Unión Internacional de Telecomunicaciones

UIT-T J.191

(03/2004)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE J: REDES DE CABLE Y TRANSMISIÓN DE PROGRAMAS RADIOFÓNICOS Y TELEVISIVOS, Y DE OTRAS SEÑALES MULTIMEDIOS

Módems de cable

Lote de características basadas en el protocolo Internet para mejorar los módems de cable

Recomendación UIT-T J.191

UIT-T

Unión Internacional de Telecomunicaciones

Recomendación UIT-T J.191

Lote de características basadas en el protocolo Internet para mejorar los módems de cable

Resumen

Esta Recomendación presenta un juego de características basadas en el protocolo Internet (IP) que pueden añadirse a los módems de cable o incorporarse en un dispositivo autónomo, para que los operadores de cable puedan ofrecer a sus clientes un conjunto suplementario de servicios mejorados, entre ellos el soporte de la calidad de servicio (QoS) IPCablecom, las características adicionales de administración y configuración de los servicios y mejoras en el direccionamiento y en el tratamiento de los paquetes.

Orígenes

La Recomendación UIT-T J.191 fue aprobada el 15 de marzo de 2004 por la Comisión de Estudio 9 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

© UIT 2005

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

Recomendación UIT-T J.191

Lote de características basadas en el protocolo Internet para mejorar los módems de cable

1 Alcance

Esta Recomendación presenta un juego de características basadas en el protocolo Internet (IP) que pueden añadirse a los módems de cable o incorporarse en un dispositivo autónomo, para que los operadores de cable puedan ofrecer a sus clientes un conjunto suplementario de servicios mejorados, entre ellos el soporte de la calidad de servicio (QoS) IPCablecom, las características adicionales de administración y configuración de los servicios y mejoras en el direccionamiento y en el tratamiento de los paquetes. Esta Recomendación implementa el dominio IPCable2Home definido en la Rec. UIT-T J.190.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

2.1 Referencias normativas

– Recomendación UIT-T J.112 anexo B (2004), *Especificaciones de interfaces de servicios de datos por cable: Especificación de la interfaz de radiofrecuencia*.

– Recomendación UIT-T J.161 (2001), *Requisitos de los códecs de audio para la prestación de servicios de audio bidireccionales por redes de televisión por cable que utilizan módems de cable*.

– Recomendación UIT-T J.163 (2004), *Calidad de servicio dinámica para la prestación de servicios en tiempo real por las redes de televisión por cable que utilizan módems de cable*.

– Recomendación UIT-T J.170 (2002), *Especificación de la seguridad de IPCablecom*.

– Recomendación UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*.

– Recomendación UIT-T X.690 (2002) | ISO/CEI 8825-1:2002, *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación básica, de las reglas de codificación canónica y de las reglas de codificación distinguida*.

– ISO/CEI 15802-3:1998 (ANSI/IEEE Std 802.1D), *Information technology – Telecommunications and information exchange between systems – Local area networks – Media access control (MAC) bridges*.

– FIPS 140-2-2001, *Security Requirements for Cryptographic Modules*.

– FIPS 180-2-2002, *Secure hash standard*.

– FIPS 186-2-2000, *Digital signature standard (DSS)*.

– IETF RFC 768 (1980), *User Datagram Protocol (UDP)*.

– IETF RFC 792 (1981), *Internet Control Message Protocol, DARPA Internet Program, Protocol specification*.

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

– IETF RFC 1034 (1987), *Domain Names – Concepts and Facilities*.

– IETF RFC 1035 (1987), *Domain Names – Implementation and Specification*.

– IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication layers*.

– IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP)*.

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

– IETF RFC 1901 (1996), *Introduction to community-based SNMPv2*.

– IETF RFC 2011 (1996), *SNMPv2 Management Information Base for the Internet Protocol using SMIv2*.

– IETF RFC 2013 (1996), *SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2*.

– IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*.

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

– IETF RFC 2233 (1997), *The Interfaces Group MIB using SMIv2*.

– IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2*.

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

– IETF RFC 2437 (1998), *PKCS #1: RSA Cryptography Specifications Version 2.0*.

– IETF RFC 2576 (2000), *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*.

– IETF RFC 2578 (1999), *Structure of Management Information Version 2 (SMIv2)*.

– IETF RFC 2579 (1999), *Textual Conventions for SMIv2*.

– IETF RFC 2580 (1999), *Conformance Statements for SMIv2*.

