat de succès/échec de l'opération d'approvisionnement. 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-14 DOIT survenir après achèvement de l'étape CHPSWMS-13.	
CHPSWMS-15	SNMP INFORM Le dispositif PS DOIT envoyer au système NMS un message SNMP INFORM (objet cabhPsDevInitTrap) contenant une notification "approvisionnement terminé". L'état FAIL se produit quand le traitement du fichier de configuration échoue. Sinon l'état d'approvisionnement est PASS. Le dispositif PS DOIT mettre à jour la valeur de l'objet cabhPsDevProvState avec l'état 'pass' (1) quand les étapes de flux d'approvisionnement CHPSWMS-1 à CHPSWMS-15 ont été menées à bien. Le dispositif PS DOIT mettre à jour la valeur de l'objet cabhPsDevProvState avec l'état 'fail' (3) et signaler un événement indiquant l'échec du processus d'approvisionnement si le temporisateur d'approvisionnement des services portail arrive à expiration avant que la valeur de l'objet cabhPsDevProvState soit mise à jour avec l'état 'pass'.	CHPSWMS-15 DOIT survenir après achèvement de l'étape CHPSWMS-14.	Si le dispositif PS ne reçoit pas de réponse au message INFORM d'approvisionnement terminé, 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 d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement SNMP

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
Etapes facultatives			
CHPSWMS-16	Requête SNMP GET Si l'une quelconque des capacités additionnelles du dispositif est requise par le système d'approvisionnement, 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 d'approvisionnement peut utiliser une requête GET-Bulk afin d'obtenir plusieurs éléments informatifs dans un seul message.	L'étape CHPSWMS-16 n'est pas censée intervenir avant CHPSWMS-15.	Retourner à CHPSWMS-1.
CHPSWMS-17	Réponse à la requête SNMP GET Etape itérative: le dispositif PS répond aux messages de demande GET-REQUEST ou GET-Bulk 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 d'approvisionnement.	Si l'étape CHPSWMS-16 se produit, l'étape CHPSWMS-17 DOIT survenir après achèvement de l'étape CHPSWMS-16.	N/A
CHPSWMS-18	Création du fichier de configuration Etape facultative: le système d'approvisionnement fait appel aux informations des étapes CHPSWMS-16 et CHPSWMS-17 d'approvisionnement du dispositif PS afin de créer un fichier de configuration du PS. Le système d'approvisionnement 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-17 se produit, l'étape CHPSWMS-18 DOIT survenir après achèvement de l'étape CHPSWMS-17.	N/A

Tableau 13-3/J.192 – Description des flux pour le processus d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement SNMP

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-19	Demande SET (mise à jour) du protocole SNMP Le système d'approvisionnement 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 PS et le hachage du fichier de configuration comme décrit dans le § 7.4.4.1, "Format du fichier de configuration – Exigences" (mode d'approvisionnement 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 demande 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-18 se produit, l'étape CHPSWMS-19 DOIT survenir après achèvement de l'étape CHPSWMS-18.	Retourner à CHPSWMS-1 si l'ensemble a été reçu, mais qu'il y ait eu une erreur de traitement.
CHPSWMS-20	Demande de transfert TFTP Si le système NMS déclenche le dispositif PS afin de télécharger un fichier de configuration du PS comme décrit dans le § 7.4.4.1, le dispositif PS envoie au serveur TFTP une demande de requête GET du protocole TFTP afin de demander le fichier spécifié de configuration du PS.	Si l'étape CHPSWMS-19 se produit, l'étape CHPSWMS-20 DOIT survenir après achèvement de l'étape CHPSWMS-19.	Passer à l'étape CHPSWMS-19.

Tableau 13-3/J.192 – Description des flux pour le processus d'approvisionnement à l'interface PS/WAN-Man en mode d'approvisionnement SNMP

Etape du flux	Approvisionnement à l'interface PS/WAN-Man: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-21	Envoi par le serveur TFTP du fichier de configuration Après que le dispositif PS a reçu le fichier de configuration du PS, celui-ci calcule le hachage du fichier de configuration du PS et le compare à la valeur reçue au cours de l'étape CHPSWMS-19. Le dispositif PS traite ensuite le fichier de configuration du 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 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-20 se produit, l'étape CHPSWMS-21 se produit après achèvement de l'étape CHPSWMS-20.	Si le téléchargement TFTP échoue, signaler une erreur, passer à CHPSWMS-22 et continuer à essayer CHPSWMS-20 (continuer à essayer le téléchargement du fichier de configuration du PS). Si le traitement du fichier de configuration produit une erreur, continuer et signaler l'erreur comme événement.
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 demande de 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 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 portail mais signaler une erreur et continuer à essayer 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 PS et également selon qu'un fichier de configuration du PS est nécessaire.			

13.4.1 Téléchargement du fichier de configuration de l'interface PS/WAN-Man

Le dispositif PS fonctionnant en mode d'approvisionnement SNMP pourrait contenir suffisamment d'informations par défaut à la construction afin de permettre le fonctionnement du côté LAN ou du côté WAN ou des deux côtés sans téléchargement de fichier de configuration du PS. Si le dispositif PS doit fonctionner en mode d'approvisionnement SNMP, le système NMS pourrait déclencher le téléchargement d'un fichier de configuration du PS pour l'approvisionnement initial afin de remplacer la valeur par défaut à la construction 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 PS ou par une commande SNMP de mise à jour (SET) pendant l'initialisation.

13.4.2 Temporisateur d'approvisionnement des services portail

Un temporisateur d'approvisionnement est offert afin de garantir que le dispositif PS continuera de fonctionner pendant le processus d'approvisionnement même si une opération ne se termine pas. L'objet de temporisateur, cabhPsDevProvTimer, a une durée d'initialisation par défaut de 5 min.

13.4.3 Messages INFORM d'enrôlement d'approvisionnement/d'approvisionnement terminé

Pour le dispositif PS fonctionnant en mode d'approvisionnement SNMP seulement, le message INFORM d'enrôlement d'approvisionnement (objet cabhPsDevProvEnrollTrap) permet au serveur d'approvisionnement de déterminer que le dispositif PS est prêt pour le fichier de configuration du PS.

En mode d'approvisionnement DHCP ou en mode d'approvisionnement SNMP, le message-transfert d'approvisionnement terminé (objet cabhPsDevInitTrap) indique si la séquence d'approvisionnement s'est achevée correctement ou non.

13.4.4 Approvisionnement de journalisation SYSLOG

L'adresse IP du serveur SYSLOG DOIT être approvisionnée 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 d'approvisionnement et des erreurs

Comme indiqué dans les Tableaux 13-1 et 13-3, un échec au cours des étapes du processus d'approvisionnement provoque généralement le redémarrage du processus à la première étape, CHPSWMD-1 ou CHPSWMS-1.

13.5 Processus d'approvisionnement de l'interface PS/WAN-Data

Le dispositif PS demande zéro, une ou plusieurs adresse(s) 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 LAN.

Il n'y a aucune différence entre les modes d'approvisionnement DHCP et SNMP en terme de fonctionnement de l'interface PS/WAN-Data.

Les diagrammes suivants illustrent les flux de message qui sont à utiliser afin d'accomplir l'approvisionnement des adresses IP d'interface PS/WAN-Data. Le processus d'approvisionnement 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 d'approvisionnement pour l'adresse (les adresses) d'interface PS/WAN-Data se produit, il DOIT suivre la séquence illustrée dans la Figure 13-6 et décrit en détail dans le Tableau 13-4.

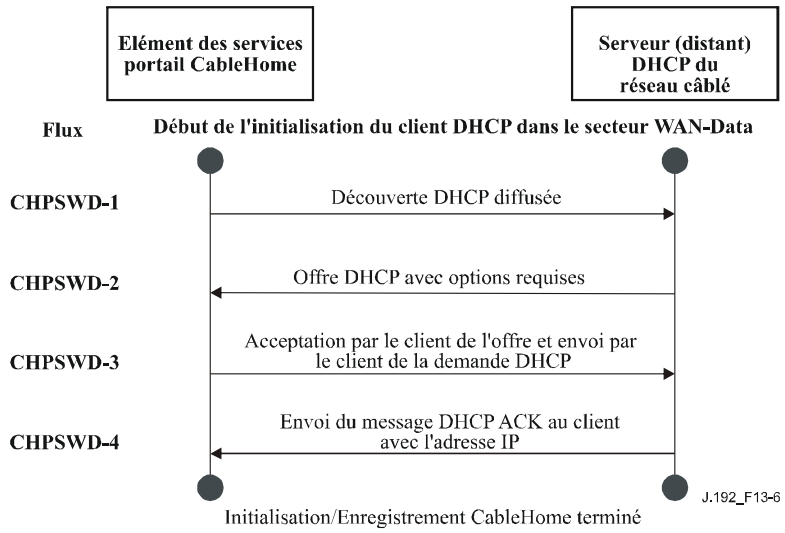


Figure 13-6/J.192 – Processus d'approvisionnement de l'interface PS/WAN-Data

Tableau 13-4/J.192 – Description des flux pour le processus d'approvisionnement de l'interface PS/WAN-Data

Etape du flux	Approvisionnement d'adresse d'interface PS/WAN-Data	Séquence normale	Séquence d'échec
CHPSWD-1	Découverte diffusée par DHCP Le dispositif PS diffuse un message DHCP DISCOVER y compris les options obligatoires énumérées dans le Tableau 7-10, "Options DHCP de client CDC contenues dans les messages DISCOVER et REQUEST".	Passer à CHPSWD-2.	En cas d'échec selon le protocole DHCP, répéter CHPSWD-1.
CHPSWD-2	DHCP OFFER Le serveur DHCP en tête de réseau reçoit le paquet DHCP DISCOVER, attribue une adresse IP extraite de la réserve d'adresses WAN-Data, construit un paquet DHCP OFFER et transmet le message OFFER du protocole DHCP à l'agent-relais DHCP [RFC 3046] situé dans le système CMTS.	Passer à CHPSWD-3.	En cas d'échec, le client arrivera en fin de temporisation selon le protocole DHCP, et l'étape CHPSWD-1 sera répétée.
CHPSWD-3	DHCP REQUEST Le portail CDP envoie un message DHCP REQUEST au serveur DHCP choisi afin d'accepter le message OFFER du protocole DHCP conformément aux exigences relatives au client du document [RFC 2131].	CHPSWD-3 DOIT survenir après achèvement de l'étape CHPSWD-2.	En cas d'échec selon le protocole DHCP, revenir à CHPSWD-1.
CHPSWD-4	DHCP ACK Le serveur DHCP envoie au portail CDP un message DHCP ACK qui contient l'adresse IPv4 pour l'interface PS/WAN-Data.	CHPSWD-4 DOIT survenir après achèvement de l'étape CHPSWD-3. L'approvisionnement se termine avec l'achèvement de l'étape CHPSWD-4.	En cas d'échec selon le protocole DHCP, revenir à CHPSWD-1.

13.6 Processus d'approvisionnement: point extrême dans le secteur LAN-Trans

Les éléments logiques de point extrême (BP) sont tenus d'implémenter deux protocoles pendant leur processus d'approvisionnement: les messages DHCP [RFC 2131] et BP_Init, définis dans le § 6.5.3.2, "Fonction de messagerie LAN du point MBP".

La fonction de portail CDP (CDS) de l'élément de services PS répond aux messages DHCP envoyés par les points BP dans le secteur LAN-Pass conformément aux exigences définies dans le § 7.3.3.1.4, "Fonction de serveur CDS – Exigences". La fonction de portail CMP du dispositif PS répond au message BP_Init reçu des points BP, comme décrit dans le § 6.3.3.4, "Fonction de messagerie LAN du portail CMP".

Le présent paragraphe décrit le processus d'approvisionnement lorsque le système NMS a approvisionné le dispositif PS de façon à fonctionner en mode primaire de traitement de paquet pour conversion C-NAT ou C-NAPT (voir le § 8). Il n'y a aucune différence, en terme de processus d'approvisionnement de point BP dans le secteur LAN-Trans, entre les modes d'approvisionnement DHCP et SNMP.

Le processus d'approvisionnement de point extrême dans le secteur LAN-Trans DOIT survenir par la séquence illustrée dans la Figure 13-7 et décrite en détail dans le Tableau 13-5.

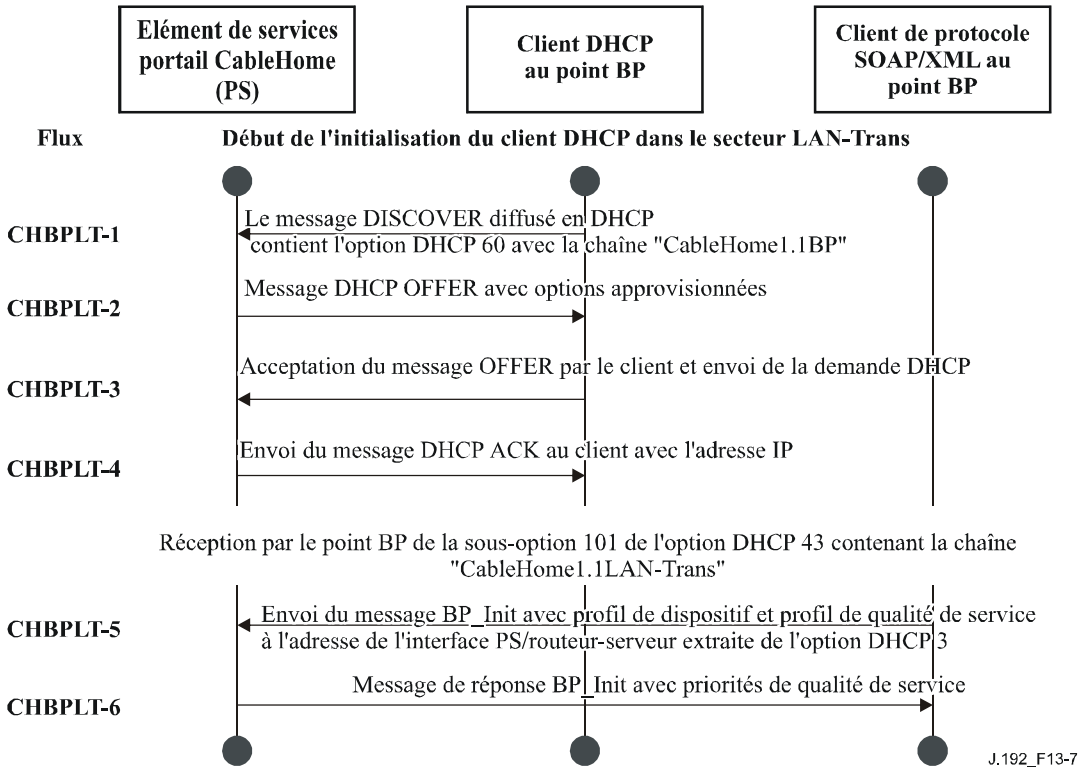


Figure 13-7/J.192 – Processus d'approvisionnement pour un point extrême dans le secteur LAN-Trans

Tableau 13-5/J.192 – Description des flux pour le processus d'approvisionnement de point BP dans le domaine LAN-Trans

Etape du flux	Approvisionnement d'adresse de client LAN-Trans	Séquence normale	Séquence d'échec
CHBPLT-1	Découverte diffusée par DHCP Le client du protocole DHCP (Note 1) envoie un message diffusé DHCP DISCOVER sur son réseau local (LAN) (Note 2). Le point BP est tenu d'inclure l'option DHCP 60 contenant la chaîne "CableHome1.1BP".	Passer à CHBPLT-2.	En cas d'échec selon le protocole DHCP, répéter CHBPLT-1.
CHBPLT-2	DHCP OFFER Le dispositif PS reçoit le message DHCP DISCOVER sur son interface avec un réseau LAN et examine le champ "chaddr". Si: – il y a une adresse LAN-Trans disponible; et – il n'y a aucune considération administrative qui motive le refus de l'adresse LAN-Trans au client; alors le dispositif PS DOIT envoyer un message DHCP OFFER au client afin de lui offrir l'adresse LAN-Trans soit par unidiffusion soit par diffusion sur liaison spécifique (conformément au bit BROADCAST du champ de fanions du message DHCP DISCOVER). Si le message DHCP DISCOVER incluait l'option DHCP 60 contenant la chaîne "CableHome1.1BP", le dispositif PS est tenu d'inclure la sous-option 101 de l'option DHCP 43 contenant la chaîne "CableHome1.1LANTrans" dans le message OFFER du message DHCP.	Passer à CHBPLT-3.	En cas d'échec, le client arrivera en fin de temporisation selon le protocole DHCP, et l'étape CHBPLT-1 sera répétée.
CHBPLT-3	DHCP REQUEST Le client DHCP du dispositif IP de réseau LAN reçoit le message DHCP OFFER. Quand un client DHCP du dispositif IP de réseau LAN souhaite accepter un message DHCP OFFER, on suppose qu'il va formater et envoyer un paquet DHCP REQUEST en utilisant la diffusion sur liaison spécifique (Note 3).	Passer à CHBPLT-4.	En cas d'échec, le client arrivera en fin de temporisation selon le protocole DHCP, et l'étape CHBPLT-1 sera répétée.

Tableau 13-5/J.192 – Description des flux pour le processus d'approvisionnement de point BP dans le domaine LAN-Trans

Etape du flux	Approvisionnement d'adresse de client LAN-Trans	Séquence normale	Séquence d'échec
CHBPLT-4	DHCP ACK Le dispositif PS reçoit la demande DHCP sur son interface avec un réseau LAN. Si l'adresse LAN-Trans indiquée continue à être assignable, le dispositif PS DOIT alors envoyer le message DHCP ACK au client, soit par unidiffusion soit par diffusion sur liaison spécifique (conformément au bit BROADCAST du champ de fanions du message DHCP REQUEST). Le message DHCP ACK comprend la sous-option 101 de l'option DHCP 43 avec la chaîne "CableHome1.1LAN-Trans". C'est une indication au point extrême qu'il est dans le secteur d'adresses du réseau LAN-Trans et qu'il a reçu l'adresse IP de l'interface PS/routeur-serveur dans l'option DHCP 3. Le point BP est donc tenu d'envoyer ses messages BP_Init à l'adresse IP de l'interface PS/routeur-serveur.	Passer à CHBPLT-5.	En cas d'échec, le client arrivera en fin de temporisation selon le protocole DHCP, et l'étape CHBPLT-1 sera répétée.
CHBPLT-5	BP_Init Le point BP envoie un message BP_Init de protocole SOAP/XML avec ses profils de dispositif et de qualité de service, à l'adresse IP de l'interface PS/routeur-serveur.	Passer à CHBPLT-6.	Si le point BP ne reçoit pas BP_Init_Response, il réessaye BP_Init pendant un total de trois tentatives.
CHBPLT-6	BP_Init_Response Le dispositif PS envoie un message BP_Init_Response de protocole SOAP/XML au point extrême.	Approvisionnement terminé.	
NOTE 1 – Si le client est informé de son adresse IP précédente (p. ex. après un réamorçage), il peut omettre le message DHCP DISCOVER et passer à l'étape 3. NOTE 2 – Si le client est situé sur un réseau sans diffusion, il est censé envoyer le message en unidiffusion au serveur DHCP. NOTE 3 – Si le client est situé sur un réseau sans diffusion, il est censé envoyer le message en unidiffusion aux services portail.			

13.7 Processus d'approvisionnement: dispositif IP de réseau LAN situé dans le secteur LAN-Pass

Certaines applications de réseau LAN 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 traversée (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 'traversée', ou lorsqu'il écrit les adresses MAC de dispositifs IP de réseau LAN individuels dans la table de traversée (objet cabhCapPassthroughTable). La Figure 13-8 décrit le processus de requête et d'attribution d'une adresse réseau à des dispositifs IP de réseau LAN pour lesquels le dispositif PS a été préconfiguré de façon à dériver le trafic. Quand le dispositif PS a été configuré de façon à dériver le trafic pour un dispositif IP de réseau LAN, les messages DHCP DISCOVER et REQUEST envoyés par ce dispositif IP de réseau LAN seront servis par le serveur DHCP du réseau câblé et non par le serveur CDS.

Un dispositif IP de réseau LAN non conforme à l'environnement IPCable2Home est censé implémenter un client du protocole DHCP et demander une location d'adresse IP par protocole DHCP [RFC 2131]. Un dispositif IP de réseau LAN conforme à l'environnement IPCable2Home, c'est-à-dire qui implémente 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. L'élément logique de point extrême d'un dispositif IP de réseau LAN conforme à l'environnement IPCable2Home est également tenu d'échanger des messages BP_Init avec le dispositif PS, comme décrit dans le § 6.5.3.2, "Fonction de messagerie LAN du point MBP". Le présent paragraphe décrit la messagerie BP requise. La messagerie DHCP censée intervenir entre un dispositif IP de réseau LAN non conforme et un serveur DHCP va normalement suivre les quatre premières étapes de la messagerie DHCP requise au point BP. Cependant, un dispositif IP de réseau LAN non conforme n'est pas susceptible d'inclure la chaîne d'option DHCP 61 "CableHome 1.1 BP <*adresse matérielle*>".

Le processus d'approvisionnement du dispositif IP de réseau LAN situé dans le secteur LAN-Pass est tenu d'intervenir par la séquence illustrée dans la Figure 13-8 et décrite en détail dans le Tableau 13-6.

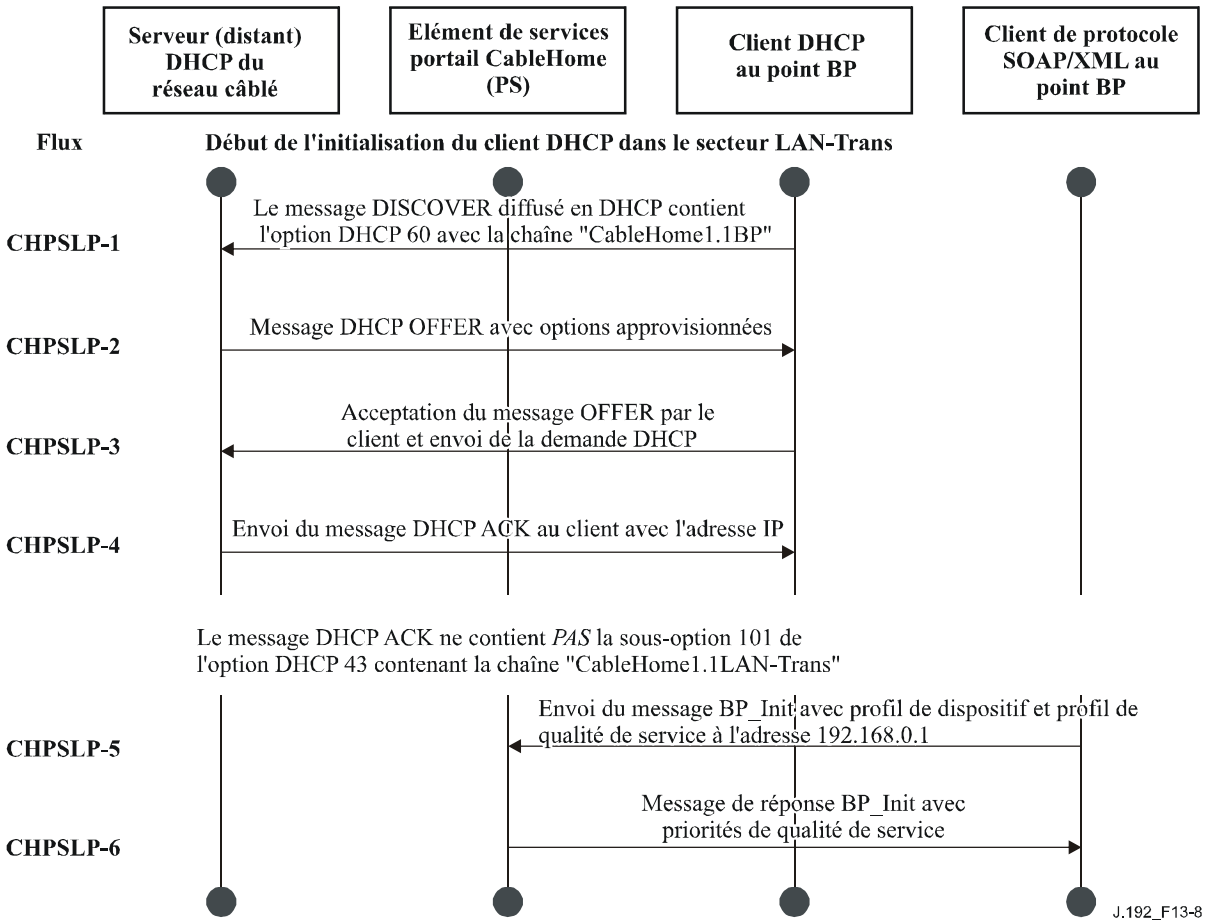


Figure 13-8/J.192 – Processus d'approvisionnement du dispositif IP de réseau LAN situé dans le secteur LAN-Pass

Tableau 13-6/J.192 – Description des flux pour le processus d'approvisionnement du dispositif IP de réseau LAN situé dans le secteur LAN-Pass

Etape du flux	Approvisionnement de l'adresse de traversée du client	Séquence normale	Séquence d'échec
CHPSLP-1	Découverte diffusée par DHCP Le point BP ou le dispositif IP de réseau LAN non conforme à l'environnement IPCable2Home diffuse un message DHCP DISCOVER sur son réseau local (LAN) (Note). Le dispositif PS reçoit le paquet diffusé DHCP DISCOVER sur son interface avec un réseau LAN et est tenu de dériver en transparence ce paquet vers l'interface avec un réseau WAN sans en changer le contenu. Voir § 8.3.4, "Exigences relatives au portail CAP".	Passer à CHPSLP-2.	En cas d'échec selon le protocole DHCP, répéter CHPSLP-1.
CHPSLP-2	DHCP OFFER Le serveur DHCP situé dans le réseau du câblo-opérateur reçoit le paquet DHCP DISCOVER et attribue une adresse IP accessible de l'extérieur avec les autres options, construit un paquet DHCP OFFER et transmet le message OFFER du protocole DHCP au dispositif IP de réseau LAN. Le dispositif PS est tenu de dériver en transparence le message OFFER du protocole DHCP de son interface avec un réseau WAN à son interface avec un réseau LAN sans changer le contenu du paquet IP. Voir § 8.3.4, "Exigences relatives au portail CAP".	Passer à CHPSLP-3.	En cas d'échec, le dispositif IP de réseau LAN arrivera en fin de temporisation selon le protocole DHCP, et l'étape CHPSLP-1 sera répétée.
CHPSLP-3	DHCP REQUEST Le dispositif IP de réseau LAN reçoit le message OFFER du protocole DHCP et envoie un message DHCP REQUEST. Le dispositif PS est tenu de dériver en transparence la demande DHCP, de son interface avec un réseau LAN à son interface avec un réseau WAN, sans changer le contenu du paquet IP. Voir § 8.3.4, "Exigences relatives au portail CAP".	Passer à CHPSLP-4.	En cas d'échec selon le protocole DHCP, répéter CHPSLP-1.

Tableau 13-6/J.192 – Description des flux pour le processus d'approvisionnement du dispositif IP de réseau LAN situé dans le secteur LAN-Pass

Etape du flux	Approvisionnement de l'adresse de traversée du client	Séquence normale	Séquence d'échec
CHPSLP-4	DHCP ACK Le serveur DHCP situé dans le réseau du câblo-opérateur reçoit la demande DHCP et envoie le message ACK du protocole DHCP au dispositif IP de réseau LAN avec l'adresse IPv4 du dispositif IP de réseau LAN. Le dispositif PS est tenu de dériver en transparence le message ACK du protocole DHCP, de son interface avec un réseau WAN à son interface avec un réseau LAN sans changer le contenu du paquet IP. Voir § 8.3.4, "Exigences relatives au portail CAP". Le message DHCP ACK est censé ne pas contenir la sous-option 101 de l'option DHCP 43 avec la chaîne "CableHome 1.1 LAN-Trans". Ce message signale au point BP qu'il est situé dans le secteur d'adresses du réseau LAN-Pass et qu'il n'a pas reçu l'adresse de l'interface PS/routeur-serveur dans l'option DHCP 3, de sorte qu'il est tenu d'envoyer ses messages BP_Init à l' adresse IP 192.168.0.1 "notoire" du dispositif PS. Voir § 6.5.3.2, "Fonction de messagerie LAN du point MBP".	Passer à CHPSLP-5.	En cas d'échec, le dispositif IP de réseau LAN arrivera en fin de temporisation selon le protocole DHCP, et l'étape CHPSLP-1 sera répétée.
CHPSLP-5	BP_Init Le point BP envoie un message BP_Init de protocole SOAP/XML avec ses profils de dispositif et de qualité de service, au dispositif PS.	Passer à CHPSLP-6.	Si le point BP ne reçoit pas BP_Init_Response, il réessaye BP_Init pendant un total de trois tentatives.
CHPSLP-6	BP_Init_Response Le dispositif PS envoie un message BP_Init_Response de protocole SOAP/XML, au point extrême.	Approvisionnement terminé	
NOTE – Si le client est situé sur un réseau sans diffusion, il doit envoyer le message en unidiffusion au serveur DHCP ou à l'agent-relais DHCP [RFC 3046] situé dans le réseau câblé.			

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 à la construction (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] système			
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
ifType	lecture seule	–	N/A
ifMtu	lecture seule	–	N/A
ifSpeed	lecture seule	–	N/A
ifPhysAddress	lecture seule	–	N/A
ifAdminStatus	lecture-écriture	Non	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

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
ipNetToMediaTable/ipNetToMediaEntry			
ipNetToMediaIfIndex	lecture-création	Non	N/A
ipNetToMediaPhyAddress	lecture-création	Non	N/A
ipNetToMediaNetAddress	lecture-création	Non	N/A

ipNetToMediaType	lecture-création	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
udpLocalPort	lecture seule	–	N/A

transmission [draft-ietf-ipcdn-bpiplus-mib-05] **docsIfMib** **docsBpi2MIB** **docsBpi2MIBObjects** **docsBpi2CmObjects**			
docsBpi2CmDeviceCertTable/docsBpi2CmDeviceCertEntry			
docsBpi2CmDeviceCmrt	lecture seule	–	N/A
docsBpi2CmDeviceManufCert	lecture seule	–	N/A
docsBpi2CodeDownloadGroup			
docsBpi2CodeDownloadStatusCode	lecture seule	–	N/A
docsBpi2CodeDownloadStatusString	lecture seule	–	N/A
docsBpi2CodeMfgOrgName	lecture seule	–	N/A
docsBpi2CodeMfgCodeAccessStart	lecture seule	–	N/A
docsBpi2CodeMfgCvcAccessStart	lecture seule	–	N/A
docsBpi2CodeCoSignerOrgName	lecture seule	–	N/A
docsBpi2CodeCoSignerCodeAccessStart	lecture seule	–	N/A
docsBpi2CodeCoSignerCvcAccessStart	lecture seule	–	N/A
docsBpi2CodeCvcUpdate	lecture-écriture	Oui	1
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
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
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	20
docsDevFilterIpControl	lecture-création	Oui	20
docsDevFilterIpIfIndex	lecture-création	Oui	20
docsDevFilterIpDirection	lecture-création	Non	N/A
docsDevFilterIpBroadcast	lecture-création	Non	N/A
docsDevFilterIpSaddr	lecture-création	Oui	20
docsDevFilterIpSmask	lecture-création	Oui	20
docsDevFilterIpDaddr	lecture-création	Oui	20
docsDevFilterIpDmask	lecture-création	Oui	20
docsDevFilterIpProtocol	lecture-création	Oui	20
docsDevFilterIpSourcePortLow	lecture-création	Oui	20
docsDevFilterIpSourcePortHigh	lecture-création	Oui	20
docsDevFilterIpDestPortLow	lecture-création	Oui	20
docsDevFilterIpDestPortHigh	lecture-création	Oui	20
docsDevFilterIpMatches	lecture seule	–	N/A
docsDevFilterIpTos	lecture-création	Non	N/A
docsDevFilterIpTosMask	lecture-création	Non	N/A
docsDevFilterIpContinue	lecture-création	Non	N/A
docsDevFilterIpPolicyId	lecture-création	Oui	20
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
cabhPsDevProvConfigFileSize	lecture seule	–	N/A
cabhPsDevWanDataMacAddress			
cabhPsDevTypeIdentifier	lecture seule	–	N/A
cabhPsDevSetToFactory	lecture-écriture	Non	N/A
cabhPsDevTodSyncStatus	lecture seule	–	N/A
cabhPsDevProvMode	lecture seule	–	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
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

cabhPsDevAttrib
cabhPsDevBpAttrib

cabhPsDevBpProfileTable/cabhPsDevBpProfileEntry			
cabhPsDevBpIndex	non accessible	–	N/A
cabhPsDevBpDeviceType	lecture seule	–	N/A
cabhPsDevBpManufacturer	lecture seule	–	N/A
cabhPsDevBpManufacturerURL	lecture seule	–	N/A
cabhPsDevBpSerialNumber	lecture seule	–	N/A
cabhPsDevBpHardwareVersion	lecture seule	–	N/A
cabhPsDevBpHardwareOptions	lecture seule	–	N/A
cabhPsDevBpModelName	lecture seule	–	N/A
cabhPsDevBpModelNumber	lecture seule	–	N/A
cabhPsDevBpModelURL	lecture seule	–	N/A
cabhPsDevBpModelUPC	lecture seule	–	N/A
cabhPsDevBpModelSoftwareOs	lecture seule	–	N/A
cabhPsDevBpModelSoftwareVersion	lecture seule	–	N/A
cabhPsDevBpLanInterface	lecture seule	–	N/A
cabhPsDevBpNumberInterfacePriorities	lecture seule	–	N/A
cabhPsDevBpPhysicalLocation	lecture seule	–	N/A
cabhPsDevBpPhysicalAddress	lecture seule	–	N/A

cabhPsDevPsStats

cabhPsDevLanIpTrafficResetCounters	lecture-écriture	Non	N/A
cabhPsDevLanIpTrafficCountersLastReset	lecture seule	–	N/A
cabhPsDevLanIpTrafficEnabled	lecture-écriture	Non	N/A

cabhPsDevLanIpTrafficTable/cabhPsDevLanIpTrafficEntry			
cabhPsDevLanIpTrafficIndex	non accessible	–	N/A
cabhPsDevLanIpTrafficInetAddressType	lecture seule	–	N/A
cabhPsDevLanIpTrafficInetAddress	lecture seule	–	N/A
cabhPsDevLanIpTrafficInOctets	lecture seule	–	N/A
cabhPsDevLanIpTrafficIpOutOctets	lecture seule	–	N/A

cabhSecMib
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	Oui	N/A
cabhSec2FwEventLastSetToFactory	lecture seule	Oui	N/A
cabhSec2FwPolicySuccessfulFileURL	lecture seule	Oui	1

cabhSec2FwEvent

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

cabhSec2FwLogEntry

cabhSec2FwLogIndex	non accessible	–	N/A
cabhSec2FwLogEventType	lecture seule	–	N/A
cabhSec2FwLogEventPriority	lecture seule	–	N/A
cabhSec2FwLogEventId	lecture seule	–	N/A
cabhSec2FwLogTime	lecture seule	–	N/A
cabhSec2FwLogIpProtocol	lecture seule	–	N/A
cabhSec2FwLogIpSourceAddr	lecture seule	–	N/A
cabhSec2FwLogIpDestAddr	lecture seule	–	N/A
cabhSec2FwLogIpSourcePort	lecture seule	–	N/A
cabhSec2FwLogIpDestPort	lecture seule	–	N/A
cabhSec2FwLogMessageType	lecture seule	–	N/A
cabhSec2FwLogReplayCount	lecture seule	–	N/A
cabhSec2FwLogMIBPointer	lecture seule	–	N/A

cabhSec2FwFilter **cabhSec2FwFilterScheduleTable** **cabhSec2FwFilterScheduleEntry**			
cabhSec2FwFilterScheduleIndex	non accessible	–	N/A
cabhSec2FwFilterScheduleRowStatus	lecture-création	Oui	1
cabhSec2FwFilterScheduleStartTime	lecture-création	Oui	1
cabhSec2FwFilterScheduleEndTime	lecture-création	Oui	1
cabhSec2FwFilterScheduleDOW	lecture-création	Oui	1
cabhSecCertObjects			
cabhSecCertPsCert	lecture seule	–	1
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
cabhCapMap			
cabhCapMappingTable/cabhCapMappingEntry			
cabhCapMappingIndex	non accessible	–	N/A
cabhCapMappingWanAddrType	lecture-création	Oui[2]	16
cabhCapMappingWanAddr	lecture-création	Oui[2]	16
cabhCapMappingWanPort	lecture-création	Oui[2]	16
cabhCapMappingLanAddrType	lecture-création	Oui[2]	16
cabhCapMappingLanAddr	lecture-création	Oui[2]	16
cabhCapMappingLanPort	lecture-création	Oui[2]	16
cabhCapMappingMethod	lecture seule	–	N/A
cabhCapMappingProtocol	lecture-création	Oui[2]	16
cabhCapMappingRowStatus	lecture-création	Oui	16
cabhCapPassthroughTable/cabhCapPassthroughEntry			
cabhCapPassthroughIndex	non accessible	–	N/A
cabhCapPassthroughMACAddr	lecture-création	Oui	16

[2] Les objets de type cabhCapMappingEntry sont persistants s'ils sont approvisionnés par le système NMS et non persistants s'ils sont créés dynamiquement sur la base du trafic sortant. Voir § 8.3.4.4.

cabhCapPassthroughRowStatus	lecture-création	Oui	16
cabhCdpMib **cabhCdpObjects** **cabhCdpBase**			
cabhCdpSetToFactory	lecture-écriture	Non	N/A
cabhCdpLanTransCurCount	lecture seule	–	N/A
cabhCdpLanTransThreshold	lecture-écriture	Non	N/A
cabhCdpLanTransAction	lecture-écriture	Non	N/A
cabhCdpWanDataIpAddrCount	lecture-écriture	Non	N/A
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/cabhCdpWanDataAddrEntry			
cabhCdpWanDataAddrIndex	non accessible	–	N/A
cabhCdpWanDataAddrClientId	lecture-création	Non	N/A
cabhCdpWanDataAddrIpType	lecture seule	–	N/A
cabhCdpWanDataAddrIp	lecture seule	–	N/A
cabhCdpWanDataAddrRenewalTime	lecture seule	–	N/A
cabhCdpWanDataAddrRowStatus	lecture-création	Non	N/A
cabhCdpWanDnsServerTable/cabhCdpWanDnsServerEntry			
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
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
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-écriture	Oui	1
cabhCdpServerDhcpAddress	lecture-écriture	Oui	1
cabhCtpMib **cabhCtpObjects** **cabhCtpBase**			
cabhCtpSetToFactory	lecture-écriture	Non	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
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
cabhCtpPingMinRTT	lecture seule	–	N/A
cabhCtpPingMaxRTT	lecture seule	–	N/A
cabhCtpPingNumIcmpError	lecture seule	–	N/A
cabhCtpPingIcmpError	lecture seule	–	N/A
cabhQosMib **cabhPriorityQosMibObjects** **cabhPriorityQosBase**			
cabhPriorityQosSetToFactory	lecture-écriture	Non	N/A
cabhPriorityQosLastReset	lecture seule	No	N/A
cabhPriorityQosMasterTable/cabhPriorityQosMasterEntry			
cabhPriorityQosMasterApplicationId	non accessible	–	N/A
cabhPriorityQosMasterDefaultCHPriority	lecture-création	Oui	16
cabhPriorityQosMasterRowStatus	lecture-création	Oui	16
cabhPriorityQosBp			
cabhPriorityQosBpTable/cabhPriorityQosBpEntry			
cabhPriorityQosBpIndex	non accessible	–	N/A
cabhPriorityQosBpIpAddrType	lecture seule	–	N/A
cabhPriorityQosBpIpAddr	lecture seule	–	N/A
cabhPriorityQosBpApplicationId	lecture seule	–	N/A
cabhPriorityQosBpDefaultCHPriority	lecture seule	–	N/A
cabhPriorityQosBpDestTable/cabhPriorityQosBpDestEntry			
cabhPriorityQosBpDestIndex	non accessible	–	N/A
cabhPriorityQosBpDestIpAddrType	lecture seule	–	N/A
cabhPriorityQosBpDestIpAddr	lecture seule	–	N/A
cabhPriorityQosBpDestPort	lecture seule	–	N/A
cabhPriorityQosBpDestIpPortPriority	lecture seule	–	N/A

cabhPriorityQosPs			
cabhPriorityQosPsIfAttribTable/cabhPriorityQosPsIfAttribEntry			
cabhPriorityQosPsIfAttribIfNumPriorities	lecture seule	–	N/A
cabhPriorityQosPsIfAttribIfNumQueues	lecture seule	–	N/A
experimental **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**			
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
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
SNMP-VIEW-BASED-ACM-MIB [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
snmpCommunityMIB [RFC 2576] **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
clabMfgCVCCert	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 transferts automatiques (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 que implémentée par la table locale d'événements dans le document [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 transfert 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 le document [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 transfert" 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 transfert
Erreurs DHCP avant l'achèvement de l'approvisionnement							
Initialiser	CDC	Critique	DHCP ECHOUE – flux DISCOVER envoyé, aucune offre reçue		D01.0	68000100	
Initialiser	CDC	Critique	DHCP ECHOUE – demande envoyée, aucune réponse		D02.0	68000200	
Initialiser	CDC	Critique	DHCP ECHOUE – 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 d'approvisionnement		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 l'approvisionnement							
Initialiser	ToD	Avertissement	Demande d'heure envoyée – aucune réponse reçue		D04.1	68000401	cabhPsDevInitTrap
Initialiser	ToD	Avertissement	Réponse ToD reçue – format de données non valide		D04.2	68000402	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 transfert
Erreurs TFTP avant l'achèvement de l'approvisionnement							
Initialiser	TFTP	Erreur	TFTP échoué – demande envoyée – Aucune réponse		D05.0	68000500	cabhPsDevInitTrap (Le transfert 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 (Le transfert n'est applicable qu'au mode d'approv. SNMP.)
Initialiser	TFTP	Erreur	TFTP échoué – Paquets dans le DESORDRE		D07.0	68000700	cabhPsDevInitTrap (Le transfert 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 (Le transfert n'est applicable qu'au mode d'approv. SNMP.)
Initialiser	TFTP	Erreur	TFTP échoué – nombre maximal de réessais dépassé	Pour SYSLOG seulement: ajouter: limite de réessais = <P1> P1 = nombre maximal de réessais	D09.0	68000900	cabhPsDevInitTrap (Le transfert 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 transfert
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		D20.0	68002000	
Initialiser	TLS	Critique	Connexion TLS expirée et nombre maximal de réessais dépassé		D21.0	68002100	
Initialiser	TLS	Critique	Erreur fatale TLS. <P1>	P1= code d'erreur à partir du document [RFC 2246]	D22.0	68002200	
HTTP							
Initialiser	HTTP	Critique	Téléchargement du fichier de configuration échoué, mais réessai prévu. Erreur HTTP. <P1>	P1= codes d'état à partir du document [RFC 2616]	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.		D31.0	68003100	
Initialiser	HTTP	Critique	Téléchargement sécurisé du fichier de configuration correctement achevé.		D32.0	68003200	

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 transfert
Analyse sémantique de TLV							
Initialiser	Analyse sémantique de TLV	Avertissement	TLV-28 – OID non reconnu		I401.0	73040100	cabhPsDevInit TLVUnknownTrap
Initialiser	Analyse sémantique de TLV	Avertissement	Inconnu TLV <P1>	Pour SYSLOG seulement, <P1> = le nuplet TLV complet en hexadécimal.	I401.1	73040101	cabhPsDevInitTLV UnknownTrap
Initialiser	Analyse sémantique de TLV	Erreur	Format/contenu de TLV non valide <P1>	Pour SYSLOG seulement, <P1> = le nuplet TLV complet en hexadécimal.	I401.2	73040102	
Approvisionnement							
Initialiser	Approvisionnement terminé	Remarque	Approvisionnement terminé	Pour SYSLOG seulement, ajouter MAC Addr: <P1>. P1 = adresse MAC du PS	I11.0	73001100	cabhPsDevInitTrap
Initialisation de mise à jour logicielle*							
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

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 transfert
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
Echec général de mise à jour logicielle*							
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

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 transfert
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
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

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 transfert
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
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*							
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

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 transfert
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
Echec DHCP après achèvement de l'approvisionnement							
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 l'approvisionnement							
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

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 transfert
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
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

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 transfert
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
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 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

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 transfert
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
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