– IETF RFC 2669 (1999), *DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems*.

– IETF RFC 2670 (1999), *Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces*.

– IETF RFC 2786 (2000), *Diffie-Helman USM Key Management Information Base and Textual Convention*.

– IETF RFC 2863 (2000), *The Interfaces Group MIB*.

– IETF RFC 3022 (2001), *Traditional IP Network Address Translator (Traditional NAT)*.

– IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

– IETF RFC 3291 (2002), *Textual Conventions for Internet Network Addresses*.

– IETF RFC 3396 (2002), *Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)*.

– IETF RFC 3412 (2002), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*.

– IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) applications*.

– IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

– IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

– IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for Simple Network Management Protocol (SNMP)*.

– IETF RFC 3417 (2002), *Transport Mappings for the Simple Network Management Protocol (SNMP)*.

– IETF RFC 3418 (2002), *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*.

2.2 Referencias informativas

– Recomendación UIT-T J.190 (2002), *Arquitectura de MediaHomeNet que soporta servicios basados en cable*.

– IETF RFC 347 (1972), *Echo Process*.

– IETF RFC 1949 (1996), *Scalable Multicast Key Distribution*.

– IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations*.

– IETF RFC 2979 (2000), *Behavior of and Requirements for Internet Firewalls*.

– IETF RFC 3235 (2002), *Network Address Translator (NAT) – Friendly Application Design Guidelines*.

– draft-ietf-ipcdn-bpiplus-mib-12 INTERNET DRAFT – *DOCSIS Baseline Privacy Plus MIB – Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus*, October 2003.

– ICSA, Inc.: Firewall Buyer's Guide, 1998, *www.icsalabs.com*.

3 Términos y definiciones

En esta Recomendación se definen los términos siguientes.

3.1 portal de seguridad del cable (CSP, *cable security portal*): Elemento funcional que proporciona las funciones de gestión de seguridad y traducción entre el HFC y el hogar.

3.2 servidor de gestión de llamadas (CMS, *call management server*): [IPCablecom] Controla las conexiones de audio. Se denomina asimismo agente de llamadas en la terminología MGCP/SGCP.

3.3 calidad de servicio dinámica (DQoS, *dynamic quality of service*): [IPCablecom] Se asigna a cada una de las comunicaciones sobre la marcha en función de la QoS solicitada.

3.4 adaptador de terminal de medios insertado (E-MTA, *embedded multimedia terminal adapter*): [IPCablecom] Nodo sencillo que contiene un MTA y un módem de cable.

3.5 módem de cable mejorado con protocolo Internet: Módem de cable que se ha mejorado por la adición de funciones IP definidas en esta Recomendación.

3.6 servicio de portal (PS, *portal service*): Elemento funcional que proporciona las funciones de gestión y traducción entre el HFC y el hogar.

3.7 dispositivo protocolo Internet de la red de área local: El dispositivo IP de LAN representa el típico dispositivo IP que se instala en el hogar, dotado además de una pila TCP/IP y de un cliente DHCP.

3.8 transferencia: Se trata de una subfunción del CAP, la función transferencia hace de puente para los paquetes entre el lado WAN-data del CAP y el lado LAN-pass sin introducir modificaciones.

3.9 adaptador de terminal de medios autónomo (S-MTA, *stand-alone multimedia terminal adapter*): Nodo sencillo que contiene un MTA y un MAC que no es DOCSIS (por ejemplo, Ethernet).

4 Abreviaturas, siglas o acrónimos y convenios

4.1 Abreviaturas, siglas o acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos.

ASP	Apoderado específico de la aplicación (*application-specific proxy*)
CA	Autoridad de certificación (*certificate authority*)
CAP	Portal de dirección del cable (*cable address portal)*
CAT	Traducción de dirección del cable (*cable address translation*)
CDC	Cliente DHCP del cable (*cable DHCP client*)
CDP	Portal DHCP del cable (*cable DHCP portal*)
CM	Módem de cable (*cable modem*)
CMP	Portal de gestión del cable (*cable management portal*)
CMS	Servidor de gestión de llamadas (*call management server*)
CMTS	Sistema de terminación de módem de cable (*cable modem termination system*)
C-NAPT	Traducción de dirección y puertos de la red de cable (*cable network address and portal translation*)
C-NAT	Traducción de dirección de la red de cable (*cable network address translation*)
CNP	Portal de denominación del cable (*cable naming portal*)
CQoS	Calidad de servicio del cable (*cable quality-of-service*)
CQP	Portal de calidad de servicio del cable (*cable quality-of-service portal*)
CRL	Lista de revocación de certificados (*certificate revocation list*)
CSP	Portal de seguridad del cable (*cable security portal*)
CTP	Portal de prueba del cable (*cable testing portal*)
CVC	Certificado de verificación de código (*code verification certificate*)
CVS	Signatura de verificación de código (*code verification signature*)
CxP	Subfunción PS del cable (*cable PS sub-function*)
DER	Reglas de codificación distinguida (*distinguished encoding rules*)

DHCP	Protocolo dinámico de configuración de anfitrión (*dynamic host configuration protocol*)
DNS	Sistema de nombres de dominio (*domain name system*)
DOCSIS	Especificación de interfaz del servicio de datos por cable (*data-over-cable service interface specification*)
DQoS	Calidad de servicio dinámica (IPCablecom) (*dynamic quality of service (IPCablecom)*)
E-MTA	Adaptador de terminal de medios insertado (*embedded multimedia terminal adapter*)
FTP	Protocolo de transferencia de ficheros (*file transfer protocol*)
FW	Barrera contra fuegos (*firewall*)
GMT	Tiempo medio de Greenwich (*Greenwich mean time*)
HEX	Hexadecimal
HFC	Híbrido fibra coaxial (*hybrid fibre coax*)
ICMP	Protocolo de mensajes de control Internet (*Internet control message protocol*)
IGMP	Protocolo de gestión del grupo Internet (*Internet group management protocol*)
IP	Protocolo Internet (*Internet protocol*)
KDC	Centro de distribución de claves (*key distribution centre*)
LAN-Pass	Dirección de transferencia de LAN (*pass-through LAN address*)
LAN-Trans	Dirección traducida de LAN (*translated LAN address*)
MAC	Control de acceso a medios (*media access control*)
MGCP	Protocolo de control de pasarela de medios (*media gateway control protocol*)
MIB	Base de información de gestión (*management information base*)
MTA	Adaptador de terminal multimedios (o multimedia) (*multimedia terminal adapter*)
NAPT	Traducción de dirección de red y del portal (*network address and portal translation*)
NAT	Traducción de dirección de red (*network address translation*)
NCS	Señalización de llamada basada en la red (*network-based call signalling*)
NMS	Sistema de gestión de red (*network management system*)
OID	Identificador de objeto (*object identifier*)
OSI	Interconexión de sistemas abiertos (*open system interconnection*)
OSS	Sistema de soporte de operaciones (*operations support system*)
PDU	Unidad de datos de protocolo (*protocol data unit*)
PING	Grupo de paquetes entre redes (*packet inter-network grouper*)
PKI	Infraestructura de claves públicas (*public key infrastructure*)
PKINIT	Autenticación inicial para criptografía de clave pública (*public-key cryptography for initial authentication*)
PS WAN-Data	Interfaz de datos entre elemento servicio de portal y la red de área extensa (*portal service element WAN data interface*)

PS WAN-Man Interfaz de gestión entre el elemento servicio de portal y la red de área extensa (*portal service element WAN management interface*)

PS Servicio de portal (*portal service*)

QoS Calidad de servicio (*quality of service*)

RFC Petición de comentarios (*request for comments*)

RSA Rivest, Shamir y Adleman

SHA-1 Algoritmo de troceo seguro 1 (*secure hash algorithm 1*)

S-MTA Adaptador de terminal de medios autónomo (*stand-alone multimedia terminal adapter*)

SNMP Protocolo simple de gestión de red (*simple network management protocol*)

SOA Comienzo de autoridad (*start of authority*)

SPF Filtrado dinámico de paquetes (*stateful packet filtering*)

SYSLOG Registro de sistema (*system log*)

TCP Protocolo de control de transmisión (*transmission control protocol*)

TFTP Protocolo de transferencia de ficheros trivial (*trivial file transfer protocol*)

TLV Tipo-longitud-valor (*type-lenght-value*)

UDP Protocolo de datagrama de usuario (*user datagram protocol*)

USFS Conmutador de retransmisión en sentido ascendente (*upstream selective forwarding switch*)

USM Modelo de seguridad de usuario (*user security model*)

UTC Tiempo universal coordinado (*coordinated universal time*)

VACM Modelo de control de accesos basado en vistas (*view-based access control model*)

VoIP Voz sobre el protocolo Internet (*voice over Internet protocol*)

WAN Red de área extensa (*wide area network*)

WAN-Data Sector de direcciones de datos de la red de área extensa (*wide area network data address realm*)

WAN-Man Sector de direcciones de gestión de la red de área extensa (*wide area network management address realm*)

4.2 Convenios

Al aplicar la presente Recomendación, las palabras clave "DEBE(N)", "DEBERÁ(N)" y "REQUERIDO" han de interpretarse como definitorias de un aspecto obligatorio de la presente Recomendación. Las palabras clave utilizadas en la presente Recomendación para indicar que un determinado requisito tiene un cierto grado de importancia se resumen en el cuadro a continuación.