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 transfert
Evénements de portail CSP							
CSP	Pare-feu	Remarque	Pare-feu de type 1 activé <P1> valeur MIB	P1 = valeur de l'objet cabhSecFwEventType 1Enable	P101.1	80010101	cabhPsDevCSPTrap
CSP	Pare-feu	Remarque	Pare-feu de type 2 activé <P1> valeur MIB	P1 = valeur de l'objet cabhSecFwEventType 2Enable	P101.2	80010102	cabhPsDevCSPTrap
CSP	Pare-feu	Remarque	Pare-feu de type 3 activé <P1> valeur MIB	P1 = valeur de l'objet cabhSecFwEventType 3Enable	P101.3	80010103	cabhPsDevCSPTrap
CSP	Pare-feu	Remarque	Pare-feu de type 4 activé <P1> valeur MIB	P1 = valeur de l'objet cabhSecFwEventType 4Enable	P101.4	80010104	cabhPsDevCSPTrap
CSP	Pare-feu	Remarque	Pare-feu de type 5 activé <P1> valeur MIB	P1 = valeur de l'objet cabhSecFwEventType 5Enable	P101.5	80010105	cabhPsDevCSPTrap
CSP	Pare-feu	Remarque	Pare-feu de type 6 activé <P1> valeur MIB	P1 = valeur de l'objet cabhSecFwEventType 6Enable	P101.6	80010106	cabhPsDevCSPTrap
CSP	Pare-feu	Avertissement	Pare-feu de type 1 – Evénement de dépassement de seuil		P102.1	80010201	cabhPsDevCSPTrap
CSP	Pare-feu	Avertissement	Pare-feu de type 2 – Evénement de dépassement de seuil		P102.2	80010202	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 transfert
CSP	Pare-feu	Avertissement	Pare-feu de type 3 – Evénement de dépassement de seuil		P102.3	80010203	cabhPsDevCSPTrap
CSP	Pare-feu	Avertissement	Pare-feu de type 4 – Evénement de dépassement de seuil		P102.4	80010204	cabhPsDevCSPTrap
CSP	Pare-feu	Avertissement	Pare-feu de type 5 – Evénement de dépassement de seuil		P102.5	80010205	cabhPsDevCSPTrap
CSP	Pare-feu	Avertissement	Pare-feu de type 6 – Evénement de dépassement de seuil		P102.6	80010206	cabhPsDevCSPTrap
CSP	Pare-feu TFTP	Critique	Téléchargement TFTP de Fichier de politique de pare-feu échoué: demande envoyée, aucune réponse.	P1 = URL du fichier de politique de pare-feu demandée	P130.0	80013000	cabhPsDevCSPTrap
CSP	Pare-feu TFTP	Critique	TFTP échoué – Fichier de politique de pare-feu non trouvé	P1 = URL du fichier de politique de pare-feu demandée	P131.0	80013100	cabhPsDevCSPTrap
CSP	Pare-feu TFTP	Critique	TFTP échoué – Fichier de politique de pare-feu non valide	P1 = URL du fichier de politique de pare-feu demandée	P132.0	80013200	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 transfert
CSP	Pare-feu TFTP	Critique	Téléchargement du fichier de politique de pare-feu achevé mais échec du contrôle du hachage SHA-1	P1 = URL du fichier de politique de pare-feu demandée, P2 = valeur du fichier de politique de pare-feu	P133.0	80013300	cabhPsDevCSPTrap
CSP	Pare-feu TFTP	Critique	Téléchargement du fichier de politique de pare-feu a dépassé le nombre maximal admissible de réessais TFTP	P1 = URL du fichier de politique de pare-feu demandée	P134.0	80013400	cabhPsDevCSPTrap
CSP	Pare-feu TFTP	Remarque	Téléchargement du fichier de politique de pare-feu TFTP réussi	P1 = URL du fichier de politique de pare-feu demandée Pour SYSLOG seulement: ajouter: limite de réessais = <P2> P2 = nombre maximal admissible 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

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 transfert
CAP	C-NAPT	Avertissement	CAP incapable d'effectuer le mappage C-NAPT. Aucune Adresse IP de réseau WAN disponible.		P250.0	80025000	cabhPsDevCAPTrap
Evénements de portail CTP							
CTP	Utilitaire de vitesse de connexion	Remarque	Essai par utilitaire de vitesse de connexion achevé avec succès	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	Essai par utilitaire de vitesse de connexion expiré	P1 = adresse IP d'origine P2 = adresse IP de destination P3 = protocole P4 = valeur de temporisateur (millisec)	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 transfert
CTP	Utilitaire de vitesse de connexion	Remarque	Essai par utilitaire de vitesse de connexion abandonné	P1 = adresse IP d'origine P2 = adresse IP de destination P3 = protocole P4 = valeur de temporisateur (millisec)	P303.0	80030300	cabhPsDevCtpTrap
CTP	Utilitaire de sondage par écho	Remarque	Essai par utilitaire de sondage par écho achevé avec succès	P1 = adresse IP d'origine P2 = adresse IP de destination P3 = temps moyen d'aller-retour	P320.0	80032000	cabhPsDevCtpTrap
CTP	Utilitaire de sondage par écho	Remarque	Essai par utilitaire de sondage par écho expiré	P1 = adresse IP d'origine P2 = adresse IP de destination P3 = nombre de demandes envoyées P4 = nombre de réponses reçues	P321.0	80032100	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 transfert
CTP	Utilitaire de sondage par écho	Remarque	Essai par utilitaire de sondage par écho abandonné	P1 = adresse IP d'origine P2 = adresse IP de destination P3 = nombre de demandes envoyées P4 = nombre de réponses reçues	P322.0	80032200	cabhPsDevCtpTrap
NOTE – Les événements de mise à jour logicielle (téléchargement sécurisé de logiciel) ne s'appliquent qu'aux services 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 transferts automatiques

Tous les transferts automatiques sont définis dans la spécification de base MIB PSDev (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:

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;

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.

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:

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;

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;

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;

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 régional (WAN) du pare-feu, mais elle n'empêche pas ce type d'attaques venant du côté domestique du pare-feu. Elle ne protège pas non plus contre le vol de service;

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 l'approvisionnement en service et pour les réservations de qualité de service (QoS).

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 points d'accès que le client en a besoin sans ouvrir de points d'accès qui ne sont pas requis pour la communication entre les réseaux LAN et WAN. La limitation d'ouverture de points d'accès et de sessions entre les réseaux LAN et WAN peut assurer une protection du réseau LAN domestique à l'encontre d'attaques. Si les points d'accès 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 LAN. 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 points d'accès.

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 passant par le pare-feu sont décrites en termes de protocoles, de numéros de point d'accès 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 à la construction des points d'accès 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 à la construction 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 points d'accès 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 CableHome fonctionne correctement. Les scénarios comprennent une définition "xxx à xxx" qui indique le nombre de serveurs locaux de réseau LAN qui communiquent avec des serveurs locaux de réseau WAN (p. ex. la définition "point à multipoint" indique qu'un seul serveur de réseau local (LAN) communique simultanément avec de nombreux serveurs locaux de réseau WAN). 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.

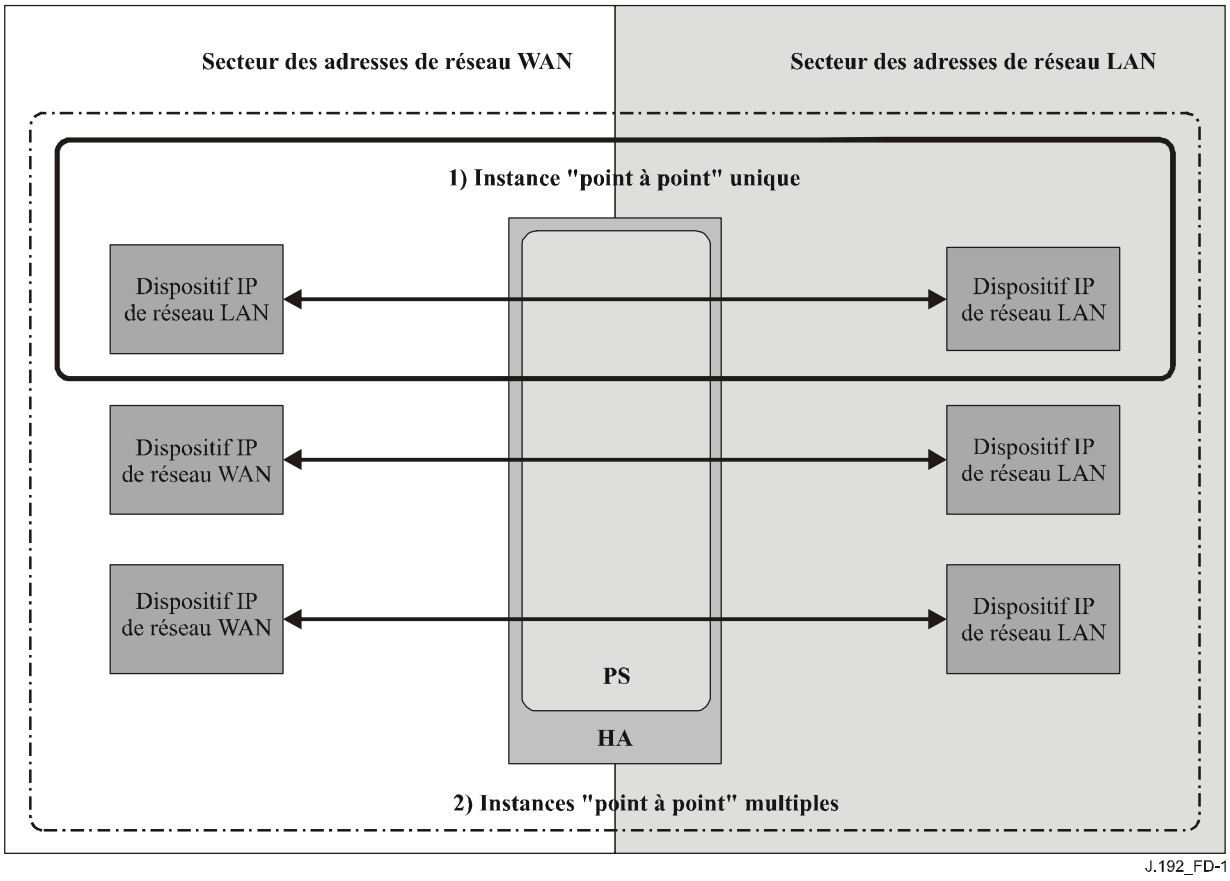


Figure D.1/J.192 – Scénarios "point à point"

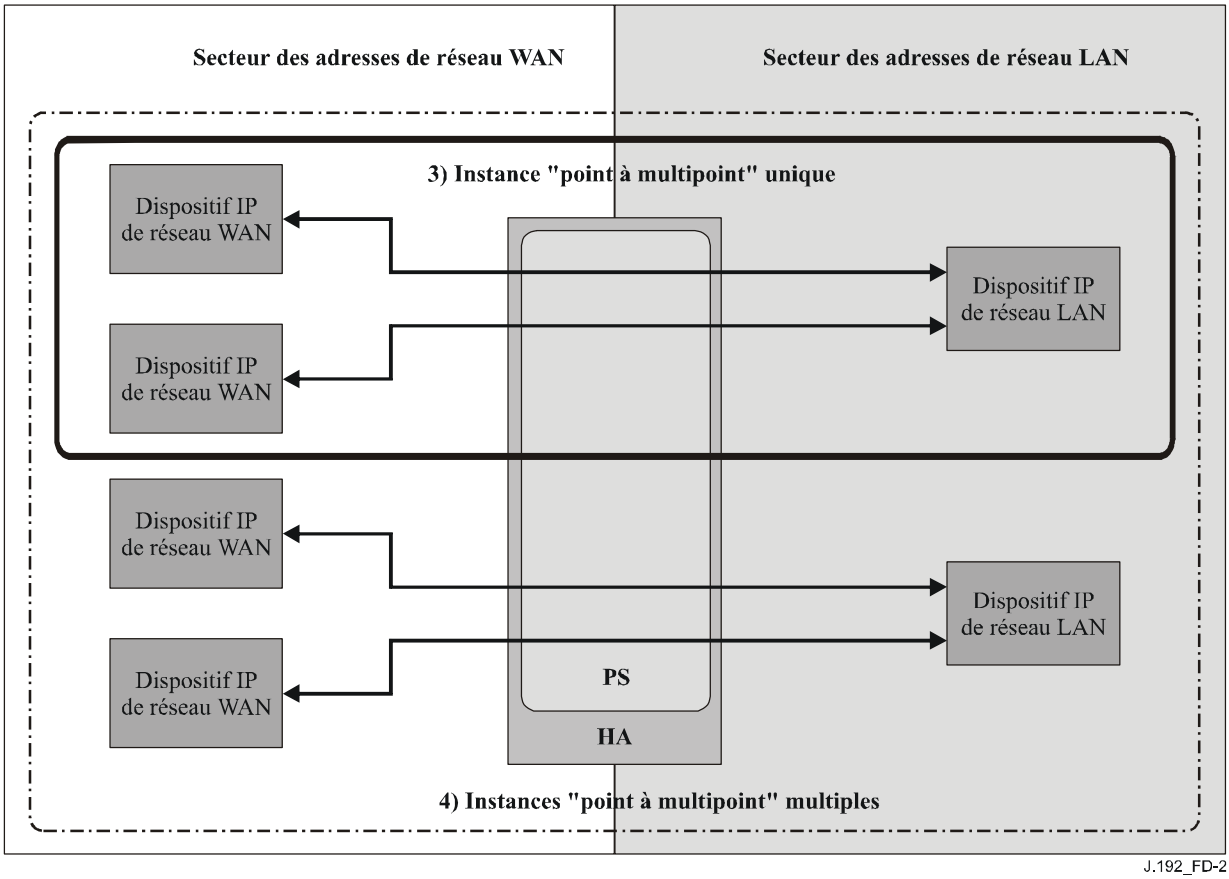


Figure D.2/J.192 – Scénarios "point à multipoint"

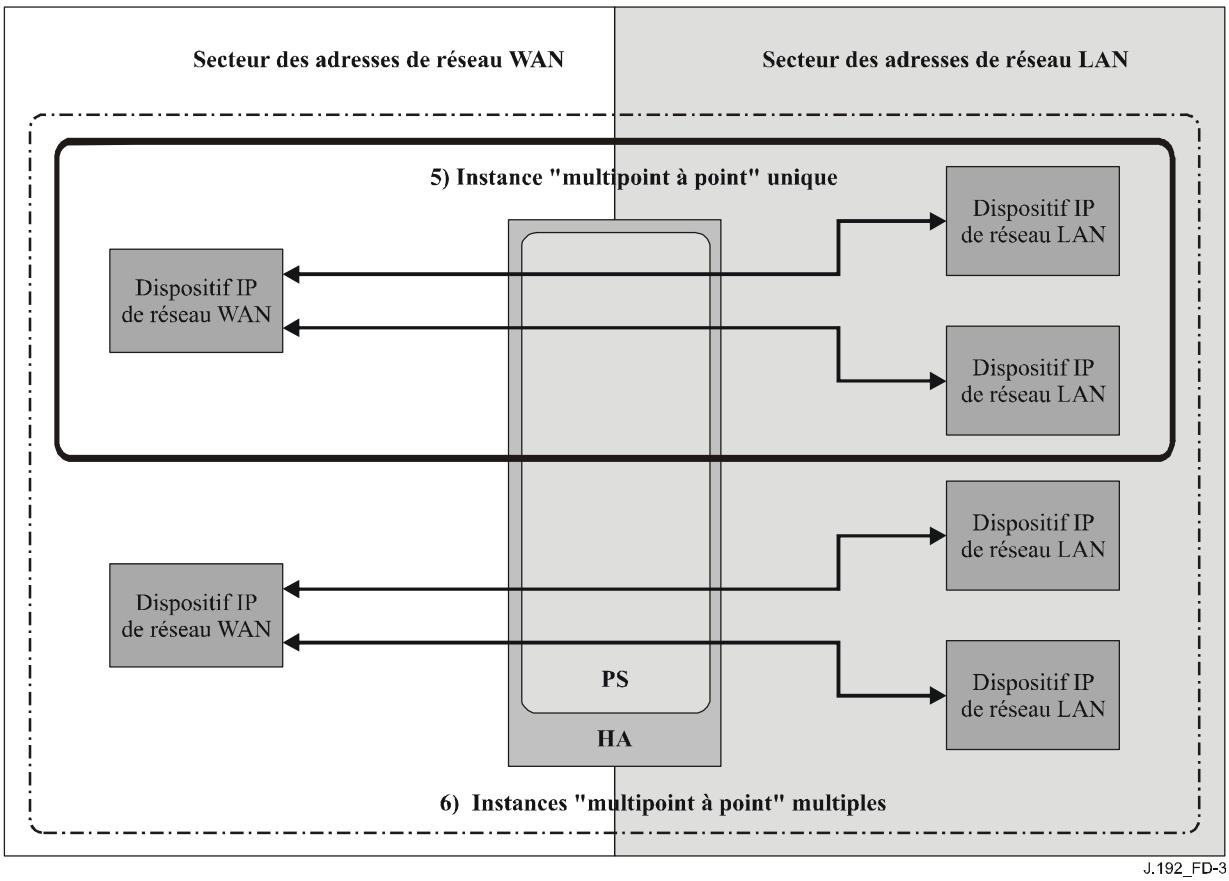


Figure D.3/J.192 – Scénarios "multipoint à point"

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 point d'accès 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 d'approvisionnement terminé 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	Points d'accès	Commentaire
AOL IM	TCP/5190, 5191, 5192, 5193 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 traversée) mode de traversée d'homologues IPCablecom et LAN
IRC	TCP/6665-6669	
Kerberos	1293	Secteur d'adresses IPCablecom et IPCable2Home du PS
L2TP	UDP/1701	

Tableau D.1/J.192 – Protocoles tenus d'opérer par conversion CAT et pare-feu CH

Application/Protocole	Points d'accès	Commentaire
MediaPlayer (Windows)	TCP/80;1755	
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	Point d'accès 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	Points d'accès	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 point d'accès 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

Appplication/ Protocole	Point d'accès	1) Relation point à point unique	2) Relation point à point multiples	3) Relation point à multipoint unique	4) Relation point à multipoint multiples	5) Relation multipoint à point unique	6) Relation multipoint à point 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 points d'accès 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 30000).	X	X	X	X			

Tableau D.2/J.192 – Applications qui nécessitent une politique de pare-feu et une passerelle ALG

Appplication/ Protocole	Point d'accès	1) Relation point à point unique	2) Relation point à point multiples	3) Relation point à multipoint unique	4) Relation point à multipoint multiples	5) Relation multipoint à point unique	6) Relation multipoint à point multiples	Commentaires
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 point d'accès 80 offre une performance inférieure à l'optimum.
Window Messenger (SIP)		X	X					Disponible sur Windows XP seulement

Annexe E

Bases MIB

E.1 Exigence relative à la base MIB de portail d'adressage IPCable2Home (CAP)