"DEBE(N)" Esta palabra o el adjetivo "REQUERIDO" significan que el elemento es un requisito absoluto de la presente Recomendación.

"NO DEBE(N)" Esta frase significa que el elemento constituye una prohibición absoluta en la presente Recomendación.

"DEBERÍA(N)" Esta palabra o el adjetivo "RECOMENDADO" significa que, en determinadas circunstancias, puede haber motivos justificados para ignorar este elemento, aunque deben tenerse en cuenta todas las repercusiones, estudiando detenidamente todas y cada una de las circunstancias antes de optar por una alternativa diferente.

"NO DEBERÍA(N)" Esta expresión significa que, en determinadas circunstancias, puede haber razones por las que la actuación consignada resulte aceptable e incluso útil, debiendo considerarse todas las repercusiones y estudiando cuidadosamente todas las circunstancias antes de emprender las acciones descritas en este epígrafe.

"PUEDE(N)" Esta palabra y el adjetivo "OPCIONAL(ES)" indican que este elemento es opcional. Por ejemplo un fabricante puede optar por incorporar este elemento por exigencias de un mercado determinado o porque aporta mejoras significativas al producto, mientras que otro fabricante puede optar por suprimir dicho elemento.

5 Arquitectura de referencia

La presente Recomendación proporciona un conjunto de características basadas en el protocolo Internet que pueden añadirse a un módem de cable, o incorporarse en un dispositivo autónomo, de modo que los operadores de cable puedan ofrecer a sus clientes un conjunto adicional de servicios mejorados. Estas características basadas en IP residen en un elemento lógico denominado el servicio de portal (PS o simplemente portal). Los dispositivos dotados de estas características mejoradas reciben el nombre de pasarelas particulares, y son implementaciones de IPCable2Home, como se describe en la Rec. UIT-T J.190.

Sus principales aspectos y características son los siguientes:

– Gestión y configuración:
  - Gestión y configuración remotas de la pasarela particular.
  - Apoderado de gestión sencilla de la pasarela particular para dispositivos en el hogar basados en IP.
  - Prestación sin intervención para la pasarela residencial.

– Direccionamiento y tratamiento de paquetes:
  - Traducción de direcciones de uno a varios para los dispositivos del hogar.
  - Traducción biunívoca de direcciones para los dispositivos del hogar.
  - Direccionamiento no traducido para los dispositivos del hogar (aplicaciones que no admiten NAT).
  - Protección del tráfico HFC contra las comunicaciones internas de los dispositivos en el hogar.
  - Soporte de direccionamiento en el hogar en caso de interrupción del HFC.
  - Servidor DNS sencillo en la pasarela particular.

– Calidad de servicio (QoS):
  - Funcionalidad de puenteo transparente de la pasarela particular para la mensajería de QoS IPCablecom enviada a las aplicaciones homologadas con IPCablecom o recibida de éstas.

– Seguridad:
  - Autenticación de la pasarela particular.
  - Mensajes de gestión segura de la pasarela particular.

- Descarga segura de ficheros de configuración y de soporte lógico.
- QoS segura en el enlace HFC.
- Gestión remota de la barrera contra fuegos de la pasarela particular.

La comunicación en la LAN y en la WAN está basada en el protocolo IPv4, el cual tendrá ventajas sobre los protocolos específicos que se definen en el resto de esta Recomendación. Los dispositivos conformes DEBEN aplicar la versión 4 de la serie de los protocolos IP (IPv4).

En el resto de esta cláusula se analiza la arquitectura de referencia de seis perspectivas:

- Lógica (5.1).
- Funcional (5.2).
- De la interfaz de mensajería (5.3).
- De información (5.4).
- De explotación (5.5).
- De la interfaz física (5.6).

5.1 Arquitectura lógica de referencia

Como se ilustra en la figura 5-1, en esta cláusula se introducen los conceptos lógicos del dominio de IPCable2Home, de los elementos lógicos y de la clase de dispositivo de acceso a la vivienda (HA, *home access*).

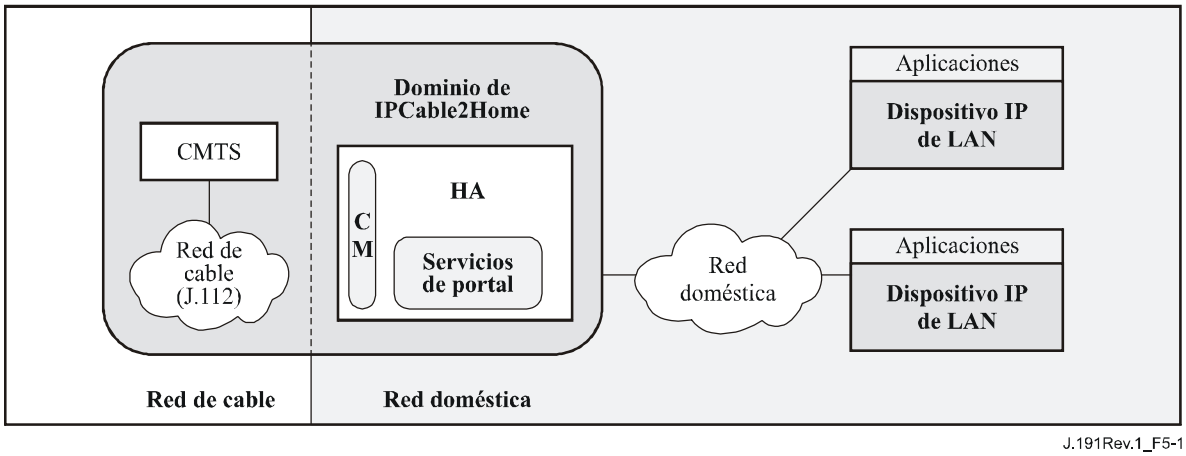


Figura 5-1/J.191 – Conceptos lógicos esenciales

5.1.1 Dominios de IPCable2Home

El dominio de IPCable2Home representa el conjunto de los elementos de red que tienen conformidad con esta Recomendación, y se representan a modo de diagrama como una región sombreada en la figura 5-1. Esta región es útil como una herramienta visual para identificar plenamente ese tipo de elementos conformes dentro de la red doméstica. Los elementos que residen en el dominio de IPCable2Home (elementos conformes) son gestionados directamente por los operadores.

5.1.2 Elementos lógicos

El marco de arquitectura introduce el concepto de elementos lógicos. Los elementos lógicos de IPCable2Home son entidades funcionales limitadas de manera lógica que pueden generar y responder a los mensajes conformes a IPCable2Home. Estos elementos lógicos funcionan en la capa de protocolo de red y por encima de la misma, de modo que permanecen independientes de cualquier tecnología de red física particular. Además, incluyen la capacidad para recoger y

comunicar información necesaria para gestionar y entregar servicios por las redes de IPCable2Home. En esta Recomendación se define una entidad lógica sencilla denominada elemento de servicios de portal (PS, *portal service*).

5.1.2.1 Servicios de portal (PS)

Un portal es un elemento lógico que proporciona al mismo tiempo la seguridad, la gestión, la configuración y los servicios de direccionamiento. Se definen tres conjuntos de funciones de servicios de portal; a saber: el conjunto de funciones de gestión, el de calidad de servicio (QoS, *quality of service*) y el de seguridad. El elemento lógico PS constituye el fundamento de la arquitectura de referencia lógica.

5.1.3 Clases de dispositivos

El marco de arquitectura también utiliza el concepto de clases de dispositivos para añadir un contexto tangible a los elementos lógicos y a las combinaciones de los mismos. El concepto de clase de dispositivo de IPCable2Home no impone restricciones a los dispositivos físicos o a las combinaciones de los elementos lógicos dentro de esos dispositivos. Gracias a las clases de dispositivos se pueden representar los grupos de elementos lógicos de una manera informativa, auque no se las considera definitivas o restrictivas.

En IPCable2Home, la clase de dispositivo HA representa la ubicación física del elemento lógico PS y permite que los elementos de red dentro del dominio de IPCable2Home interfuncionen con dispositivos IP de LAN. El dispositivo HA tiene una sola interfaz conforme con la parte de RF del módem de cable, un solo elemento lógico PS y puede tener cero o más interfaces IP de LAN.