Exigences

La base MIB de portail CAP CableHome™ DOIT être implémentée comme défini ci-dessous.

```
CABH-CAP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Unsigned32          FROM SNMPv2-SMI
    TEXTUAL-CONVENTION,
    TruthValue,
    RowStatus,
    PhysAddress         FROM SNMPv2-TC
    OBJECT-GROUP,
    MODULE-COMPLIANCE   FROM SNMPv2-CONF
    InetAddressType,
    InetAddress,
    InetPortNumber      FROM INET-ADDRESS-MIB
    clabProjCableHome   FROM CLAB-DEF-MIB;

--============================================================================
--
--     Historique:
--
--     Date      Module modifié par:       Raison
--     04/05/02                            Edition I01
--     09/20/02                            Edition I02
--     04/11/03                            Edition I03
--
--============================================================================

cabhCapMib MODULE-IDENTITY
    LAST-UPDATED    "200304110000Z"--11 avril 2003
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Adresse postale: Cable Television Laboratories, Inc.
                 400 Centennial Parkway
                 Louisville, Colorado 80027-1266
                 Etats-Unis d'Amérique
            Tél: +1 303-661-9100
            Fax: +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
     "Le présent module de base MIB fournit les objets de gestion de base pour
     la portion de portail d'adressage CableHome (CAP) de la base de données PS.


        Remerciements:
        Roy Spitzer           -     Consultant à CableLabs
        Mike Mannette         -     Consultant à CableLabs
        Randy Dunton          -     Intel
```

```
        Dmitrii Loukianov     -     Intel
        Itay Sherman          -     Texas Instruments
        Chris Zacker          -     Broadcom
        Rick Vetter           -     Consultant à CableLabs
        John Bevilacqua       -     SOCIETE YAS"
    ::=  { clabProjCableHome 3 }

-- Conventions textuelles

CabhCapPacketMode ::= TEXTUAL-CONVENTION
       STATUS current
       DESCRIPTION
          "Type de données établi quand
          une association ou un mappage est établi."
       SYNTAX INTEGER {
          napt          (1),  -- Conversion NAT y compris point d'accès
          nat           (2),  -- Conversion NAT de base
          passthrough   (3)   -- Adresse externe de traversée
          }


cabhCapObjects      OBJECT IDENTIFIER ::= { cabhCapMib 1 }
cabhCapBase         OBJECT IDENTIFIER ::= { cabhCapObjects 1 }
cabhCapMap          OBJECT IDENTIFIER ::= { cabhCapObjects 2 }


--=====================================================================
--
--     Paramètres généraux de portail CAP
--
--=====================================================================

cabhCapTcpTimeWait OBJECT-TYPE
    SYNTAX Unsigned32
    UNITS "seconds"
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
    "Cet objet indique la durée maximale d'inactivité à attendre avant de
    considérer que la session TCP est fermée. Il n'a aucune relation avec l'état
    d'attente TIME_WAIT de session TCP auquel il est fait référence dans le
    document [RFC 793]"
    DEFVAL { 300 }
    ::= { cabhCapBase 1 }


cabhCapUdpTimeWait OBJECT-TYPE
       SYNTAX      Unsigned32
       UNITS        "seconds"
       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
        "Durée d'inactivité à attendre avant de détruire les mappages CAP pour le
        protocole UDP."
       DEFVAL { 300 }  -- 5 minutes
       ::={ cabhCapBase 2 }

cabhCapIcmpTimeWait OBJECT-TYPE
       SYNTAX      Unsigned32
       UNITS       "seconds"
       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
        "Durée d'inactivité à attendre avant de détruire
```

```
       les mappages CAP pour ICMP."
       DEFVAL { 300 }  --  5 minutes
       ::= { cabhCapBase 3 }


cabhCapPrimaryMode OBJECT-TYPE
    SYNTAX      CabhCapPacketMode
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
    "Mode primaire de traitement de paquet à utiliser."
    DEFVAL { napt }
    ::= { cabhCapBase 4 }

cabhCapSetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
      "La lecture de cet objet renvoie toujours la valeur false(2). Quand
      l'objet cabhCapSetToFactory est réglé à true(1), le dispositif PS doit
      effectuer les actions suivantes:

1.     Supprimer toutes les entrées dans les objets cabhCapMappingTable et
       cabhCapPassthroughTable.
2.     Réinitialiser les objets suivants à leur valeur par défaut à la
       construction:
                cabhCapTcpTimeWait,
                cabhCapUdpTimeWait,
                cabhCapIcmpTimeWait,
                cabhCapPrimaryMode."

     ::= { cabhCapBase 5 }

--------------------------------------------------------------------
--
--     cabhCapMappingTable (Table de mappage du portail CAP)
--
--     L'objet cabhCapMappingTable contient les informations pour tous les
--     mappages de portail CAP
--------------------------------------------------------------------

cabhCapMappingTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCapMappingEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
    "Cette table contient les mappages d'adresse IP entre des adresses de réseau
privé ou des adresses réseau avec des numéros de point d'accès/numéros de
séquence ICMP, attribuées à des dispositifs situés dans le réseau LAN domestique
de l'abonné, et entre des adresses réseau avec ou sans numéros de point
d'accès/numéros de séquence ICMP, attribuées par le câblo-opérateur et censées
être dans un sous-réseau distinct de ces adresses IP privées. La table de
mappage du portail CAP est utilisée par la fonction de portail d'adressage
CableHome (CAP) du dispositif PS afin de prendre des décisions de réexpédition
de paquet."
    ::= {  cabhCapMap 1 }

cabhCapMappingEntry OBJECT-TYPE
    SYNTAX      CabhCapMappingEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "Liste des mappages entre adresses IP de réseau privé (LAN)et adresses IP
```

```
      attribuées par le câblo-opérateur (WAN), mémorisés dans le dispositif PS
      et utilisés par le dispositif PS afin de prendre des décisions de
      réexpédition de paquet."
    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
      }

cabhCapMappingIndex    OBJECT-TYPE
    SYNTAX              INTEGER   (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "Indice pointant dans la table de mappage du portail CAP."
    ::= { cabhCapMappingEntry 1 }

    cabhCapMappingWanAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Type d'adresse IP attribuée du côté WAN"
    DEFVAL { ipv4 }
    ::= { cabhCapMappingEntry 2 }

cabhCapMappingWanAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
    "Adresse IP attribuée par le serveur (DHCP) d'adresses du câblo-opérateur
    et contenant l'adresse IP du côté WAN du nuplet de mappage au portail CAP.
    Cet objet est rempli soit dynamiquement par le trafic sortant de réseau LAN
    vers réseau WAN ou statiquement par le câblo-opérateur."

cabhCapMappingWanPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Numéro de point d'accès TCP/UDP ou numéro de séquence ICMP du côté WAN.
       Un numéro de point d'accès égal à 0 indique un mappage de conversion NAT.
       Un numéro de point d'accès différent de zéro indique un mappage de
       conversion NAPT."
    DEFVAL { 0 }
    ::= { cabhCapMappingEntry 4 }

cabhCapMappingLanAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Type d'adresse IP attribuée du côté LAN."
```

```
    DEFVAL { ipv4 }
    ::= { cabhCapMappingEntry 5 }

cabhCapMappingLanAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Adresse IP attribuée par la fonction de serveur DHCP du dispositif PS
       (serveur DHCP CableHome, serveur CDS) et contenant l'adresse IP du
       côté LAN du nuplet de mappage au portail CAP. Cet objet est rempli soit
       dynamiquement par suite du trafic sortant de LAN à WAN ou statiquement
       par le câblo-opérateur."
    ::= { cabhCapMappingEntry 6 }

cabhCapMappingLanPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
    "Numéro de point d'accès TCP/UDP ou numéro de séquence ICMP du côté LAN.
    Un numéro de point d'accès/numéro séquentiel égal à 0 indique un mappage de
    conversion NAT. Un numéro de point d'accès/numéro séquentiel différent de
    zéro indique un mappage de conversion NAPT."
    DEFVAL { 0 }
    ::= { cabhCapMappingEntry 7 }

cabhCapMappingMethod OBJECT-TYPE
    SYNTAX      INTEGER {
          static   (1),
          dynamic  (2)
          }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Indique comment ce mappage a été créé. La valeur 'static' signifie
       qu'il a été approvisionné et la valeur 'dynamic' signifie qu'il a été
       manipulé par le dispositif PS lui-même."
    ::= { cabhCapMappingEntry 8 }

cabhCapMappingProtocol OBJECT-TYPE
    SYNTAX      INTEGER {
          other   (1),  -- tout autre protocole; p. ex. IGMP
          icmp    (2),
          udp     (3),
          tcp     (4)
                  }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Protocole pour ce mappage."
    ::= { cabhCapMappingEntry 9 }

cabhCapMappingRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
"Verrouillage d'état de rangée pour la création et la suppression d'une entrée
d'objet cabhCapMappingTable. La modification de la valeur des colonnes d'adresse
IP ou de numéro de point d'accès dans la table de mappage du portail CAP peut
avoir une incidence sur le trafic actif, de sorte que le dispositif PS empêchera
la modification des colonnes de cette table et renverra une erreur de type
'inconsistentValue' quand l'objet cabhCapMappingRowStatus aura la valeur
```

```
active(1). Le dispositif PS NE DOIT PAS autoriser que l'élément RowStatus soit
mis à la valeur notInService(2) par un gestionnaire. Une rangée nouvellement
créée ne peut pas être mise à active(1) tant que les instances correspondantes
des objets cabhCapMappingWanAddrType, cabhCapMappingWanAddr,
cabhCapMappingLanAddrType, cabhCapMappingLanAddr et cabhCapMappingProtocol n'ont
pas été réglées. Si le mode primaire de traitement de paquet est NAPT (l'objet
cabhCapPrimaryMode est à napt(1)), une rangée nouvellement créée ne peut pas
être réglée à active(1)tant qu'une valeur différente de zéro n'a pas été donnée
aux objets cabhCapMappingWanPort et cabhCapMappingLanPort. Si le mode primaire
de traitement de paquet est NAT (l'objet cabhCapPrimaryMode est à nat(2)), une
rangée nouvellement créée ne peut pas être réglée à active(1) si une valeur
différente de zéro n'a pas été donnée aux objets cabhCapMappingWanPort et
cabhCapMappingLanPort."
    ::={ cabhCapMappingEntry 10 }

--========================================================================
--
--     cabhCapPassthroughTable (Table de traversée du portail CAP)
--
--     L'objet cabhCapPassthroughTable contient les adresses de commande MAC
--     pour tous les dispositifs IP de réseau LAN qui seront configurés en mode
--     de traversée.
--
--========================================================================

cabhCapPassthroughTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCapPassthroughEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
    "Cette table contient les adresses MAC pour tous les dispositifs IP
    de réseau LAN qui sont configurés en mode de traversée."
    ::= {  cabhCapMap 2 }

cabhCapPassthroughEntry OBJECT-TYPE
    SYNTAX      CabhCapPassthroughEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
    "Liste d'adresses matérielles des dispositifs IP de réseau LAN qui sont
    configurés en mode de traversée."
    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
    "Indice d'entrée dans la table de traversée du portail CAP."
    ::= { cabhCapPassthroughEntry 1 }

cabhCapPassthroughMacAddr           OBJECT-TYPE
    SYNTAX      PhysAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
    "Adresse matérielle du dispositif IP de réseau LAN à configurer en mode
```

```
    de traversée."
    ::={cabhCapPassthroughEntry 2}

cabhCapPassthroughRowStatus   OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
"Verrouillage d'état de rangée pour la création et la suppression d'une entrée
cabhCapPassthroughTable. Tout objet modifiable dans chaque rangée peut être
modifié à tout instant lorsque la rangée est à l'état active(1)."
    ::={cabhCapPassthroughEntry 3}
--
--  Ce groupe de notification fera l'objet d'extensions futures.
--

cabhCapNotification     OBJECT IDENTIFIER ::= { cabhCapMib 2 0 }
cabhCapConformance      OBJECT IDENTIFIER ::= { cabhCapMib 3 }
cabhCapCompliances      OBJECT IDENTIFIER ::= { cabhCapConformance 1 }
cabhCapGroups           OBJECT IDENTIFIER ::= { cabhCapConformance 2 }

--
--    Groupe de notifications
--


-- déclarations de conformité

cabhCapBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
    "Déclaration de conformité pour les dispositifs qui implémentent
    l'adaptateur MTA."
    MODULE   --cabhCapMib


-- groupes inconditionnellement obligatoires

MANDATORY-GROUPS {
    cabhCapGroup
    }

::= { cabhCapCompliances 1 }


cabhCapGroup OBJECT-GROUP
    OBJECTS {
          cabhCapTcpTimeWait,
          cabhCapUdpTimeWait,
          cabhCapIcmpTimeWait,
          cabhCapPrimaryMode,
          cabhCapSetToFactory,
          cabhCapMappingWanAddrType,
          cabhCapMappingWanAddr,
          cabhCapMappingWanPort,
          cabhCapMappingLanAddrType,
          cabhCapMappingLanAddr,
          cabhCapMappingLanPort,
          cabhCapMappingMethod,
          cabhCapMappingProtocol,
          cabhCapMappingRowStatus,
          cabhCapPassthroughMacAddr,
          cabhCapPassthroughRowStatus
          }
```

```
    STATUS    current
    DESCRIPTION
        "Groupe d'objets pour Base MIB de portail CAP CableHome."
    ::= { cabhCapGroups 1 }

END
```

E.2 Exigences de base MIB de portail DHCP IPCable2Home (CDP)