Esta Recomendación también aborda los dispositivos IP de LAN que son representativos de los dispositivos IP convencionales previstos para funcionar en las redes domésticas, y se prevé que incluirán una pila de protocolos TCP/IP así como un cliente DHCP.

5.1.3.1 PS integrado y PS autónomo

Los dos componentes principales que pueden estar dentro de una pasarela particular, el módem de cable (CM, *cable modem*) DOCSIS y el elemento de servicios de portal (PS) pueden utilizar recursos de soporte físico y soporte lógico compartidos o independientes. El uso compartido de recursos entre el CM y el PS es lo que distingue el PS autónomo del PS integrado.

Un PS autónomo NO DEBE compartir componentes de soporte físico o soporte lógico con el CM. La separación del CM del PS autónomo DEBE reflejarse hacia el PS como una simple desconexión de su red WAN – es decir, el PS continuará totalmente funcional como si estuviera desconectado de la red WAN. De lo contrario, el PS se considerará integrado. Dadas estas definiciones, es posible que un PS pueda funcionar dentro del mismo gabinete físico de un CM, y aún así seguirse considerando como un PS autónomo.

El CM y el PS se consideran elementos independientes en ambos casos, autónomo e integrado, y responden a direcciones de gestión únicas. En el caso integrado, el CM y el PS pueden compartir componentes de soporte físico o soporte lógico, pero desde la perspectiva de gestión resultan entidades independientes.

En la figura 5-2 se ilustran ambos casos y la combinación de un CM y un PS se considera que engloba el concepto del dispositivo HA. En otras palabras, un HA consta de un solo CM y un solo PS. Esta suposición de un PS por cada CM se mantiene aun para el PS autónomo, es decir, se supone que se conecta sólo un PS autónomo a un CM.

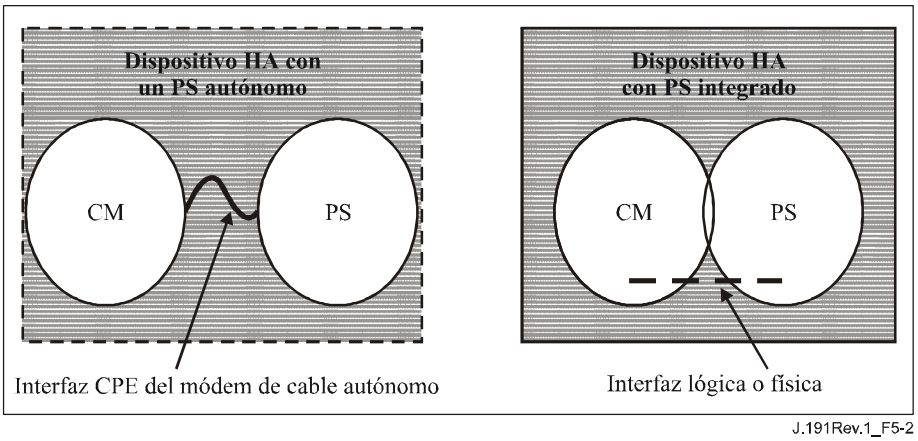


Figura 5-2/J.191 – PS autónomo y PS integrado

5.1.4 Sector de direcciones

El sector de direcciones se define como "el dominio de la red en el que las direcciones de red se asignan unívocamente a entidades susceptibles de recibir datagramas dirigidos a ellas" [RFC 2663]. En la presente Recomendación, los sectores de direcciones se clasifican en sector de direcciones de la WAN y sector de direcciones de la LAN (véase la figura 5-3).

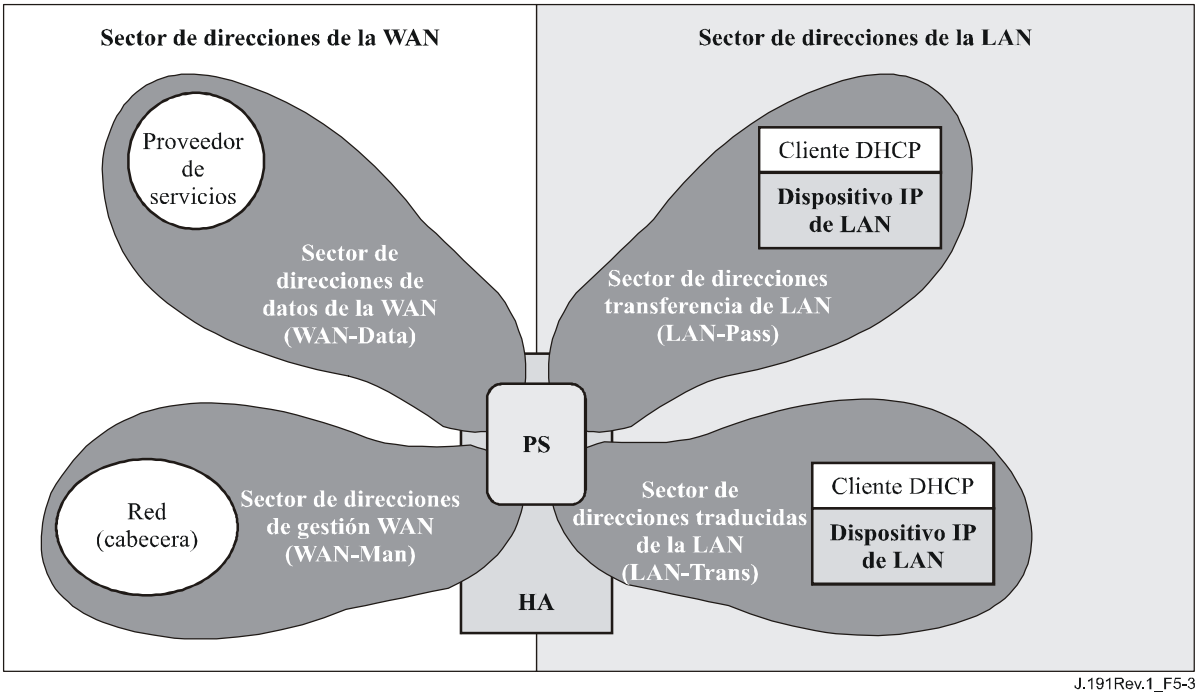


Figura 5-3/J.191 – Sector de direcciones

Las direcciones de la WAN pertenecen a uno de los dos siguientes sectores: el sector de direcciones de gestión de la WAN (WAN-Man) o el sector de direcciones de datos de la WAN (WAN-Data). Las direcciones de la LAN pertenecen asimismo a uno de los siguientes sectores: el sector de direcciones transferencia de la LAN (LAN-Pass, *pass-though LAN address*) o el sector de direcciones traducidas de la LAN (LAN-Trans). Las propiedades de estos sectores de direccionamientos son las siguientes:

- El sector de direcciones de gestión de la WAN (WAN-Man, *WAN management address realm*) tiene por objeto transportar por la red de cable el tráfico de gestión de la red entre el sistema de gestión de la red y el elemento PS. Las direcciones de este sector suelen pertenecer al espacio privado de direcciones IP.
- El sector de direcciones de datos de la WAN (WAN-Data, *WAN data address realm*) tiene por objeto transportar por la red de cable el tráfico de la aplicación del abonado y, más allá de ésta, tráfico tal como el existente entre los dispositivos IP de LAN y los servidores de Internet. Las direcciones de este sector suelen pertenecer al espacio público de direcciones IP.
- El sector de direcciones traducidas de la LAN (LAN-Trans, *translated LAN address realm*) tiene por objeto transportar tráfico de la aplicación del abonado y de gestión por la red doméstica entre los dispositivos IP de LAN y el elemento PS. Las direcciones de este sector suelen pertenecer al espacio de direcciones IP privadas, y es normal que las reutilicen distintos abonados.
- El sector de direcciones transferencia de la LAN (LAN-Pass) tiene por objeto transportar tráfico de la aplicación del abonado, como por ejemplo el tráfico entre los dispositivos IP de LAN y los servidores de Internet, por la red doméstica, la red de cable e incluso fuera de éstos. Las direcciones de este sector suelen pertenecer al espacio público de direcciones IP.

En el lado de la LAN, las direcciones del sector de direcciones transferencia de la LAN (LAN-Pass) se extraen directamente de las direcciones del sector de direcciones de datos de la WAN. Éstas son utilizadas por los dispositivos IP de LAN y por aplicaciones tales como los servicios IPCablecom que no soportan la traducción de direcciones y necesitan una dirección IP direccionable mundialmente. Además, en el lado de la LAN, los dispositivos IP de LAN pueden utilizar direcciones traducidas del sector de direcciones traducidas de la LAN (LAN-Trans).