Exigences

La base MIB de portail CDP CableHome™ DOIT être implémentée comme défini ci-dessous.

```
CABH-CDP-MIB DEFINITIONS ::= BEGIN
IMPORTS
   MODULE-IDENTITY,
   OBJECT-TYPE,
   Integer32,
   Unsigned32                  FROM SNMPv2-SMI
   MacAddress,
   TruthValue,
   DateAndTime,
   RowStatus                   FROM SNMPv2-TC
   OBJECT-GROUP,
   MODULE-COMPLIANCE           FROM SNMPv2-CONF
   InetAddressType,
   InetAddress                 FROM INET-ADDRESS-MIB
   SnmpAdminString             FROM SNMP-FRAMEWORK-MIB
   clabProjCableHome           FROM CLAB-DEF-MIB;

   --================================================================
   --
   -- Historique:
   --
   --      Date         Module modifié par         Raison
   --      04/05/02                                édition I01
   --      09/20/02                                édition I02
   --      10/25/02                                Révisions par groupe IETF I-D
   --      04/11/03                                édition I03
   --
   --================================================================

   cabhCdpMib MODULE-IDENTITY
       LAST-UPDATED    "200304110000Z" -- 11 avril 2003
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Adresse postale:  Cable Television Laboratories, Inc.
             400 Centennial Parkway
             Louisville, Colorado 80027-1266
             Etats-Unis d'Amérique
            Tél: +1 303-661-9100
            Fax: +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
       "Le présent module de base MIB fournit les objets de gestion de base
       pour  la portion relative au portail DHCP CableHome (CDP) de la base
       de données PS.


            Remerciements:
            Roy Spitzer             -     Consultant à CableLabs
            Mike Mannette           -     Consultant à CableLabs
            Randy Dunton            -     Intel
```

```
            Dmitrii Loukianov       -     Intel
            Itay Sherman            -     Texas Instruments
            Chris Zacker            -     Broadcom
            Rick Vetter             -     Consultant à CableLabs
            John Bevilacqua         -     Société YAS"
    ::=  { clabProjCableHome 4 }


cabhCdpObjects    OBJECT IDENTIFIER ::= { cabhCdpMib 1 }
cabhCdpBase       OBJECT IDENTIFIER ::= { cabhCdpObjects 1 }
cabhCdpAddr       OBJECT IDENTIFIER ::= { cabhCdpObjects 2 }
cabhCdpServer     OBJECT IDENTIFIER ::= { cabhCdpObjects 3 }
--
--  Le groupe ci-dessous décrit les objets de base dans le portail DHCP
--  CableHome. Le reste de ce groupe traite des adresses définies
--  du côté LAN.

cabhCdpSetToFactory OBJECT-TYPE
    SYNTAX TruthValue
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
            "La lecture de cet objet renvoie toujours la valeur false(2).
            Quand l'objet cabhCdpSetToFactory est réglé à true(1),
            le dispositif PS doit effectuer les actions suivantes:
            1. supprimer toutes les entrées cabhCdpLanAddrEntries
               contenues dans la table d'adresses de réseau LAN
               du portail CDP.
            2. Le serveur CDS doit offrir les options DHCP par défaut
               à la construction à la prochaine échéance de renouvellement
               de location.
            3. réinitialisation des objets suivants à leur valeur par défaut
               à la construction:
            cabhCdpLanTransThreshold,
            cabhCdpLanTransAction,
            cabhCdpWanDataIpAddrCount,
            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
            "Nombre actuel de connexions louées actives dans la table
            cabhCdpLanAddrTable (nombre d'entrées de rangée dans la
            table qui ont une valeur d'objet cabhCdpLanAddrMethod égale à
            reservationActive(2) ou dynamicActive (4)). Ce décompte ne
            contient pas les connexions louées qui ont expiré ou les
            réservations non associées à une location actuelle."
    ::= { cabhCdpBase 2 }

cabhCdpLanTransThreshold OBJECT-TYPE
    SYNTAX INTEGER (0..65533)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Seuil numérique des adresses IP assignées ou attribuées
            dans le secteur LAN-Trans, au-dessus duquel le dispositif PS
            produit une condition d'alarme. Chaque fois que l'on essaie
            d'attribuer une adresse IP de réseau LAN-Trans quand le décompte
            cabhCdpLanTransCurCount est supérieur ou égal au seuil
            cabhCdpLanTransThreshold, un événement est produit. Une valeur
            égale à 0 indique que le portail CDP règle le seuil au plus grand
            nombre d'adresses de la réserve d'adresses du réseau LAN."
DEFVAL {0 }
::= { cabhCdpBase 3 }

cabhCdpLanTransAction OBJECT-TYPE
    SYNTAX INTEGER {
    normal (1),
    noAssignment (2)
    }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Action effectuée quand le serveur CDS attribue une
            adresse LAN-Trans et quand le nombre d'adresses LAN-Trans
            attribuées (objet cabhCdpLanTransCurCount) est supérieur
            au seuil (objet cabhCdpLanTransThreshold). Cette action
            est la suivante:
            'normal' - attribuer une adresse IP de réseau LAN-Trans
            comme ce serait normalement le cas si le seuil n'avait
            pas été dépassé.
            'noAssignment' - ne pas attribuer d'adresse IP de réseau LAN-Trans."
DEFVAL { normal }
::= { cabhCdpBase 4 }

cabhCdpWanDataIpAddrCount OBJECT-TYPE
    SYNTAX INTEGER ( 0..63 )
    MAX-ACCESS read-write
    STATUS     current
    DESCRIPTION
            "Nombre d'adresses IP de réseau WAN-Data que le
             client CDC du PS doit essayer d'acquérir par
             protocole DHCP."
DEFVAL {0 }
::= { cabhCdpBase 5 }
--
--     Tables de gestion d'adresses au portail CDP
--
--================================================================
--
--     cabhCdpLanAddrTable (Tables d'adresses LAN au portail CDP)
--
--     L'objet cabhCdpLanAddrTable contient les paramètres DHCP
```

```
--     pour chaque adresse IP servie au secteur LAN-Trans.
--
--     Cette table contient une liste des entrées pour les paramètres de
--     portail CDP du côté LAN. Ces paramètres peuvent être réglés soit
--     par le portail CDP ou par le câblo-opérateur au moyen du portail CMP.
--==========================================================================

cabhCdpLanAddrTable OBJECT-TYPE
       SYNTAX      SEQUENCE OF CabhCdpLanAddrEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
             "Cette table est une liste des paramètres de secteur LAN-Trans.
             Elle possède une seule entrée de rangée pour chaque adresse IP
             de réseau LAN-Trans assignée. Chaque rangée doit avoir au moins
             une valeur valide d'objet cabhCdpLanAddrMethod, une valeur d'objet
             cabhCdpLanAddrIpType, une valeur unique d'objet cabhCdpLanAddrIp et
             une valeur unique d'objet cabhCdpLanAddrClientId.
             Attribution d'adresse statique/manuelle: afin de créer une
             nouvelle réservation d'adresse DHCP, le système NMS crée une
             rangée avec:
             -   un indice composé d'un nouvelle adresse cabhCdpLanAddrIp
                 avec son type cabhCdpLanAddrIpType;
             -   un nouvel identificateur unique cabhCdpLanAddrClientID;
             -   (des champs LeaseCreateTime et LeaseExpireTime vides);
             -   et un état cabhCdpLanDataAddrRowStatus de valeur
                 CreateAndGo(4).
             Si la syntaxe et les valeurs de la nouvelle rangée -indiquant
             une réservation- sont valides, le dispositif PS doit mettre
             l'objet cabhCdpLanAddrMethod à la valeur reservationInactive(1)
             et l'objet     cabhCdpLanDataAddrRowStatus à la valeur active(1).
             Quand le dispositif PS accorde une location pour une adresse IP
             réservée, il doit régler l'objet cabhCdpLanAddrMethod à
             reservationActive(2) pour cette rangée. Quand une location pour
             une adresse IP réservée arrive à expiration, le dispositif PS doit
             régler l'objet cabhCdpLanAddrMethod à reservationInactive(1)
             pour la rangée correspondante. Pour les entrées de rangée qui
             représentent des réservations de location -les rangées dans
             lesquelles l'objet cabhCdpLanAddrMethod a une valeur
             reservationInactive(1)ou reservationActive(2)- la valeur des
             objets cabhCdpLanAddrIpType, cabhCdpLanAddrIp,
             cabhCdpLanAddrClientID, cabhCdpLanAddrMethod et
             cabhCdpLanAddrHostName DOIT persister au-delà des
             réamorçages du dispositif PS.
             Attribution dynamique d'adresse: quand le dispositif PS
             accorde une location pour une adresse IP non réservée,
             il doit régler l'objet cabhCdpLanAddrMethod pour cette
             rangée à dynamicActive(4). Quand une location pour
             une adresse IP non réservée arrive à expiration,
             le dispositif PS doit régler l'objet cabhCdpLanAddrMethod
             de la rangée correspondante à dynamicInactive(3). Le PS
             doit créer de nouvelles entrées de rangée au moyen de
             valeurs d'objet cabhCdpLanAddrIp qui sont uniques dans
             cette table. Si toutes les valeurs cabhCdpLanAddrIp contenues
             dans l'étendue définie par cabhCdpLanPoolStart et cabhCdpLanPoolEnd
             sont utilisées dans cette table, le dispositif PS peut remplacer
             par surécriture l'identificateur cabhCdpLanAddrClientId -d'une
             rangée qui a un objet cabhCdpLanAddrMethod ayant une valeur
             dynamicInactive(3)- par une nouvelle valeur de
             cabhCdpLanAddrClientId et utiliser cette adresse cabhCdpLanAddrIp
             en tant que partie d'une nouvelle location. Pour les entrées de
             rangée qui représentent des connexions louées actives -rangées dans
             lesquelles l'objet cabhCdpLanAddrMethod a une valeur égale à
             dynamicActive(4)- la valeur des objets cabhCdpLanAddrIpType,
```

```
            cabhCdpLanAddrIp, cabhCdpLanAddrClientID, cabhCdpLanAddrMethod
            et cabhCdpLanAddrHostName doit persister au-delà des réamorçages."
        ::= {  cabhCdpAddr 1 }

    cabhCdpLanAddrEntry OBJECT-TYPE
        SYNTAX      CabhCdpLanAddrEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "Liste de paramètres généraux applicables à des réservations
            et locations d'adresse IP de secteur LAN-Trans"
        INDEX { cabhCdpLanAddrIpType, cabhCdpLanAddrIp }
        ::= { cabhCdpLanAddrTable 1 }

    CabhCdpLanAddrEntry ::= SEQUENCE {
       cabhCdpLanAddrIpType                InetAddressType,
       cabhCdpLanAddrIp                    InetAddress,
       cabhCdpLanAddrClientID              MacAddress,
       cabhCdpLanAddrLeaseCreateTime       DateAndTime,
       cabhCdpLanAddrLeaseExpireTime       DateAndTime,
       cabhCdpLanAddrMethod                INTEGER,
       cabhCdpLanAddrHostName              SnmpAdminString,
       cabhCdpLanAddrRowStatus             RowStatus
        }

    cabhCdpLanAddrIpType OBJECT-TYPE
        SYNTAX      InetAddressType
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "Type d'adresse IP attribuée au dispositif IP de réseau LAN
                dans le secteur LAN-Trans."
        ::= { cabhCdpLanAddrEntry 1 }

    cabhCdpLanAddrIp OBJECT-TYPE
        SYNTAX      InetAddress
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
        "Adresse attribuée au dispositif IP de réseau LAN.
        Ce paramètre est introduit par le portail CDP quand le serveur CDS
        accorde une location à un dispositif IP de réseau LAN situé dans le
        secteur LAN-Trans, et crée une rangée dans cette table.
        En variante, ce paramètre peut être introduit par le système NMS
        au moyen du portail CMP, quand le système NMS crée une nouvelle
        réservation DHCP d'adresse. Chaque adresse cabhCdpLanAddrIp contenue
        dans la table doit s'inscrire dans l'étendue d'adresses IP définie
        expressément par les objets cabhCdpLanPoolStart et cabhCdpLanPoolEnd.
        Le dispositif PS doit renvoyer une erreur de type inconsistentValue
        si le système NMS essaye de créer une entrée de rangée avec une valeur
        d'objet cabhCdpLanAddrIP qui tombe en dehors de cette étendue ou qui
        n'est pas unique par rapport à toutes les entrées cabhCdpLanAddrIP
        existant dans cette table. Le type d'adresse de cet objet est spécifié
        par cabhCdpLanAddrIpType."
        ::= { cabhCdpLanAddrEntry 2 }

    cabhCdpLanAddrClientID OBJECT-TYPE
        SYNTAX           MacAddress
        MAX-ACCESS       read-create
        STATUS           current
        DESCRIPTION
"Adresse matérielle du client (c'est-à-dire du dispositif IP de réseau LAN)
comme indiqué dans le champ "chaddr" de son message DHCP REQUEST. Il y a une
relation univoque entre l'adresse matérielle et le dispositif IP de réseau LAN.
```

```
Ce paramètre est introduit par le dispositif PS (CDP) quand le serveur CDS
accorde une location à un dispositif IP de réseau LAN situé dans le secteur LAN-
Trans, et crée une rangée dans cette table. En variante, ce paramètre peut être
créé par le système NMS au moyen du portail CMP quand le système NMS crée une
nouvelle réservation DHCP d'adresse en accédant à l'objet
cabhCdpLanDataAddrRowStatus avec un indice composé d'une adresse unique
cabhCdpLanAddrIp et en créant une rangée avec un identificateur unique
cabhCdpLanAddrClientID."
       ::= { cabhCdpLanAddrEntry 3 }

   cabhCdpLanAddrLeaseCreateTime OBJECT-TYPE
       SYNTAX      DateAndTime
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
          "Date et heure auxquelles la location a été créée
          dans le réseau LAN-Trans (si elle n'a pas encore été renouvelée)
          ou auxquelles elle a été renouvelée en dernier."
       ::= { cabhCdpLanAddrEntry 4 }

   cabhCdpLanAddrLeaseExpireTime OBJECT-TYPE
       SYNTAX      DateAndTime
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
          "Date et heure auxquelles la location a expiré ou va expirer
          dans le réseau LAN-Trans."
       ::= { cabhCdpLanAddrEntry 5 }

   cabhCdpLanAddrMethod OBJECT-TYPE
       SYNTAX      INTEGER {
      reservationInactive (1),
      reservationActive (2),
      dynamicInactive (3),
      dynamicActive (4)
      }
      MAX-ACCESS  read-only
       STATUS     current
       DESCRIPTION
          "Méthode d'attribution d'adresse IP indiquée par cette rangée.
          La valeur reservationInactive(1)indique une adresse IP réservée
          qui n'a pas encore été louée ou dont la location a expiré.
          La valeur reservationActive(2) indique une adresse IP réservée
          qui a une location active. La valeur dynamicInactive(3) indique
          une adresse IP qui a été une fois attribuée dynamiquement à un
          dispositif LAN-Trans mais dont la location actuelle a expiré.
          La valeur dynamicActive(4) indique une adresse IP qui a été
          attribuée dynamiquement à un dispositif LAN-Trans qui a une
          location actuelle."
      ::= { cabhCdpLanAddrEntry 6 }

   cabhCdpLanAddrHostName OBJECT-TYPE
       SYNTAX      SnmpAdminString(SIZE(0..80))
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
          "Nom du serveur local d'adresses IP de réseau LAN, sur la
          base de l'option DHCP 12."
          option 12."
       ::= { cabhCdpLanAddrEntry 7 }

   cabhCdpLanAddrRowStatus OBJECT-TYPE
       SYNTAX      RowStatus
       MAX-ACCESS  read-create
```

```
        STATUS      current
        DESCRIPTION
    "Verrouillage d'état de rangée pour création et suppression
    d'entrées de rangée.
    Le dispositif PS ne doit pas permettre au système NMS de mettre
    à jour (SET) l'objet RowStatus à la valeur notInService(2).
    Le dispositif PS doit attribuer un objet RowStatus de valeur notInService(2)
    à toute nouvelle entrée de rangée créée avec une valeur d'identificateur non
    unique dans l'objet cabhCdpLanAddrClientID.
    Le dispositif PS doit attribuer un objet RowStatus de valeur notReady(3)
    à toute nouvelle entrée de rangée créée sans identificateur
    cabhCdpLanAddrClientID. Le dispositif PS empêchera la modification
    des colonnes de cette table et renverra une erreur de type inconsistentValue
    si le système NMS essaye de créer de telles modifications alors que la valeur
    de l'objet RowStatus est active(1)."
        ::= { cabhCdpLanAddrEntry 8 }

--================================================================================
--
--      cabhCdpWanDataAddrTable (Tables d'adresses de réseau WAN-Data
        du portail CDP)
--
--      L'objet cabhCdpWanDataAddrTable contient les paramètres de
--      configuration ou DHCP pour chaque mappage d'adresse IP
--      sur une adresse IP de réseau WAN-Data.
--
--================================================================================

cabhCdpWanDataAddrTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCdpWanDataAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Cette table contient des informations de secteur d'adresses
            de réseau WAN-Data."
    ::= {  cabhCdpAddr 2 }

cabhCdpWanDataAddrEntry OBJECT-TYPE
    SYNTAX      CabhCdpWanDataAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Liste de paramètres généraux pour secteur d'adresses
        de réseau WAN-Data de portail CDP."
    INDEX { cabhCdpWanDataAddrIndex }
    ::= { cabhCdpWanDataAddrTable 1 }

CabhCdpWanDataAddrEntry ::= SEQUENCE {
       cabhCdpWanDataAddrIndex       INTEGER,
       cabhCdpWanDataAddrClientId    OCTET STRING,
       cabhCdpWanDataAddrIpType      InetAddressType,
       cabhCdpWanDataAddrIp          InetAddress,
       cabhCdpWanDataAddrRenewalTime Integer32,
       cabhCdpWanDataAddrRowStatus   RowStatus
    }


cabhCdpWanDataAddrIndex OBJECT-TYPE
    SYNTAX      INTEGER (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "Indice de pointage dans la table."
    ::= { cabhCdpWanDataAddrEntry 1 }
```

```
cabhCdpWanDataAddrClientId OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE (1..80))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
"Unique identificateur de client de réseau WAN-Data utilisé lors d'une tentative
d'acquisition d'une adresse IP de réseau WAN-Data par protocole DHCP."
    ::= { cabhCdpWanDataAddrEntry 2 }

cabhCdpWanDataAddrIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Type d'adresse attribuée du côté WAN-Data."
    DEFVAL { ipv4 }
    ::= { cabhCdpWanDataAddrEntry 3 }

cabhCdpWanDataAddrIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Adresse attribuée du côté WAN-Data."
    ::= { cabhCdpWanDataAddrEntry 4 }

cabhCdpWanDataAddrRenewalTime OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Durée restant avant que la location arrive à expiration.
       Cette valeur est fondée sur l'option DHCP 51."
    ::= { cabhCdpWanDataAddrEntry 5 }

cabhCdpWanDataAddrRowStatus OBJECT-TYPE
       SYNTAX      RowStatus
       MAX-ACCESS  read-create
       STATUS      current
       DESCRIPTION
          "Verrouillage d'état de rangée pour création et suppression
          d'entrées de rangée. Tout objet remplaçable par surécriture
          dans une rangée peut être modifié à tout instant alors que
          la rangée est à la valeur active(1). Le dispositif PS doit
          attribuer un objet RowStatus de valeur notInService(2) à
          toute nouvelle entrée de rangée créée avec un objet
          cabhCdpWanDataAddrClientId qui n'est pas unique dans
          cette table."

       ::= { cabhCdpWanDataAddrEntry 6 }
--================================================================
--
-- cabhCdpWanDnsServerTable (Table de serveur DNS du réseau WAN-Data
-- au portail CDP)
--
-- L'objet cabhCdpWanDnsServerTable est une table de 3 serveurs DNS
-- de réseau câblé et de réseau Internet.
--
--================================================================
cabhCdpWanDnsServerTable OBJECT-TYPE
        SYNTAX SEQUENCE OF CabhCdpWanDnsServerEntry
        MAX-ACCESS      not-accessible
        STATUS          current
```

```
        DESCRIPTION
        "Cette table contient les adresses IP des serveurs DNS
        de réseau câblé et de réseau Internet, dans l'ordre de
        préférence où le portail CNP du dispositif PS va les
        rechercher quand il ne peut pas résoudre une interrogation DNS
        au moyen d'informations locales. Les entrées contenues dans cette
        table sont mises à jour avec les informations contenues dans
        l'option DHCP 6, reçue pendant les deux processus d'acquisition
        d'adresse IP dans les réseaux WAN-Man et WAN-Data."
::= { cabhCdpAddr 3 }

cabhCdpWanDnsServerEntry OBJECT-TYPE
        SYNTAX CabhCdpWanDnsServerEntry
        MAX-ACCESS      not-accessible
        STATUS    current
        DESCRIPTION
        "Liste de serveurs DNS de réseau câblé et de réseau Internet."
        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
        "Ordre de préférence pour les serveurs DNS de réseau câblé
        et de réseau Internet, comme énumérés dans l'option DHCP 6
        (serveur de domaine). Chaque fois que le client CDC reçoit des
        informations d'adresse IP valides dans l'option DHCP 6, dans
        le cadre de l'acquisition ou du renouvellement de location
        d'une adresse IP de réseau WAN-Man ou WAN-Data, ce client
        doit mettre à jour ces informations dans cette table.
        Etant donné que les entrées dans l'option DHCP 6 sont énumérées
        dans l'ordre de préférence,l'entrée de priorité la plus élevée
        dans l'option DHCP 6 doit correspondre à la rangée ayant un objet
        cabhCdpWanDnsServerOrder de valeur égale à 1. Si l'option DHCP 6
        contient 2 adresses IP valides, le dispositif PS doit mettre à jour
        les rangées en mettant l'objet cabhCdpWanDnsServerOrder aux valeurs 1
        et 2.
        Si l'option DHCP 6 contient 3 adresses IP valides, le dispositif PS
        doit mettre à jour les rangées en mettant l'objet
        cabhCdpWanDnsServerOrder aux valeurs de 1, 2, et 3.
        Les éventuelles informations de serveur DNS incluses
        dans l'option DHCP 6 au-delà des noms primaires, secondaires
        et tertiaires ne seront pas représentées dans cette table."
::= { cabhCdpWanDnsServerEntry 1 }

cabhCdpWanDnsServerIpType OBJECT-TYPE
        SYNTAX      InetAddressType
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
        "Ce paramètre indique le type d'adresse IP d'un serveur DNS
        de réseau WAN".
```

```
        DEFVAL { ipv4 }
::= { cabhCdpWanDnsServerEntry 2 }

cabhCdpWanDnsServerIp OBJECT-TYPE
        SYNTAX      InetAddress
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
        "Ce paramètre indique l'adresse IP d'un Serveur DNS
        de réseau WAN. Le type de cette adresse est spécifié
        par l'objet cabhCdpWanDnsServerIpType."
        ::= { cabhCdpWanDnsServerEntry 3 }

--
--     "Valeurs d'option du côté serveur DHCP (CDS) pour le secteur LAN Trans."
--
cabhCdpLanPoolStartType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Type d'adresse du début de liste d'adresses IP de réseau LAN-Trans."
      DEFVAL { ipv4 }
    ::= { cabhCdpServer 1 }

cabhCdpLanPoolStart OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
   "Début de liste d'adresses IP de réseau LAN-Trans."
      DEFVAL { 'c0a8000a'h } -- 192.168.0.10
      -- 192.168.0.0 est le numéro du réseau
      -- 192.168.0.255 est l'adresse de diffusion et l'adresse
      -- 192.168.0.1 est réservée pour le routeur
    ::= { cabhCdpServer 2 }

cabhCdpLanPoolEndType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Type d'adresse de la fin de liste d'adresses IP de réseau LAN-Trans."
      DEFVAL { ipv4 }
    ::= { cabhCdpServer 3 }

cabhCdpLanPoolEnd OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Fin de liste d'adresses IP dans le secteur LAN-Trans."
      DEFVAL { 'c0a800fe'h } -- 192.168.0.254
    ::= { cabhCdpServer 4 }

cabhCdpServerNetworkNumberType      OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
  "Type d'adresse IP du numéro de réseau dans le secteur LAN-Trans."
         DEFVAL  { ipv4 }
    ::= { cabhCdpServer 5 }
```

```
cabhCdpServerNetworkNumber          OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
          "Numéro de réseau dans le secteur LAN-TRANS."
       DEFVAL  { 'c0a80000'h }
    ::= { cabhCdpServer 6 }

cabhCdpServerSubnetMaskType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Type de masque de sous-réseau dans le secteur LAN-TRANS."
       DEFVAL { ipv4 }
    ::= { cabhCdpServer 7 }

cabhCdpServerSubnetMask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
         "Valeur d'option 1 – Valeur de masque de sous-réseau
         dans le secteur LAN-TRANS."
       DEFVAL { 'ffffff00'h }  -- 255.255.255.0
    ::= { cabhCdpServer 8 }

cabhCdpServerTimeOffset OBJECT-TYPE
    SYNTAX      Integer32 (-86400..86400) -- 0 à 24 heures (en secondes)
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Valeur d'option 2 - Valeur de décalage temporel du secteur LAN-Trans
       par rapport au temps universel coordonné (UTC)."
       DEFVAL { 0 }      -- UTC
    ::= { cabhCdpServer 9 }

cabhCdpServerRouterType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Type d'adresse - Routeur pour le secteur d'adresses
            du réseau LAN-Trans."
       DEFVAL { ipv4 }
    ::= { cabhCdpServer 10 }

cabhCdpServerRouter     OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Valeur d'option 3 - Routeur pour le secteur d'adresses
            du réseau LAN-Trans."
       DEFVAL { 'c0a80001'h }  -- 192.168.0.1
    ::= { cabhCdpServer 11 }

cabhCdpServerDnsAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
```

```
       "Type d'adresse IP des serveurs DNS du secteur
       d'adresses LAN-Trans."
       DEFVAL { ipv4 }
    ::= { cabhCdpServer 12 }

cabhCdpServerDnsAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Adresse IP des serveurs DNS du secteur d'adresses LAN-Trans.
       Par défaut, il n'y a qu'un seul serveur DNS et c'est l'adresse
       spécifiée dans la valeur d'option 3 - cabhCdpServerRouter.
       Une seule adresse est spécifiée."
       DEFVAL { 'c0a80001'h } -- 192.168.0.1
    ::= { cabhCdpServer 13 }

cabhCdpServerSyslogAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Type d'adresse IP des serveurs de journalisation SYSLOG
       du secteur LAN-Trans."
       DEFVAL { ipv4 }
    ::= { cabhCdpServer 14 }

cabhCdpServerSyslogAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Adresses IP des serveurs de journalisation SYSLOG
       du secteur LAN-Trans. Par défaut, il n'y a aucun serveur
       de journalisation SYSLOG. La valeur par défaut à la
       construction contient l'indication que la valeur d'absence
       de serveur SYSLOG est égale à (0.0.0.0)."
       DEFVAL { '00000000'h } -- 0.0.0.0
    ::= { cabhCdpServer 15 }

cabhCdpServerDomainName OBJECT-TYPE
    SYNTAX      SnmpAdminString(SIZE(0..128))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
     "Valeur d'option 15 - Nom de domaine du secteur d'adresses
     du réseau LAN-Trans."
       DEFVAL {""}
    ::= { cabhCdpServer 16 }

cabhCdpServerTTL OBJECT-TYPE
    SYNTAX      INTEGER (0..255)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Valeur d'option 23 - Temps de recherche de relais
            dans le secteur LAN-Trans."
       DEFVAL  { 64 }
    ::= { cabhCdpServer 17 }

cabhCdpServerInterfaceMTU       OBJECT-TYPE
    SYNTAX      Integer32 (0 | 68..4096)
    MAX-ACCESS  read-write
    STATUS      current
```

```
    DESCRIPTION
        "Valeur d'option 26 - Unité MTU d'interface dans le
        secteur LAN-Trans. Si la valeur de cet objet est 0,
        le dispositif PS ne doit pas inclure cette option
        dans ses messages DHCP OFFER ou ACK à des dispositifs IP
        de réseau LAN."
      DEFVAL { 0 }
    ::= { cabhCdpServer 18 }

cabhCdpServerVendorSpecific   OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..255))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Valeur d'option 43 - Options propres au vendeur."
      DEFVAL  { ''h }
    ::= { cabhCdpServer 19 }

cabhCdpServerLeaseTime  OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
    "Valeur d'option 51 – Durée de location pour les dispositifs IP
    de réseau LAN situés dans le secteur LAN-Trans(en secondes)."
      DEFVAL  { 3600 }
    ::= { cabhCdpServer 20 }

cabhCdpServerDhcpAddressType  OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
    "Valeur d'option 54 - Type d'adresse IP de serveur DHCP
    dans le secteur LAN-Trans."
      DEFVAL { ipv4 }
      ::= { cabhCdpServer 21 }

cabhCdpServerDhcpAddress      OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Valeur d'option 54 - Adresse IP de serveur DHCP
            dans le secteur LAN-Trans. Sa valeur par défaut
            est l'adresse du routeur comme spécifié dans l'objet
            cabhCdpServerRouter. En variante, un vendeur peut
            décider de séparer l'adresse du serveur CDS de
            celle du routeur."
      DEFVAL { 'c0a80001'h }        --    192.168.0.1
      ::= { cabhCdpServer 22 }

cabhCdpServerControl OBJECT-TYPE
    SYNTAX      INTEGER {
      restoreConfig(1)
      commitConfig (2),
      }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
"Commande pour la configuration du serveur CDS (serveur DHCP). Toutes les
modifications apportées aux objets de base MIB cabhCdpServer sont reflétées lors
de la lecture de la valeur de ces objets de base MIB; cependant, ces
```

```
modifications ne sont PAS appliquées à la configuration actuelle du serveur CDS
tant qu'elles n'ont pas été correctement validées au moyen de l'objet
cabhCdpServerControl.

Si les modifications qui sont apportées aux objets de base MIB cabhCdpServer ne
sont pas encore correctement validées auprès du serveur CDS, l'objet
cabhCdpServerControl peut servir à non valider toutes les modifications
apportées à la dernière configuration valide du serveur CDS et à ignorer toutes
les modifications intermédiaires.

restoreConfig - Le réglage de l'objet cabhCdpServerControl à cette valeur
provoquera la réinitialisation de toutes les modifications apportées aux objets
cabhCdpServer non encore validés, aux valeurs extraites de la configuration
actuelle du serveur CDS actif.

commitConfig – Le réglage de l'objet cabhCdpServerControl à cette valeur
incitera le serveur CDS à valider et à appliquer à sa configuration actuelle les
réglages valides de l'objet MIB cabhCdpServer. L'objet cabhCdpServerCommitStatus
détaillera l'état de cette opération."


      DEFVAL { restoreConfig }
    ::= { cabhCdpServer 23 }


cabhCdpServerCommitStatus OBJECT-TYPE
    SYNTAX      INTEGER {
       commitSucceeded   (1),
       commitNeeded      (2),
       commitFailed      (3)
       }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
"Indique l'état de la validation des valeurs actuelles de l'objet MIB
cabhCdpServer selon la configuration actuelle du serveur CDS (serveur DHCP).

commitSucceeded - cette valeur indique que les valeurs actuelles de l'objet MIB
cabhCdpServer sont valides et ont été correctement validées selon la
configuration actuelle du serveur CDS.

commitNeeded - cette valeur indique que la valeur d'un ou de plusieurs objets
dans le groupe MIB cabhCdpServer a été modifiée mais n'a pas encore été validée
selon la configuration actuelle du serveur CDS.

commitFailed – cette valeur indique que le dispositif PS n'a pas été en mesure
de valider les valeurs de l'objet MIB cabhCdpServer selon la configuration
actuelle du serveur CDS en raison de conflits entre ces valeurs."

   DEFVAL { commitSucceeded }
   ::= { cabhCdpServer 24 }


--
-- ce groupe de notifications fera l'objet d'extensions futures.
--

cabhCdpNotification OBJECT IDENTIFIER ::= { cabhCdpMib 2 0 }
cabhCdpConformance  OBJECT IDENTIFIER ::= { cabhCdpMib 3 }
cabhCdpCompliances  OBJECT IDENTIFIER ::= { cabhCdpConformance 1 }
cabhCdpGroups       OBJECT IDENTIFIER ::= { cabhCdpConformance 2 }

--
--    Groupe de notifications
```

```
--


-- déclarations de conformité

cabhCdpBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
            "Déclaration de conformité pour les dispositifs
            qui implémentent l'adaptateur MTA."
    MODULE   -- cabhCdpMib

-- groupes inconditionnellement obligatoires


    MANDATORY-GROUPS {
            cabhCdpGroup
    }

::= { cabhCdpCompliances 3 }

cabhCdpGroup   OBJECT-GROUP

   OBJECTS {
   cabhCdpSetToFactory,
   cabhCdpLanTransCurCount,
   cabhCdpLanTransThreshold,
   cabhCdpLanTransAction,
   cabhCdpWanDataIpAddrCount,

   cabhCdpLanAddrClientID,
   cabhCdpLanAddrLeaseCreateTime,
   cabhCdpLanAddrLeaseExpireTime,
   cabhCdpLanAddrMethod,
   cabhCdpLanAddrHostName,
   cabhCdpLanAddrRowStatus,

   cabhCdpWanDataAddrClientId,
   cabhCdpWanDataAddrIpType,
   cabhCdpWanDataAddrIp,
   cabhCdpWanDataAddrRenewalTime,
   cabhCdpWanDataAddrRowStatus,

   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
}
STATUS current
DESCRIPTION
"Groupe d'objets pour base MIB de portail CDP CableHome."
::= { cabhCdpGroups 1 }

END
```

E.3 Exigences de base MIB de portail d'essai IPCable2Home (CTP)

Exigences

La base MIB du portail CTP CableHome™ DOIT être implémentée comme défini ci-dessous.

```
CABH-CTP-MIB DEFINITIONS ::= BEGIN
IMPORTS
   MODULE-IDENTITY,
   OBJECT-TYPE          FROM SNMPv2-SMI
   TruthValue,
   TEXTUAL-CONVENTION   FROM SNMPv2-TC
   OBJECT-GROUP,
   MODULE-COMPLIANCE    FROM SNMPv2-CONF
   InetAddressType,
   InetAddress,
   InetAddressIPv4,
   InetAddressIPv6      FROM INET-ADDRESS-MIB
   clabProjCableHome    FROM CLAB-DEF-MIB;

--=================================================================
--
--     Historique:
--
--     Date      Module modifié par:       Raison
--     04/05/02                            édition I01
--     09/20/02                            édition I02
--     04/11/03                            édition I03
--
--=================================================================

cabhCtpMib MODULE-IDENTITY
    LAST-UPDATED  "200304110000Z"-- 11 avril 2003
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Adresse postale: Cable Television Laboratories, Inc.
            400 Centennial Parkway
            Louisville, Colorado 80027-1266
            Etats-Unis d'Amérique

            Tél: +1 303-661-9100
            Fax: +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
            "Le présent module de base MIB définit les commandes
            de diagnostic offertes par le portail d'essai CableHome (CTP).

      Remerciements:
      Roy Spitzer             -     Consultant à CableLabs
```

```
      Mike Mannette           -     Consultant à CableLabs
      Randy Dunton            -     Intel
      Dmitrii Loukianov       -     Intel
       Wes Peters             -     DoBox, Inc.
       Chris Zacker                 Broadcom"
    ::=  { clabProjCableHome 5 }

-- Conventions textuelles


cabhCtpObjects          OBJECT IDENTIFIER ::= { cabhCtpMib 1 }
cabhCtpBase             OBJECT IDENTIFIER ::= { cabhCtpObjects 1 }
cabhCtpConnSpeed        OBJECT IDENTIFIER ::= { cabhCtpObjects 2 }
cabhCtpPing             OBJECT IDENTIFIER ::= { cabhCtpObjects 3 }

--
--     Le groupe ci-dessous décrit les objets de base dans
--     le portail d'essai CableHome.
--

cabhCtpSetToFactory     OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Le réglage de cet objet à true(1) provoque l'effacement
            de toutes les tables contenues dans la base MIB du portail CTP
            et le retour à leur valeur par défaut de tous les objets de
            base MIB de portail CTP possédant de telles valeurs. La lecture
            de cet objet renvoie toujours la valeur false(2)."
    ::={cabhCtpBase 1}

--
--     Paramètres et résultats de la commande de vitesse de connexion
--

cabhCtpConnSrcIpType    OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
    "Type d'adresse IP utilisée en tant qu'adresse d'origine pour
    l'essai de vitesse de connexion."
       DEFVAL { ipv4 }
    ::= { cabhCtpConnSpeed 1 }

cabhCtpConnSrcIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
"Adresse IP utilisée comme adresse d'origine pour l'essai de vitesse de
connexion. La valeur par défaut est la valeur de l'objet cabhCdpServerRouter
(192.168.0.1)."
       REFERENCE
          "Spécification Cablehome section 6.4.4"
       DEFVAL { 'c0a80001'h } -- 192.168.0.1
    ::= { cabhCtpConnSpeed 2 }

cabhCtpConnDestIpType   OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
```

```
"Type d'adresse IP de destination pour l'utilitaire de vitesse de connexion de
portail CTP."
       DEFVAL { ipv4 }
    ::={ cabhCtpConnSpeed 3 }

cabhCtpConnDestIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
    "Adresse IP utilisée comme adresse de destination pour l'essai de vitesse de
    connexion."
    ::= { cabhCtpConnSpeed 4 }

cabhCtpConnProto OBJECT-TYPE
       SYNTAX    INTEGER {
                   udp               (1),
                   tcp               (2)
                   }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Protocole utilisé dans l'essai de vitesse de connexion. L'essai en
protocole TCP est facultatif."
       DEFVAL { udp }
    ::= { cabhCtpConnSpeed 5 }


cabhCtpConnNumPkts      OBJECT-TYPE
    SYNTAX       INTEGER (1..65535)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Nombre de paquets que le portail CTP doit envoyer sur déclenchement
d'exécution de l'utilitaire de vitesse de connexion."
       DEFVAL { 100 }
       ::= { cabhCtpConnSpeed 6 }

cabhCtpConnPktSize      OBJECT-TYPE
       SYNTAX    INTEGER (64..1518)
       MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Longueur des trames d'essai."
       REFERENCE
           ""
       DEFVAL { 1518 }
       ::= { cabhCtpConnSpeed 7 }

cabhCtpConnTimeOut      OBJECT-TYPE
       SYNTAX    INTEGER (0..600000)          -- Max 10 minutes
       UNITS         "milliseconds"
       MAX-ACCESS    read-write
       STATUS        current
       DESCRIPTION
    "Valeur de temporisation pour la réponse. Une valeur égale à zéro
    indique l'absence de temporisation et ne peut être utilisée qu'en
    protocole TCP."
       DEFVAL {30000}  -- 30 secondes
    ::= { cabhCtpConnSpeed 8 }

cabhCtpConnControl      OBJECT-TYPE
SYNTAX    INTEGER {
       start(1),
```

```
       abort(2)
       }
MAX-ACCESS   read-write
STATUS       current
DESCRIPTION
"Commande de l'utilitaire de vitesse de connexion. Le réglage de cet objet à la
valeur start(1) provoque l'exécution de l'utilitaire de vitesse de connexion. Le
réglage de cet objet à abort(2) provoque l'arrêt de l'exécution de l'utilitaire
de vitesse de connexion. Ce paramètre ne devrait être réglé que par protocole
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
   "Etat de l'utilitaire de vitesse de connexion."
DEFVAL   { notRun }
::={ cabhCtpConnSpeed 10 }

cabhCtpConnPktsSent     OBJECT-TYPE
       SYNTAX    INTEGER (0..65535)
       MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
    "Nombre de paquets que le portail CTP a émis après avoir reçu l'ordre
d'exécuter l'utilitaire de vitesse de connexion."
       ::= { cabhCtpConnSpeed 11 }

cabhCtpConnPktsRecv     OBJECT-TYPE
       SYNTAX    INTEGER (0..65535)
       MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Nombre de paquets que le portail CTP a reçus après avoir exécuté
l'utilitaire de vitesse de connexion."
       ::= { cabhCtpConnSpeed 12 }

cabhCtpConnRTT   OBJECT-TYPE
       SYNTAX INTEGER (0..600000)
       UNITS     "millisec"
       MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Temps d'aller-retour pour l'ensemble des paquets envoyés à destination
        – et reçus en provenance – du dispositif IP de réseau LAN cible."
       ::= { cabhCtpConnSpeed 13 }

cabhCtpConnThroughput   OBJECT-TYPE
       SYNTAX    INTEGER (0..65535)
       MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Débit utile moyen d'aller-retour mesuré en
            kilobits par seconde.""
       ::= { cabhCtpConnSpeed 14 }
```

```
--
--     Paramètres et résultats pour la commande de sondage par écho
--

cabhCtpPingSrcIpType    OBJECT-TYPE
SYNTAX       InetAddressType
MAX-ACCESS   read-write
STATUS    current
DESCRIPTION
  "Type d'adresse IP pour l'adresse d'origine de l'utilitaire de sondage
  par écho au portail CTP."
DEFVAL { ipv4 }
::={ cabhCtpPing 1 }

cabhCtpPingSrcIp OBJECT-TYPE
       SYNTAX     InetAddress
       MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
    "Adresse IP utilisée comme adresse d'origine pour l'essai de sondage
    par écho. La valeur par défaut est celle de l'objet cabhCdpServerRouter
    (192.168.0.1)."
    REFERENCE
             "section 6.4.4 de la spécification CableHome 1.0"
    DEFVAL { 'c0a80001'h }
       ::= { cabhCtpPing 2 }

cabhCtpPingDestIpType   OBJECT-TYPE
SYNTAX       InetAddressType
MAX-ACCESS   read-write
STATUS    current
DESCRIPTION
   "Type d'adresse IP pour l'adresse de destination de l'utilitaire de sondage
   par écho au portail CTP."
DEFVAL { ipv4 }
::={ cabhCtpPing 3 }

cabhCtpPingDestIp OBJECT-TYPE
       SYNTAX    InetAddress
       MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
    "Adresse IP de destination utilisée comme adresse de destination pour
    l'essai de sondage par écho."
       ::= { cabhCtpPing 4 }

cabhCtpPingNumPkts      OBJECT-TYPE
       SYNTAX    INTEGER (1..4)
       MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
             "Nombre de paquets à envoyer à chaque serveur."
       DEFVAL {1}
       ::= { cabhCtpPing 5 }

cabhCtpPingPktSize      OBJECT-TYPE
       SYNTAX    INTEGER (64..1518)
       MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
             "Longueur des trames d'essai."
```

```
       DEFVAL {64}
       ::= { cabhCtpPing 6 }

cabhCtpPingTimeBetween  OBJECT-TYPE
       SYNTAX    INTEGER (0..600000)
       UNITS       "millisecondes"
       MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Durée écoulée entre l'envoi d'un sondage par écho et la suivante."
       DEFVAL { 1000 }
    ::= { cabhCtpPing 7 }

cabhCtpPingTimeOut            OBJECT-TYPE
SYNTAX    INTEGER (1..600000)
UNITS        "millisecondes"
MAX-ACCESS   read-write
STATUS    current
DESCRIPTION
"Temporisation de la réponse de sondage par écho (réponse ICMP) pour un seul
message de sondage par écho transmis (demande ICMP)."
DEFVAL  { 1000 } -- 1 seconde
::={ cabhCtpPing 8 }

cabhCtpPingControl      OBJECT-TYPE
SYNTAX    INTEGER {
       start(1),
       abort(2)
       }
MAX-ACCESS   read-write
STATUS       current
DESCRIPTION
"Commande de l'utilitaire de sondage par écho. Le réglage de cet objet à
start(1) provoque l'exécution de l'utilitaire de sondage par écho. Le réglage de
cet objet à abort(2) provoque l'arrêt de l'exécution de l'utilitaire de sondage
par écho. Ce paramètre ne devrait être réglé que par protocole 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
   "Etat de l'utilitaire de sondage par écho."
DEFVAL   { notRun }
::={ cabhCtpPing 10 }


cabhCtpPingNumSent      OBJECT-TYPE
SYNTAX       INTEGER (0..4)
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION
  "Nombre de sondages par écho envoyés."
::={ cabhCtpPing 11 }
```

```
cabhCtpPingNumRecv      OBJECT-TYPE
       SYNTAX    INTEGER (0..255)
       MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Nombre de sondages par écho reçus."
       ::= { cabhCtpPing 12 }

cabhCtpPingAvgRTT OBJECT-TYPE
       SYNTAX    INTEGER (0..600000)
       UNITS       "millisec"
       MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
    "Valeur moyenne des temps d'aller-retour des paquets acquittés."
       ::= { cabhCtpPing 13 }

cabhCtpPingMaxRTT OBJECT-TYPE
       SYNTAX    INTEGER (0..600000)
       UNITS       "millisec"
       MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
    "Temps d'aller-retour maximal résultant des paquets acquittés."
       ::= { cabhCtpPing 14 }

cabhCtpPingMinRTT OBJECT-TYPE
       SYNTAX    INTEGER (0..600000)
       UNITS       "millisec"
       MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
    "Temps d'aller-retour minimal résultant des paquets acquittés."
       ::= { cabhCtpPing 15 }

cabhCtpPingNumIcmpError OBJECT-TYPE
       SYNTAX    INTEGER (0..255)
       MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Nombre d'erreurs ICMP."
       ::= { cabhCtpPing 16 }

cabhCtpPingIcmpError    OBJECT-TYPE
       SYNTAX    INTEGER (0..255)
       MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Dernière erreur ICMP."
       ::= { cabhCtpPing 17 }

--=========================================================================

--
-- ce groupe de notifications fera l'objet d'extensions futures.
--

cabhCtpNotification OBJECT IDENTIFIER ::= { cabhCtpMib 2 0 }
cabhCtpConformance  OBJECT IDENTIFIER ::= { cabhCtpMib 3 }
cabhCtpCompliances  OBJECT IDENTIFIER ::= { cabhCtpConformance 1 }
cabhCtpGroups       OBJECT IDENTIFIER ::= { cabhCtpConformance 2 }

--
--  Groupe de notifications
```

```
--

-- déclarations de conformité

cabhCtpBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
            "Déclaration de conformité pour les dispositifs qui implémentent
            la capacité de service portail."
    MODULE   -- cabhCtpMib



-- groupes inconditionnellement obligatoires

    MANDATORY-GROUPS {
            cabhCtpGroup
    }

::= { cabhCtpCompliances 3 }


cabhCtpGroup OBJECT-GROUP
    OBJECTS {

          cabhCtpSetToFactory,
          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
        "Groupe d'objets pour base MIB de portail CTP CableHome."
    ::= { cabhCtpGroups 1 }
```

```
END
```

E.4 Exigences relatives à la base MIB de dispositif PS (PSDev) IPCable2Home

Exigences

La base MIB PSDev CableHome™ DOIT être implémentée comme défini ci-dessous.

```
CABH-PS-DEV-MIB DEFINITIONS ::= BEGIN
IMPORTS
   MODULE-IDENTITY,
   OBJECT-TYPE,
   Integer32,
   NOTIFICATION-TYPE          FROM SNMPv2-SMI
   TruthValue,
   PhysAddress,
   DateAndTime,
   TEXTUAL-CONVENTION         FROM SNMPv2-TC
   SnmpAdminString            FROM SNMP-FRAMEWORK-MIB
   OBJECT-GROUP,
   MODULE-COMPLIANCE,
   NOTIFICATION-GROUP         FROM SNMPv2-CONF

   InetAddressType,
   InetAddress                FROM INET-ADDRESS-MIB

   docsDevSwCurrentVers,
   docsDevEvLevel,
   docsDevEvId,
   docsDevEvText,
   docsDevSwFilename,
   docsDevSwServer            FROM DOCS-CABLE-DEVICE-MIB -- RFC2669

   cabhCdpServerDhcpAddress,
   cabhCdpWanDataAddrClientId,
   cabhCdpLanTransThreshold,
   cabhCdpLanTransCurCount    FROM CABH-CDP-MIB

   clabProjCableHome          FROM CLAB-DEF-MIB;

--================================================================
--
--     Historique:
--
--     Date      Module modifié par       Raison
--     04/05/02                           Edition I01
--     09/20/02                           Edition I02
--     04/11/03                           Edition I03
--
--================================================================


cabhPsDevMib MODULE-IDENTITY
    LAST-UPDATED    "200304110000Z"-- 11 avril 2003
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
             Adresse postale: Cable Television Laboratories, Inc.
             400 Centennial Parkway
             Louisville, Colorado 80027-1266
             Etats-Unis d'Amérique
```

```
            Tél: +1 303-661-9100
            Fax: +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
            "Le présent module de base MIB fournit les objets de gestion
            de base pour le dispositif PS. Ce paramètre du dispositif PS
            décrit les attributs généraux du dispositif PS et ses
            caractéristiques comportementales. L'essentiel de la base MIB
            de dispositif PS est nécessaire pour le téléchargement d'un fichier
            de configuration.

            Remerciements:
            Roy Spitzer     - Consultant à CableLabs
            Mike Mannette   - Consultant à CableLabs
            Itay Sherman    - Texas Instruments
            Chris Zacker    - Broadcom
            Rick Vetter     - Consultant à CableLabs "
    ::=  { clabProjCableHome 1 }

-- Conventions textuelles
       X509Certificate ::= TEXTUAL-CONVENTION
           STATUS current
           DESCRIPTION
"Certificat numérique X509 codé comme un objet ASN.1 en règles DER."
           SYNTAX OCTET STRING (SIZE (0..4096))


cabhPsDevMibObjects    OBJECT IDENTIFIER ::= { cabhPsDevMib 1 }
cabhPsDevBase       OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 1 }
cabhPsDevProv    OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 2 }

--
-- le groupe ci-dessous décrit les objets de base dans le dispositif PS.
-- Ce sont des paramètres qui dépendent du dispositif.
--

cabhPsDevDateTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "Date et heure, avec informations facultatives
            sur le fuseau horaire."
    ::= { cabhPsDevBase 1 }

cabhPsDevResetNow       OBJECT-TYPE
SYNTAX       TruthValue
MAX-ACCESS   read-write
STATUS       current
DESCRIPTION
"Le réglage de cet objet à true(1) provoque le réamorçage du dispositif PS
autonome ou intégré. Le code du dispositif s'initialise comme si le dispositif
redémarrait à partir d'une remise sous tension. Le portail CMP garantit que les
valeurs de cet objet de base MIB persistent comme spécifié dans l'Appendice I de
la spécification CableHome 1.0. La lecture de cet objet renvoie toujours la
valeur false(2)."
::= { cabhPsDevBase 2 }

cabhPsDevSerialNumber OBJECT-TYPE
SYNTAX      SnmpAdminString (SIZE (0..128))
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "Numéro de série du constructeur pour ce dispositif PS. Ce paramètre
```

```
    est fourni par le constructeur et est conservé en mémoire non volatile."
::= { cabhPsDevBase 3 }

cabhPsDevHardwareVersion OBJECT-TYPE
SYNTAX      SnmpAdminString (SIZE (0..48))
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "Version du matériel du constructeur pour ce dispositif PS. Ce paramètre
    est fourni par le constructeur et est conservé en mémoire non volatile."
::= { cabhPsDevBase 4 }

cabhPsDevWanManMacAddress  OBJECT-TYPE
SYNTAX      PhysAddress
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
"Adresse MAC à l'interface PS/WAN-Man. C'est l'adresse matérielle du dispositif
PS qui doit être utilisée par le client CDC afin d'identifier de façon univoque
le dispositif PS auprès du serveur DHCP du réseau de transmission de données par
câble pour l'acquisition d'une adresse IP à utiliser pour la messagerie de
gestion entre le système NMS du réseau câblé et le portail CMP."


::= { cabhPsDevBase 5 }

cabhPsDevWanDataMacAddress  OBJECT-TYPE
       SYNTAX      PhysAddress
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
"Adresse MAC à l'interface PS/WAN-Data. Le dispositif PS pourrait avoir de
multiples interfaces avec le réseau WAN-Data, qui partageront la même adresse
matérielle. Les identificateurs de client seront uniques de façon que chacun
puisse se faire attribuer une adresse IP différente et unique."


    ::= { cabhPsDevBase 6 }

cabhPsDevTypeIdentifier    OBJECT-TYPE
       SYNTAX      SnmpAdminString
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
"Copie de l'identificateur du type de dispositif utilisé dans l'option DHCP 60,
échangée entre le dispositif PS et le serveur DHCP."
       ::= { cabhPsDevBase 7 }

cabhPsDevSetToFactory    OBJECT-TYPE
       SYNTAX      TruthValue
       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
"Le réglage de cet objet à true(1) met tous les objets de base MIB PsDev à la
valeur par défaut à la construction. La lecture de cet objet renvoie toujours la
valeur false(2)."

    ::= { cabhPsDevBase 8 }

cabhPsDevWanManClientId OBJECT-TYPE
SYNTAX          OCTET STRING (SIZE (1..80))
MAX-ACCESS      read-write
STATUS          non recommandé
DESCRIPTION
```

```
"Identificateur de client utilisé dans les demandes DHCP
de réseau WAN-MAN. La valeur par défaut est l'adresse MAC
de 6 octets."
::= { cabhPsDevBase 9 }

cabhPsDevTodSyncStatus OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
          "Cet objet indique si le dispositif PS a été capable de
          se synchroniser correctement avec le serveur temporel (ToD)
          situé dans le réseau câblé. Le dispositif PS règle cet objet
          à true(1) si le dispositif PS réussit à se synchroniser avec
          le serveur ToD. Le dispositif PS règle cet objet à false(2)
          si le dispositif PS ne réussit pas à se synchroniser avec
          le serveur ToD."
    DEFVAL { false }
::= { cabhPsDevBase 10 }

cabhPsDevProvMode       OBJECT-TYPE
       SYNTAX    INTEGER
       {
          dhcpmode(1),
          snmpmode(2),
          dormantCHmode(3)
       }
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
"Cet objet indique le mode d'approvisionnement dans lequel le dispositif PS est
en train de fonctionner. Si le dispositif PS fonctionne actuellement en mode
d'approvisionnement DHCP comme décrit dans la spécification CableHome 1.0, il
met cet objet à dhcpmode(1). Si le dispositif PS fonctionne actuellement en mode
d'approvisionnement SNMP, il règle cet objet à snmpmode(2). Si le dispositif PS
n'est pas configuré de façon à fonctionner en mode DHCP ou SNMP, il va se
replier en mode CableHome inactif, valeur dormantCHmode(3)."
::={ cabhPsDevBase 11 }


--
--  Le groupe ci-dessous définit les paramètres spécifiques de
--  l'approvisionnement
--

cabhPsDevProvisioningTimer OBJECT-TYPE
       SYNTAX      INTEGER (0..16383)
       UNITS     "minutes"
       MAX-ACCESS  read-write
       STATUS      current
       DESCRIPTION
"Cet objet permet à l'utilisateur de mettre à jour (SET) la durée du
temporisateur d'approvisionnement. La valeur est exprimée en minutes. Le réglage
du temporisateur à 0 le désactive. La valeur par défaut du temporisateur est 5."
       DEFVAL {5}
       ::=  {cabhPsDevProv 1}

cabhPsDevProvConfigFile OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..128))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
```

```
"URL du serveur local TFTP pour le téléchargement des paramètres
d'approvisionnement et de configuration vers ce dispositif. Cet objet renvoie la
valeur NULL si l'adresse du serveur est inconnue."
    ::= { cabhPsDevProv 2 }

cabhPsDevProvConfigHash OBJECT-TYPE
SYNTAX OCTET STRING (SIZE(20))
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"Hachage du contenu du fichier de configuration du PS, calculé par le système
NMS et envoyé au dispositif PS. Pour l'algorithme d'authentification SHA-1, la
longueur du hachage est de 160 bits. Cette valeur de hachage est codée en format
binaire."
      ::= { cabhPsDevProv 3 }

cabhPsDevProvConfigFileSize OBJECT-TYPE
       SYNTAX     Integer32
       UNITS      "bytes"
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
          "Taille du fichier de configuration."
       ::={ cabhPsDevProv 4 }

cabhPsDevProvConfigFileStatus OBJECT-TYPE
       SYNTAX    INTEGER
       {
              idle      (1),
              busy    (2)
       }
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
"Cet objet indique l'état actuel du processus de téléchargement  du fichier de
configuration. Il sert à indiquer à l'entité de gestion que le dispositif PS va
ignorer les déclencheurs du fichier de configuration du PS (demande de mise à
jour SET de l'objet cabhPsDevProvConfigFile) quand il sera occupé."
       ::={ cabhPsDevProv 5 }

cabhPsDevProvConfigTLVProcessed OBJECT-TYPE
       SYNTAX    INTEGER (0..16383)
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
          "Nombre d'éléments TLV traités dans fichier de configuration."
       ::={ cabhPsDevProv 6 }

cabhPsDevProvConfigTLVRejected OBJECT-TYPE
       SYNTAX    INTEGER (0..16383)
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
          "Nombre d'éléments TLV rejetés dans fichier de configuration."
       ::={ cabhPsDevProv 7 }

cabhPsDevProvSolicitedKeyTimeout OBJECT-TYPE
   SYNTAX        Integer32 (15..600)
   UNITS         "seconds"
   MAX-ACCESS    read-write
   STATUS        current
       DESCRIPTION
"Cette temporisation ne s'applique que lorsque le serveur d'approvisionnement a
lancé la gestion de clé (avec un message de réveil) pour le protocole SNMPv3.
```

```
C'est la période pendant laquelle le dispositif PS sauvegarde un nombre (dans le
champ de numéro de séquence) extrait de la demande AP envoyée et attend la
réponse AP correspondante en provenance du serveur d'approvisionnement."
       DEFVAL { 120 }
       ::= { cabhPsDevProv 8 }


cabhPsDevProvState    OBJECT-TYPE
    SYNTAX      INTEGER
    {
            pass        (1),
            inProgress  (2),
            fail        (3)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Cet objet indique l'état d'avancement du processus
             d'initialisation. Les états de succès ou d'échec
             apparaissent après l'achèvement du flux d'initialisation.
             L'état 'InProgress' apparaît du début à la fin de
             l'initialisation du dispositif PS."
    ::= { cabhPsDevProv 9 }

cabhPsDevProvAuthState    OBJECT-TYPE
    SYNTAX      INTEGER
    {
            accepted          (1),
            rejected          (2)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Cet objet indique l'état d'authentification du fichier
            de configuration."
    ::= { cabhPsDevProv 10 }

cabhPsDevProvCorrelationId    OBJECT-TYPE
    SYNTAX        Integer32
    MAX-ACCESS    read-only
    STATUS        deprecated
    DESCRIPTION
    "Valeur aléatoire produite par le dispositif PS pour utilisation
    dans l'autorisation d'enregistrement. Elle est destinée à n'être
    utilisée que dans les messages d'initialisation du dispositif PS
    et pour le téléchargement du fichier de configuration du PS.
    Cette valeur figure dans les deux messages INFORM
    cabhPsDevProvisioningStatus et cabhPsDevProvisioningEnrollmentReport
    afin de vérifier l'instance de chargement du fichier de configuration."
    ::= { cabhPsDevProv 11 }

cabhPsDevTimeServerAddrType OBJECT-TYPE
        SYNTAX      InetAddressType
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
       "Type d'adresse IP du serveur temporel (RFC-868). La version IP 4
       est normalement utilisée."
    ::= { cabhPsDevProv 12 }

cabhPsDevTimeServerAddr OBJECT-TYPE
        SYNTAX      InetAddress
        MAX-ACCESS  read-only
        STATUS      current
```

```
        DESCRIPTION
            "Adresse IP du serveur temporel (RFC-868).
            Renvoie 0.0.0.0 si l'adresse IP du serveur temporel
            est inconnue."
    ::= { cabhPsDevProv 13 }

--
-- ce groupe de notifications fera l'objet d'extensions futures.
--

cabhPsNotification OBJECT IDENTIFIER ::= { cabhPsDevMib 2 0 }
cabhPsConformance  OBJECT IDENTIFIER ::= { cabhPsDevMib 3 }
cabhPsCompliances  OBJECT IDENTIFIER ::= { cabhPsConformance 1 }
cabhPsGroups       OBJECT IDENTIFIER ::= { cabhPsConformance 2 }

--
-- Groupe de notifications.
--

cabhPsDevInitTLVUnknownTrap     NOTIFICATION-TYPE
   OBJECTS   {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
      cabhPsDevWanManMacAddress
   }
   STATUS  current
   DESCRIPTION
"Evénement dû à la détection d'éléments TLV inconnus pendant le processus
d'analyse sémantique des éléments TLV. Les valeurs des objets docsDevEvLevel,
docsDevId et docsDevEvText proviennent de l'entrée qui journalise cet événement
dans la table docsDevEventTable. La valeur de l'objet cabhPsDevWanManMacAddress
indique l'adresse de commande MAC du réseau WAN-Man du dispositif PS. Cette
partie des informations est uniforme dans tous les messages TRAP du dispositif
PS."
   ::= { cabhPsNotification 1 }

cabhPsDevInitTrap  NOTIFICATION-TYPE
   OBJECTS {
          docsDevEvLevel,
          docsDevEvId,
          docsDevEvText,
          cabhPsDevWanManMacAddress,
          cabhPsDevProvConfigFile,
          cabhPsDevProvConfigTLVProcessed,
          cabhPsDevProvConfigTLVRejected
   }
   STATUS      current
   DESCRIPTION
           "Ce message INFORM est envoyé afin de confirmer l'achèvement
           correct du processus d'approvisionnement CableHome."
   ::= { cabhPsNotification 2 }

cabhPsDevInitRetryTrap  NOTIFICATION-TYPE
   OBJECTS  {
          docsDevEvLevel,
          docsDevEvId,
          docsDevEvText,
      cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
"Evénement destiné à signaler qu'une panne s'est produite pendant le processus
d'initialisation et a été détectée dans le dispositif PS."
```

```
   ::= { cabhPsNotification 3 }

cabhPsDevDHCPFailTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       cabhCdpServerDhcpAddress
   }
   STATUS  current
   DESCRIPTION
           "Evénement destiné à signaler la panne d'un serveur DHCP.
           La valeur de l'objet cabhCdpServerDhcpAddress est l'adresse IP
           du serveur DHCP."
   ::= { cabhPsNotification 4 }


cabhPsDevSwUpgradeInitTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       docsDevSwFilename,
       docsDevSwServer
   }
   STATUS  current
   DESCRIPTION
           "Evénement destiné à signaler un événement de lancement
           de mise à jour logicielle. Les valeurs des objets docsDevSwFilename
           et docsDevSwServer indiquent le nom de l'image logicielle et
           l'adresse IP du serveur dont l'image provient."
   ::= { cabhPsNotification 5 }


cabhPsDevSwUpgradeFailTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       docsDevSwFilename,
       docsDevSwServer
   }
   STATUS  current
   DESCRIPTION
           "Evénement destiné à signaler l'échec d'un essai de mise à jour
           logicielle. Les valeurs des objets docsDevSwFilename et
           docsDevSwServer indiquent le nom de l'image logicielle et
           l'adresse IP du serveur dont l'image provient."
   ::= { cabhPsNotification 6 }


cabhPsDevSwUpgradeSuccessTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       docsDevSwFilename,
       docsDevSwServer
   }
   STATUS  current
```

```
   DESCRIPTION
           "Evénement destiné à signaler l'événement de succès de
           la mise à jour logicielle. Les valeurs des objets docsDevSwFilename
           et docsDevSwServer indiquent le nom de l'image logicielle
           et l'adresse IP du serveur dont l'image provient."
   ::= { cabhPsNotification 7 }


cabhPsDevSwUpgradeCVCFailTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress
   }
   STATUS  current
   DESCRIPTION
           "Evénement destiné à signaler qu'un échec de vérification
           de fichier de code s'est produit pendant une tentative
           de mise à jour logicielle sécurisée."
   ::= { cabhPsNotification 8 }


cabhPsDevTODFailTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevTimeServerAddr,
       cabhPsDevWanManMacAddress
   }
   STATUS  current
   DESCRIPTION
        "Evénement destiné à signaler la panne d'un serveur temporel.
        La valeur de l'objet cabhPsDevTimeServerAddr indique l'adresse
        du serveur IP."
   ::= { cabhPsNotification 9 }

cabhPsDevCdpWanDataIpTrap  NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhCdpWanDataAddrClientId,
       cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
"Evénement destiné à signaler l'échec du dispositif PS à obtenir toutes les
adresses IP de réseau WAN-Data requises. L'objet cabhCdpWanDataAddrClientId
indique l'identificateur de client pour lequel l'échec s'est produit."
   ::= { cabhPsNotification 10 }


cabhPsDevCdpThresholdTrap  NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       cabhCdpLanTransThreshold
   }
   STATUS      current
   DESCRIPTION
```

```
"Evénement destiné à signaler que le seuil du secteur LAN-Trans a été dépassé."
   ::= { cabhPsNotification 11 }

cabhPsDevCspTrap  NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
           "Evénement destiné à signaler un événement concernant
           le portail de sécurité CableHome."
   ::= { cabhPsNotification 12 }

cabhPsDevCapTrap  NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
           "Evénement destiné à signaler un événement concernant
           le portail d'adressage CableHome."
   ::= { cabhPsNotification 13 }

cabhPsDevCtpTrap  NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
           "Evénement destiné à signaler un événement concernant
           le portail d'essai CableHome."
   ::= { cabhPsNotification 14 }

cabhPsDevProvEnrollTrap  NOTIFICATION-TYPE
   OBJECTS {
       cabhPsDevHardwareVersion,
       docsDevSwCurrentVers,
       cabhPsDevTypeIdentifier,
       cabhPsDevWanManMacAddress,
       cabhPsDevProvCorrelationId
   }
   STATUS      current
   DESCRIPTION
           "Ce message INFORM est envoyé afin de lancer
           le processus d'approvisionnement CableHome."
   REFERENCE
          "Message INFORM comme défini dans le document RFC 1902"
   ::= { cabhPsNotification 15 }

cabhPsDevCdpLanIpPoolTrap NOTIFICATION-TYPE
       OBJECTS {
       docsDevEvLevel, docsDevEvId, docsDevEvText,
       cabhPsDevWanManMacAddress,
       cabhCdpLanTransCurCount
       }
```

```
       STATUS current
       DESCRIPTION
"Evénement destiné à signaler que la réserve d'adresses IP pour clients de LAN,
comme définie par les objets cabhCdpLanPoolStart et cabhCdpLanPoolEnd, est
épuisée."

       ::= { cabhPsNotification 16}

-- déclarations de conformité

cabhPsBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
            "Déclaration de conformité pour les dispositifs
            qui implémentent une capacité de dispositif PS."
    MODULE   --cabhPsMib


-- groupes inconditionnellement obligatoires

    MANDATORY-GROUPS {
            cabhPsGroup
    }

::= { cabhPsCompliances 1}


cabhPsGroup OBJECT-GROUP
    OBJECTS {
         cabhPsDevDateTime,
         cabhPsDevResetNow,
         cabhPsDevSerialNumber,
         cabhPsDevHardwareVersion,
         cabhPsDevWanManMacAddress,
         cabhPsDevWanDataMacAddress,
         cabhPsDevTypeIdentifier,
        cabhPsDevSetToFactory,
         cabhPsDevWanManClientId,
        cabhPsDevTodSyncStatus,
         cabhPsDevProvMode,
         cabhPsDevProvisioningTimer,
        cabhPsDevProvConfigFile,
        cabhPsDevProvConfigHash,
        cabhPsDevProvConfigFileSize,
        cabhPsDevProvConfigFileStatus,
        cabhPsDevProvConfigTLVProcessed,
        cabhPsDevProvConfigTLVRejected,
        cabhPsDevProvSolicitedKeyTimeout,
        cabhPsDevProvState,
        cabhPsDevProvAuthState,
         cabhPsDevProvCorrelationId,
         cabhPsDevTimeServerAddrType,
         cabhPsDevTimeServerAddr

    }
    STATUS    current
    DESCRIPTION
        "Groupe d'objets pour base MIB de dispositif PS."
    ::= { cabhPsGroups 1 }

cabhPsNotificationGroup       NOTIFICATION-GROUP
       NOTIFICATIONS {
         cabhPsDevInitTLVUnknownTrap,
         cabhPsDevInitTrap,
```

```
        cabhPsDevInitRetryTrap,
        cabhPsDevDHCPFailTrap,
        cabhPsDevSwUpgradeInitTrap,
        cabhPsDevSwUpgradeFailTrap,
        cabhPsDevSwUpgradeSuccessTrap,
        cabhPsDevSwUpgradeCVCFailTrap,
        cabhPsDevTODFailTrap,
        cabhPsDevCdpWanDataIpTrap,
        cabhPsDevCdpThresholdTrap,
        cabhPsDevCspTrap,
        cabhPsDevCapTrap,
        cabhPsDevCtpTrap,
        cabhPsDevProvEnrollTrap,
        cabhPsDevCdpLanIpPoolTrap
      }
      STATUS current
      DESCRIPTION
         "Ces notifications indiquent des changements d'état
         de l'ensemble des fonctions de services portail contenues
         dans un dispositif conforme aux spécifications CableHome(tm)
         des laboratoires CableLabs."
      ::= { cabhPsGroups 2 }
END
```

E.5 Exigences relatives à la base MIB de sécurité IPCable2Home (SEC)

Exigences

La base MIB CableHome™ sec DOIT être implémentée comme défini ci-dessous.

```
CABH-SEC-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
       Unsigned32,
       BITS,
       OBJECT-TYPE       FROM SNMPv2-SMI
       TruthValue,
       DisplayString,
       TimeStamp         FROM SNMPv2-TC
       OBJECT-GROUP,
       MODULE-COMPLIANCE FROM SNMPv2-CONF
       InetAddressIPv4   FROM INET-ADDRESS-MIB
       SnmpAdminString   FROM SNMP-FRAMEWORK-MIB -- RFC2571
       X509Certificate   FROM DOCS-BPI2-MIB
       clabProjCableHome FROM CLAB-DEF-MIB;

--=================================================================
--
--     Historique:
--
--     Date         Module modifié par      Raison
--     04/05/02                             Edition I01
--     09/20/02                             Edition I02
--     04/11/03                             Edition I03
--
--=================================================================

cabhSecMib MODULE-IDENTITY
    LAST-UPDATED    "200304110000Z"-- 11 avril 2003
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
```

```
            Adresse postale:  Cable Television Laboratories, Inc.
             400 Centennial Parkway
             Louisville, Colorado 80027-1266
                Etats-Unis d'Amérique
            Tél:  +1 303-661-9100
            Fax:  +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
            "Le présent module de base MIB fournit les objets de
            gestion de base pour les services portail de sécurité

            Remerciements:
            Roy Spitzer       -  Consultant à CableLabs
            Chris Zacker      -  Broadcom Visiting Engineer"
    ::=  { clabProjCableHome 2 }

-- Conventions textuelles


cabhSecFwObjects OBJECT IDENTIFIER ::= { cabhSecMib 1 }
cabhSecFwBase    OBJECT IDENTIFIER ::= { cabhSecFwObjects 1 }
cabhSecFwLogCtl  OBJECT IDENTIFIER ::= { cabhSecFwObjects 2 }
cabhSecCertObjects      OBJECT IDENTIFIER ::= { cabhSecMib 2 }
--
-- Le groupe ci-dessous décrit les objets de base dans le pare-feu Cablehome.
--

cabhSecFwPolicyFileEnable OBJECT-TYPE
       SYNTAX      INTEGER {
           enable        (1),
           disable       (2)
           }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
      "Ce paramètre indique s'il convient ou non d'activer la capacité
      de pare-feu."
       DEFVAL {enable}
    ::= { cabhSecFwBase 1 }

cabhSecFwPolicyFileURL OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
"Cet objet contient le nom et l'adresse IP du fichier contenant l'ensemble des
règles de la politique en format d'URL de protocole TFTP. Une fois que cet objet
a été mis à jour, il déclenche le téléchargement du fichier."

::= { cabhSecFwBase 2 }


cabhSecFwPolicyFileHash OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(20))
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
"Hachage du contenu du fichier d'ensemble de règles, calculé et envoyé au
dispositif PS avant d'envoyer le fichier d'ensemble de règles. Dans l'algorithme
d'authentification SHA-1, la longueur du hachage est de 160 bits. Cette valeur
de hachage est codée en format binaire."

::= { cabhSecFwBase 3 }
```

```
cabhSecFwPolicyFileOperStatus OBJECT-TYPE
SYNTAX    INTEGER {
inProgress(1),
complete (2),
completeFromMgt(3)  -- valeur d'état non recommandé,
failed(4)
}
MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
"La valeur inProgress(1) indique qu'un téléchargement TFTP est en cours
d'exécution. La valeur complete (2) indique que le fichier de configuration du
pare-feu a été téléchargé et configuré avec succès. Valeur completeFromMgt(3):
cet état n'est pas recommandé. La valeur failed(4) indique que la dernière
tentative de téléchargement a échoué, ordinairement en raison d'une fin de
temporisation TFTP."
::= { cabhSecFwBase 4 }


cabhSecFwPolicyFileCurrentVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
    "Version de l'ensemble de règles fonctionnant actuellement dans
    le dispositif PS. Cet objet devrait être présenté dans la syntaxe
    utilisée par le vendeur individuel afin d'identifier les versions
    logicielles. Tout élément de services PS DOIT renvoyer une chaîne
    descriptive du fichier de l'ensemble de règles téléchargé.
    Si cela n'est pas applicable, cet objet DOIT contenir une chaîne vide."
       ::= { cabhSecFwBase 5 }

--
--     Paramètres de journalisation du pare-feu
--


cabhSecFwEventType1Enable OBJECT-TYPE
SYNTAX INTEGER {
          enable (1), -- journaliser l'événement
          disable (2) -- ne pas journaliser l'événement
          }
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"Cet objet active ou désactive la journalisation des messages événementiels de
pare-feu de type 1 signalant les tentatives de traverser le pare-feu qui violent
la politique de sécurité, effectuées par des clients aussi bien privés que
publics."

DEFVAL { disable }
::= { cabhSecFwLogCtl 1 }

cabhSecFwEventType2Enable OBJECT-TYPE
SYNTAX INTEGER {
          enable (1), -- journaliser l'événement
          disable (2) -- ne pas journaliser l'événement
          }
MAX-ACCESS read-write
STATUS current
DESCRIPTION
```

```
"Cet objet active ou désactive la journalisation des messages événementiels de
pare-feu de type 2 qui signalent les tentatives identifiées d'attaque par refus
de service."

DEFVAL { disable }
::= { cabhSecFwLogCtl 2 }

cabhSecFwEventType3Enable OBJECT-TYPE
SYNTAX INTEGER {
enable (1), -- journaliser l'événement
disable (2) -- ne pas journaliser l'événement
}
MAX-ACCESS   read-write
STATUS       current
DESCRIPTION
"Cet objet active ou désactive la journalisation des messages événementiels de
pare-feu de type 3 qui signalent les modifications apportées aux paramètres
suivants de gestion du pare-feu: cabhSecFwPolicyFileURL,
cabhSecFwPolicyFileCurrentVersion, cabhSecFwPolicyFileEnable"

DEFVAL { disable }
::= { cabhSecFwLogCtl 3 }

cabhSecFwEventAttackAlertThreshold  OBJECT-TYPE
       SYNTAX    INTEGER (0..65535)
       MAX-ACCESS  read-write
       STATUS     current
       DESCRIPTION
"Si le nombre d'attaques par piratage de type 1 ou 2 dépasse ce seuil dans la
période définie par l'objet cabhSecFwEventAttackAlertPeriod, un message
d'événement de pare-feu DOIT être journalisé avec le niveau de priorité 4."
DEFVAL { 65535 }
       ::= { cabhSecFwLogCtl 4 }


cabhSecFwEventAttackAlertPeriod OBJECT-TYPE
SYNTAX INTEGER (0..65535)
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"Indique la période à utiliser (en heures) pour le seuil
cabhSecFwEventAttackAlertThreshold. Cette variable de base MIB devrait toujours
garder trace des x dernières heures d'événements, c'est-à-dire que si la
variable est réglée de façon à suivre les événements pendant 10 h, alors, quand
la 11e heure est atteinte, la 1re heure d'événements est supprimée du journal de
suivi. Une valeur par défaut est mise à zéro, c'est-à-dire à l'heure zéro, de
façon que cette variable de base MIB ne journalise aucun événement sauf
configuration contraire."
DEFVAL {0}

::= { cabhSecFwLogCtl 5 }


cabhSecCertPsCert OBJECT-TYPE
SYNTAX       X509Certificate
MAX-ACCESS   read-only
STATUS       current
DESCRIPTION
"Certificat X509 à codage DER du dispositif PS."
REFERENCE
"Exigences de la spécification CableHome 1.0 version I01 (CH-SP-I01-020405,
section 11.3) de CableLabs (exigences de sécurité)"
::= { cabhSecCertObjects 1 }
```

```
--
-- ce groupe de notifications fera l'objet d'extensions futures.
--

cabhSecNotification OBJECT IDENTIFIER ::= { cabhSecMib 3 0 }
cabhSecConformance  OBJECT IDENTIFIER ::= { cabhSecMib 4 }
cabhSecCompliances  OBJECT IDENTIFIER ::= { cabhSecConformance 1 }
cabhSecGroups       OBJECT IDENTIFIER ::= { cabhSecConformance 2 }

--
-- Groupe de notifications
--


-- déclarations de conformité

cabhSecBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
       "Déclaration de conformité pour la capacité de pare-feu CableHome."
    MODULE   -- cabhSecMib



-- groupes inconditionnellement obligatoires

    MANDATORY-GROUPS {
            cabhSecGroup
    }

::= { cabhSecCompliances 3 }


cabhSecGroup OBJECT-GROUP
    OBJECTS {
          cabhSecFwPolicyFileEnable,
          cabhSecFwPolicyFileURL,
          cabhSecFwPolicyFileHash,
          cabhSecFwPolicyFileOperStatus,
          cabhSecFwPolicyFileCurrentVersion,

          cabhSecFwEventType1Enable,
          cabhSecFwEventType2Enable,
          cabhSecFwEventType3Enable,
          cabhSecFwEventAttackAlertThreshold,
          cabhSecFwEventAttackAlertPeriod,
          cabhSecCertPsCert
    }
    STATUS    current
    DESCRIPTION
       "Groupe d'objets contenus dans la base MIB du pare-feu CableHome"
    ::= { cabhSecGroups 1 }

END
```

E.6 Exigences relatives à la base MIB de définition IPCable2Home (DEF)

```
CLAB-DEF-MIB DEFINITIONS ::= BEGIN
IMPORTS
       X509Certificate         FROM DOCS-BPI2-MIB
 -- DocsX509ASN1DEREncodedCertificate   FROM DOCS-BPI2-MIB
       MODULE-IDENTITY,
       enterprises             FROM SNMPv2-SMI;

cableLabs MODULE-IDENTITY
       LAST-UPDATED    "0209200000Z"-- 20 septembre 2002
    ORGANIZATION    "CableLabs"
    CONTACT-INFO
            "Ralph Brown
            Adresse postale: Cable Television Laboratories, Inc.
              400 Centennial Parkway
              Louisville, Colorado 80027-1266
              Etats-Unis d'Amérique
            Tél:  +1 303-661-9100
            Fax:  +1 303-661-9199
            E-mail: r.brown@cablelabs.com"
    DESCRIPTION
            "Le présent module de base MIB fournit les catégories d'objets de
gestion de base pour CableLabs."

    ::= { enterprises 4491 }

clabFunction             OBJECT IDENTIFIER ::= { cableLabs 1 }
clabFuncMib2             OBJECT IDENTIFIER ::= { clabFunction 1 }
clabFuncProprietary      OBJECT IDENTIFIER ::= { clabFunction 2 }
clabProject              OBJECT IDENTIFIER ::= { cableLabs 2 }
clabProjDocsis           OBJECT IDENTIFIER ::= { clabProject 1 }
clabProjPacketCable      OBJECT IDENTIFIER ::= { clabProject 2 }
clabProjCableHome        OBJECT IDENTIFIER ::= { clabProject 4 }
clabSecurity             OBJECT IDENTIFIER ::= { cableLabs 3}

clabSecCertObject        OBJECT IDENTIFIER ::= { clabSecurity 1 }

clabSrvcPrvdrRootCACert       OBJECT-TYPE
    SYNTAX       X509Certificate
    MAX-ACCESS    read-only
    STATUS        current
    DESCRIPTION
            "Certificat X509 à codage selon les règles DER d'autorité CA
radicale de fournisseur de services."
    REFERENCE
    "Spécification CableHome de CableLabs, section 11"
    ::= { clabSecCertObject 1 }

clabCVCRootCACert             OBJECT-TYPE
    SYNTAX       X509Certificate
    MAX-ACCESS    read-only
    STATUS       current
    DESCRIPTION
            "Certificat X509 d'autorité CA de certificat CVC de CableLabs codé
en règles DER de CableLabs"
    REFERENCE
    "Spécification CableHome de CableLabs, section 11 pour les élément PS
autonomes seulement"
    ::= { clabSecCertObject 2 }

clabCVCCACert     OBJECT-TYPE
    SYNTAX       X509Certificate
    MAX-ACCESS    read-only
```

```
    STATUS      current
    DESCRIPTION
            "Certificat X509 d'autorité CA de certificat CVC de CableLabs codé
en règles DER de CableLabs"
    REFERENCE
    "Spécification CableHome de CableLabs, section 11 pour les élément PS
autonomes seulement"
    ::= { clabSecCertObject 3 }

clabMfgCVCCert    OBJECT-TYPE
    SYNTAX      X509Certificate
    MAX-ACCESS    read-only
    STATUS        current
    DESCRIPTION
            "Certificat X509 à codage DER CVC du constructeur."
    REFERENCE
    "Spécification CableHome de CableLabs, section 11 pour les élément PS
autonomes seulement"
    ::= { clabSecCertObject 4 }

END
```

E.7 Exigences relatives à la base MIB du portail de qualité de service IPCable2Home (CQP)

Exigences

La base MIB de portail CQP CableHome™ DOIT être implémentée comme défini ci-dessous.

```
CABH-QOS-MIB DEFINITIONS ::= BEGIN
   IMPORTS
      MODULE-IDENTITY,
      OBJECT-TYPE,
      Unsigned32
                              FROM SNMPv2-SMI

      TruthValue,
      RowStatus               FROM SNMPv2-TC

      OBJECT-GROUP,
      MODULE-COMPLIANCE       FROM SNMPv2-CONF

      InetPortNumber,
      InetAddressType,
      InetAddress             FROM INET-ADDRESS-MIB

      ifIndex                 FROM IF-MIB

-- Editions de spécifications CableLabs avant les documents RFC
      clabProjCableHome       FROM CLAB-DEF-MIB;

   cabhQosMib MODULE-IDENTITY
       LAST-UPDATED    "200303010000Z"-- 1er mars 2003
       ORGANIZATION    "CableLabs Broadband Access Department"
       CONTACT-INFO
            "Kevin Luehrs
             Adresse postale: Cable Television Laboratories, Inc.
             400 Centennial Parkway
             Louisville, Colorado 80027-1266
             Etats-Unis d'Amérique
             Tél:  +1 303-661-9100
             Fax:  +1 303-661-9199
             E-mail: k.luehrs@cablelabs.com; mibs@cablelabs.com"
```

```
       DESCRIPTION
               "Le présent module de base MIB fournit les paramètres
               pour la configuration et la surveillance de la capacité CableHome
               de qualité de service priorisée."
       REVISION "200303010000Z"-- 1er mars 2003
       DESCRIPTION
      "Version initiale, publiée sous forme de document RFC xxxx."
      -- L'éditeur du document RFC attribuera le numéro xxxx
--    ::= { mib-2 xx }
-- numéro xx qui sera attribué par l'autorité IANA
-- Editions de spécifications CableLabs avant les documents RFC
    ::=  { clabProjCableHome 6 }

   -- Conventions textuelles

   cabhQosMibObjects         OBJECT IDENTIFIER ::= { cabhQosMib 1}
   cabhPriorityQosMibObjects OBJECT IDENTIFIER ::= { cabhQosMibObjects 1 }
   cabhPriorityQosBase       OBJECT IDENTIFIER ::= { cabhPriorityQosMibObjects 1
}
   cabhPriorityQosBp         OBJECT IDENTIFIER ::= { cabhPriorityQosMibObjects 2
}
   cabhPriorityQosPs         OBJECT IDENTIFIER ::= { cabhPriorityQosMibObjects 3
}

   -- future version paramétrique de QS:
   -- cabhParamQosMibObjects  OBJECT IDENTIFIER ::= { cabhQosMibObjects 2 }

   --================================================================
   --
   --  Table de référence des priorités d'application
   --
   --  L'objet cabhPriorityQosMasterTable contient la liste des
   --  priorités applicatives approvisionnées par le câblo-opérateur.
   --  Les applications sont identifiées par les numéros de point
   --  d'accès "notoires" qui leur ont été attribués par l'autorité IANA.
   --
   --================================================================
   cabhPriorityQosMasterTable  OBJECT-TYPE
         SYNTAX SEQUENCE OF CabhPriorityQosMasterEntry
         MAX-ACCESS  not-accessible
         STATUS      current
         DESCRIPTION
           "Cette table contient une liste des mappages des identificateurs
           d'application sur les priorités CableHome par défaut."
         ::= { cabhPriorityQosBase 1  }

   cabhPriorityQosMasterEntry OBJECT-TYPE
           SYNTAX CabhPriorityQosMasterEntry
           MAX-ACCESS   not-accessible
           STATUS       current
           DESCRIPTION
             "Entrée de mappage des identificateurs d'application
             sur les priorités CableHome par défaut."
      INDEX { cabhPriorityQosMasterApplicationId }
      ::= { cabhPriorityQosMasterTable 1 }


   CabhPriorityQosMasterEntry ::= SEQUENCE {
         cabhPriorityQosMasterApplicationId       Unsigned32,
         cabhPriorityQosMasterDefaultCHPriority   Unsigned32,
         cabhPriorityQosMasterRowStatus           RowStatus
        }

   cabhPriorityQosMasterApplicationId       OBJECT-TYPE
```

```
        SYNTAX                  Unsigned32 (1..65535)
        MAX-ACCESS              not-accessible
        STATUS                  current
        DESCRIPTION
     "Numéro IANA notoire de point d'accès identifiant une application."
        ::= { cabhPriorityQosMasterEntry 1 }


    cabhPriorityQosMasterDefaultCHPriority       OBJECT-TYPE
        SYNTAX                  Unsigned32 (0..7)
        MAX-ACCESS              read-create
        STATUS                  current
        DESCRIPTION
         "Priorité de qualité de service attribuée à l'application."
        ::= { cabhPriorityQosMasterEntry 2 }

    cabhPriorityQosMasterRowStatus  OBJECT-TYPE
        SYNTAX                  RowStatus
        MAX-ACCESS              read-create
        STATUS                  current
        DESCRIPTION
          "Verrouillage d'état de rangée pour la création et la suppression
          d'entrées de rangée. Le dispositif PS NE DOIT PAS permettre au système
          NMS de mettre RowStatus à notInService(2). Le dispositif PS DOIT
          attribuer à l'objet RowStatus la valeur notReady(3) dans toute nouvelle
          rangée créée sans valeur valide pour les deux entrées. Le dispositif PS
          empêchera la modification des colonnes de cette table et renverra
          une erreur de type inconsistentValue si le système NMS essaye
          d'effectuer de telles modifications alors que l'objet RowStatus est à
          l'état active(1)."
        ::= { cabhPriorityQosMasterEntry 3 }



    -- ================================================================
    --
    --  Objet SetToFactory
    --
    --  Cet objet sert à supprimer certaines des tables d'objets de base MIB QS
    --
    -- ================================================================

cabhPriorityQosSetToFactory OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
          "La lecture de cet objet renvoie toujours la valeur false(2).
          Quand cet objet est réglé à true(1), le dispositif PS DOIT supprimer
          toutes les entrées dans les tables
          cabhPriorityQosBpTable et cabhPriorityQosBpDestTable."

        ::= { cabhPriorityQosBase 2 }


    --================================================================
    --
    --  Table des priorités d'application au point BP
    --
    --  L'objet cabhPriorityQosBpTable contient la liste des
    --  points BP, des applications implémentées sur chacun de ces point
    --  et la priorité attribuée à chaque application.
    --================================================================
```

```
cabhPriorityQosBpTable OBJECT-TYPE
   SYNTAX SEQUENCE OF CabhPriorityQosBpEntry
   MAX-ACCESS not-accessible
   STATUS current
   DESCRIPTION
      "Cette table contient les priorités pour chacune des applications
      de serveur local CableHome (point BP) découvertes et les données
      associées."
         ::= {cabhPriorityQosBp 1}

cabhPriorityQosBpEntry OBJECT-TYPE
   SYNTAX       CabhPriorityQosBpEntry
   MAX-ACCESS   not-accessible
   STATUS       current
   DESCRIPTION
      "Liste de toutes les applications découvertes fonctionnant sur un
      dispositif de point BP avec leurs priorités identifiées par le
      dispositif PS."
   INDEX { cabhPriorityQosMasterApplicationId,
           cabhPriorityQosBpIpAddrType, cabhPriorityQosBpIpAddr }
   ::= { cabhPriorityQosBpTable 1 }

CabhPriorityQosBpEntry ::= SEQUENCE {
      cabhPriorityQosBpIpAddrType         InetAddressType,
      cabhPriorityQosBpIpAddr             InetAddress,
      cabhPriorityQosBpApplicationId      Unsigned32,
      cabhPriorityQosBpDefaultCHPriority  Unsigned32,
      cabhPriorityQosBpIndex              Unsigned32
      }

cabhPriorityQosBpIpAddrType   OBJECT-TYPE
   SYNTAX      InetAddressType
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "Type de l'adresse IP attribuée à un élément BP particulier."
   ::= { cabhPriorityQosBpEntry 1 }


cabhPriorityQosBpIpAddr    OBJECT-TYPE
   SYNTAX      InetAddress
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "Adresse IP attribuée à un élément BP particulier"
   ::= { cabhPriorityQosBpEntry 2 }

cabhPriorityQosBpApplicationId   OBJECT-TYPE
   SYNTAX      Unsigned32 (1..65535)
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "Numéro IANA notoire de point d'accès attribué à une
      application particulière implémentée dans le
      dispositif de serveur local CableHome où ce point BP réside."
   ::= { cabhPriorityQosBpEntry 3 }


cabhPriorityQosBpDefaultCHPriority  OBJECT-TYPE
   SYNTAX      Unsigned32 (0..7)
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "Priorité attribuée à une application particulière
```

```
       implémentée dans le dispositif de serveur local CableHome où
       ce point BP réside. Le dispositif PS remplit cette entrée conformément
       à la table de référence des priorités d'application."
   ::= { cabhPriorityQosBpEntry 4 }

cabhPriorityQosBpIndex  OBJECT-TYPE
   SYNTAX      Unsigned32 (1..65535)
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
     "Identificateur unique pour une rangée particulière dans la table
     des priorités d'application d'un point BP. Cet identificateur est
     utilisé comme indice de pointage dans la table 'intégrée' des priorités
     de destination."
        ::= { cabhPriorityQosBpEntry 5 }


--================================================================
--
--  Table des priorités de destination
--
--  L'objet cabhPriorityQosDestListTable contient la liste des
--  destinations approvisionnées (adresse IP et numéro de point d'accès)
--  auxquelles un point BP peut envoyer du trafic avec une
--  priorité de QS particulière. Toute application énumérée dans la
--  table des priorités d'application de point BP peut être approvisionnée
--  dans cette table avec une priorité de destination spécifique.

--================================================================

cabhPriorityQosBpDestTable OBJECT-TYPE
   SYNTAX SEQUENCE OF CabhPriorityQosBpDestEntry
   MAX-ACCESS    not-accessible
   STATUS        current
   DESCRIPTION
      "Cette table contient les priorités fondées sur des
       sessions établies par un dispositif de point BP, identifiées par
       une adresse IP de destination et par un numéro de point d'accès. Elle
       est pointée par un identificateur unique pour les rangées situées
       dans la table des priorités d'application au point BP."
       (cabhPriorityQoSBpTable."
       ::= {cabhPriorityQosBp 2}

cabhPriorityQosBpDestEntry OBJECT-TYPE
   SYNTAX      CabhPriorityQosBpDestEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION
      "Liste des adresses IP et des numéros de point d'accès de destination
      pour une application vers laquelle une priorité QS spéciale
      est approvisionnée."
   INDEX { cabhPriorityQosBpIndex, cabhPriorityQosBpDestIndex }
   ::= { cabhPriorityQosBpDestTable 1 }

CabhPriorityQosBpDestEntry ::= SEQUENCE {
    cabhPriorityQosBpDestIndex            Unsigned32,
    cabhPriorityQosBpDestIpAddrType       InetAddressType,
    cabhPriorityQosBpDestIpAddr           InetAddress,
    cabhPriorityQosBpDestPort             InetPortNumber,
    cabhPriorityQosBpDestIpPortPriority   Unsigned32
      }


cabhPriorityQosBpDestIndex OBJECT-TYPE
```

```
      SYNTAX      Unsigned32 (1..65535)
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
        "Indice localement unique dans la table des priorités de destination."
      ::= { cabhPriorityQosBpDestEntry 1 }

   cabhPriorityQosBpDestIpAddrType     OBJECT-TYPE
      SYNTAX      InetAddressType
      MAX-ACCESS  read-only
      STATUS      current
      DESCRIPTION
         "Type de l'adresse IP de destination."
      ::= { cabhPriorityQosBpDestEntry 2 }

   cabhPriorityQosBpDestIpAddr   OBJECT-TYPE
      SYNTAX      InetAddress
      MAX-ACCESS  read-only
      STATUS      current
      DESCRIPTION
        "Adresse IP de destination du dispositif pour lequel
        une session d'application a été établie par un dispositif
        de point BP et pour lequel une priorité de qualité de
        service spéciale a été approvisionnée."
      ::= { cabhPriorityQosBpDestEntry 3 }

   cabhPriorityQosBpDestPort     OBJECT-TYPE
      SYNTAX      InetPortNumber
      MAX-ACCESS  read-only
      STATUS      current
      DESCRIPTION
        "Numéro de point d'accès à un dispositif IP pour lequel
        une session d'application a été établie par un dispositif de
        point BP et pour lequel une priorité de qualité de service
        spéciale a été approvisionnée."
      ::= { cabhPriorityQosBpDestEntry 4 }

   cabhPriorityQosBpDestIpPortPriority    OBJECT-TYPE
      SYNTAX      Unsigned32 (0..7)
      MAX-ACCESS  read-only
      STATUS      current
      DESCRIPTION
        "Priorité de qualité de service attribuée à une session
        d'application particulière (identifiée par son adresse IP
        et par son point d'accès de destination) dans un dispositif
        de point BP"
      ::= { cabhPriorityQosBpDestEntry 5 }


   --================================================================
   --
   --  Table des attributs d'interface du dispositif PS
   --
   --  L'objet cabhPriorityQosPsIfAttribTable contient le nombre de
   --  priorités d'accès au support et le nombre de files d'attente associées à
   --  chaque interface avec un réseau LAN située dans la passerelle
   --  résidentielle.
================================================================

   cabhPriorityQosPsIfAttribTable   OBJECT-TYPE
           SYNTAX SEQUENCE OF CabhPriorityQosPsIfAttribEntry
           MAX-ACCESS   not-accessible
           STATUS    current
           DESCRIPTION
```

```
         "Cette table contient le nombre de priorités d'accès au support
         et le nombre de files d'attente associées à chaque interface
         avec un réseau LAN située dans la passerelle résidentielle."
         ::= { cabhPriorityQosPs 1  }

cabhPriorityQosPsIfAttribEntry      OBJECT-TYPE
        SYNTAX    CabhPriorityQosPsIfAttribEntry
        MAX-ACCESS   not-accessible
        STATUS       current
        DESCRIPTION
          "Nombre de priorités d'accès au support et nombre
          de files d'attente pour chaque interface avec un réseau LAN
          située dans la passerelle résidentielle. Cette table
          s'applique seulement aux interfaces par lesquelles
          des données transitent."
        INDEX { ifIndex }
        ::= { cabhPriorityQosPsIfAttribTable 1 }

CabhPriorityQosPsIfAttribEntry ::= SEQUENCE {
   cabhPriorityQosPsIfAttribIfNumPriorities    Unsigned32,
        cabhPriorityQosPsIfAttribIfNumQueues   Unsigned32
}

cabhPriorityQosPsIfAttribIfNumPriorities OBJECT-TYPE
       SYNTAX     Unsigned32 (1..8)
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
        "Nombre de priorités d'accès au support prises en charge
        par cette interface avec un réseau LAN."
::= { cabhPriorityQosPsIfAttribEntry 1 }

cabhPriorityQosPsIfAttribIfNumQueues OBJECT-TYPE
       SYNTAX     Unsigned32 (1..8)
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
        "Nombre de files d'attente associées à cette interface
        avec un réseau LAN."
::= { cabhPriorityQosPsIfAttribEntry 2 }


-- Structure générique pour notifications/transferts automatiques.
--

cabhQosNotification         OBJECT IDENTIFIER  ::= { cabhQosMib 2 }
cabhPriorityQosNotification OBJECT IDENTIFIER  ::= {
cabhQosNotification 1 }



--
-- Définitions relatives à la conformité
--
cabhQosConformance          OBJECT IDENTIFIER  ::= { cabhQosMib 3 }
cabhPriorityQosConformance  OBJECT IDENTIFIER  ::= {
cabhQosConformance 1 }
cabhPriorityQosGroups       OBJECT IDENTIFIER  ::= {
cabhPriorityQosConformance 1 }
cabhPriorityQosCompliances  OBJECT IDENTIFIER  ::= {
cabhPriorityQosConformance 2 }


-- ==================
```

```
-- déclarations de conformité

cabhPriorityQosCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
      "Déclaration de conformité pour les dispositifs qui implémentent
      la capacité CableHome 1.1 de priorité de QS."

    MODULE   --cabhPriorityQosMib



-- groupes inconditionnellement obligatoires

    MANDATORY-GROUPS {
            cabhPriorityQosGroup
    }

::= { cabhPriorityQosCompliances 1}


cabhPriorityQosGroup OBJECT-GROUP
    OBJECTS {
    cabhPriorityQosMasterDefaultCHPriority,
    cabhPriorityQosMasterRowStatus,
    cabhPriorityQosSetToFactory,
    cabhPriorityQosBpIpAddrType,
    cabhPriorityQosBpIpAddr,
    cabhPriorityQosBpApplicationId,
    cabhPriorityQosBpDefaultCHPriority,
    cabhPriorityQosBpIndex,
    cabhPriorityQosBpDestIpAddrType,
    cabhPriorityQosBpDestIpAddr,
    cabhPriorityQosBpDestPort,
    cabhPriorityQosBpDestIpPortPriority,
    cabhPriorityQosPsIfAttribIfNumPriorities,
    cabhPriorityQosPsIfAttribIfNumQueues
    }
    STATUS    current
    DESCRIPTION
        "Groupe d'objets pour la base MIB de priorité
        d'application CableHome."
         Priority MIB."
    ::= { cabhPriorityQosGroups 1 }

END
```

Appendice I

Exemples de mappage de priorité d'accès au support

La présente Recommandation définit un système de qualité de service priorisée dans lequel le trafic transitant sur les supports partagés est priorisé sur la base de la priorité attribuée aux paquets. Etant donné que différentes techniques de supports partagés prennent en charge divers nombres de priorités d'accès au support, le modèle IPCable2Home définit un procédé de mappage permettant de convertir les priorités IPCable2Home génériques en un ensemble de valeurs appelé *priorités IPCable2Home d'accès au support*. Les valeurs des priorités IPCable2Home d'accès au support décrivent le niveau de préférence qu'un paquet devrait obtenir lorsqu'il accède aux supports partagés. Le nombre de niveaux de préférence correspond au nombre disponible de priorités d'accès au support pris en charge par une technique d'accès au support donnée. Plus élevée est la valeur de priorité IPCable2Home d'accès au support pour le paquet, plus élevée est la préférence qu'il devrait obtenir afin d'accéder au support partagé. Le mappage IPCable2Home des priorités d'accès au support est séparé et distinct des mappages de priorité d'accès au support définis par défaut dans les techniques de partage de support. Ces mappages par défaut sont effectués dans la couche 2 de chaque dispositif. Quelle que soit la technique de partage de support, les paquets doivent donc recevoir le niveau relatif – d'accès préférentiel aux supports partagés – qui est requis par le mappage des priorités IPCable2Home d'accès au support. Les Tableaux I.1, I.2 et I.3 présentent des exemples de mappage pour quelques-unes des techniques d'accès partagé.

I.1 Ethernet

Le protocole Ethernet n'effectue pas de différenciation entre les paquets et ne prend donc en charge qu'une seule priorité.

Comme représenté dans le Tableau I.1, aucun ajustement spécial du mappage n'est requis.

Tableau I.1/J.192 – Mappages Ethernet

Priorité IPCable2Home générique	Mappage IPCable2Home des priorités d'accès au support	Mappage Ethernet par défaut des priorités d'accès au support
0	0	0
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0

I.2 HomePlug

Le protocole HomePlug prend en charge quatre priorités d'accès au support.

Comme représenté dans le Tableau I.2, le mappage du protocole HomePlug donne un canal d'accès préférentiel à la priorité générique IPCable2Home 0, par rapport aux priorités génériques IPCable2Home 1 et 2. Cependant, le mappage IPCable2Home des priorités d'accès au support exige que la priorité générique IPCable2Home 2 reçoive un accès supérieur par rapport aux priorités

génériques IPCable2Home 0 et 1 et que les priorités génériques IPCable2Home 0 et 1 reçoivent des droits d'accès égaux. Le vendeur doit donc garantir que les paquets reçoivent l'accès préférentiel relatif aux supports partagés qui est recherché par le mappage IPCable2Home des priorités d'accès au support.

Tableau I.2/J.192 – Mappages HomePlug

Priorité IPCable2Home générique	Mappage IPCable2Home des priorités d'accès au support	Mappage HomePlug par défaut des priorités d'accès au support
0	0	1
1	0	0
2	1	0
3	1	1
4	2	2
5	2	2
6	3	3
7	3	3

I.3 HomePNA

Le protocole HomePNA prend en charge huit priorités d'accès au support.

Comme représenté dans le Tableau I.3, le mappage HomePNA offre un canal d'accès préférentiel au niveau 0 de priorité générique IPCable2Home par rapport aux niveaux 1 et 2 de priorité générique IPCable2Home. Cependant, le mappage IPCable2Home des priorités d'accès au support exige que le niveau 2 de priorité générique IPCable2Home 2 reçoive un accès supérieur par rapport aux niveaux 0 et 1 de priorité IPCable2Home générique; il exige également que le niveau 1 de priorité générique IPCable2Home reçoive un accès supérieur par rapport au niveau 0 de priorité générique IPCable2Home. Donc, le vendeur doit garantir que les paquets reçoivent l'accès préférentiel relatif aux supports partagés qui est recherché conformément au mappage IPCable2Home des priorités d'accès au support.

Tableau I.3/J.192 – Mappages HomePNA

Priorité IPCable2Home générique	Mappage IPCable2Home des priorités d'accès au support	Mappage HomePNA par défaut des priorités d'accès au support
0	0	2
1	1	0
2	2	1
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7

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, 2005