A las interfaces LAN físicas del PS se les asigna un índice conforme con la MIB del grupo de interfaces [RFC 2233] como se describe en 6.3.8. En 6.3.8 también se define una interfaz LAN virtual que agrega las interfaces LAN físicas para el PS. La dirección IP del lado de la LAN definida para el PS está "vinculada" a esta interfaz virtual. Las funciones DHCP de PS y del servidor de nombres de dominio, y la función de encaminador del PS, son aplicaciones implementadas en el PS direccionado mediante la dirección IP del lado de la LAN vinculada a la interfaz LAN virtual.

5.2 Modelo de referencia funcional de IPCable2Home

Las funciones de IPCable2Home son servicios (capa 3 y superiores) definidos para IPCable2Home. Las mismas se ubican dentro del PS, los dispositivos IP de LAN y la cabecera. Existen funciones de IPCable2Home para cada uno de los ámbitos de especificación principales: configuración y gestión, seguridad y calidad de servicio. Las funciones de configuración y gestión, seguridad y QoS se describen brevemente en las siguientes tres cláusulas.

5.2.1 Funciones de gestión

Para dar soporte a la configuración y gestión de dispositivos de IP de LAN dentro del hogar, se definen tres clases de funciones de gestión:

- Funciones de gestión del servidor.

- Funciones de gestión del cliente.
- Funciones de gestión del portal.

Hay varias funciones de gestión del servidor que pertenecen a la cabecera (HE, *headend*). Las funciones de gestión del cliente se suelen encontrar dentro de los dispositivos IP de LAN. Las funciones de gestión del portal se encuentran en el elemento lógico PS, pudiendo incluir funcionalidades tipo servidor, tipo cliente y tipo enlace para agregar y traducir mensajes entre la cabecera y los dispositivos IP de LAN. La figura 5-4 muestra ejemplos de las funciones de gestión cliente, servidor y PS de los cuadros 5-1, 5-2 y 5-3.

Cuadro 5-1/J.191 – Descripción de las funciones de gestión servidor

Funciones de gestión servidor	Descripción
Servidor DHCP de cabecera	El servidor DHCP es un componente de la cabecera que proporciona al PS información sobre direcciones correspondiente a los sectores de dirección WAN-Man y WAN-Data.
Servidor de mensajería de gestión de la cabecera	Servidores de mensajería, descarga y notificación de eventos de la gestión de la cabecera incluidos protocolos tales como SNMP, SYSLOG y TFTP.

Cuadro 5-2/J.191 – Descripción de las funciones PS de gestión y configuración

Funciones de gestión portal	Descripción
Portal de dirección del cable (CAP, *cable address portal*)	En el PS, el CAP interconecta los sectores de direcciones de la WAN y de la LAN para el tráfico de datos (véase CAT/transferencia).
Traducción de dirección del cable (CAT, *cable address translation*)	CAT es una subfunción de la CAP que traduce direcciones del lado WAN-Data del CAP a direcciones de una única subred lógica del lado LAN-Trans.
Transferencia	Subfunción del CAP que hace de puente para los paquetes del lado WAN-Data del CAP con destino al lado LAN-Pass sin introducir modificaciones.
Portal de gestión del cable (CMP, *cable management portal*)	Función que proporciona la interfaz entre el operador y la base de datos del PS.
Portal DHCP del cable (CDP, *cable DHCP portal*)	Funciones de información de direcciones (por ejemplo, las transmitidas mediante DHCP) entre ellas un servidor para el sector LAN y un cliente para los sectores WAN.
Portal de denominaciones del cable (CNP, *cable naming portal*)	El CNP proporciona un servicio DNS sencillo para los dispositivos IP de LAN que requieran servicios de denominación.
Portal de prueba del cable (CTP, *cableHome testing portal*)	El CTP proporciona un medio remoto para iniciar verificaciones de direcciones Internet (pings) y bucles dentro de la LAN.

Cuadro 5-3/J.191 – Descripción de las funciones de gestión cliente

Funciones de gestión cliente	Descripción
Cliente DHCP del dispositivo IP de LAN	La función cliente DHCP del cable es un componente interno al hogar utilizado durante el proceso de configuración del dispositivo IP de LAN para solicitar dinámicamente direcciones IP e información de configuración de otros elementos lógicos.
Respondedor de bucle del dispositivo IP de LAN	Dentro de un dispositivo IP de LAN, el respondedor de bucle devuelve los datos procedentes de la función de bucle del CTP a esta misma.

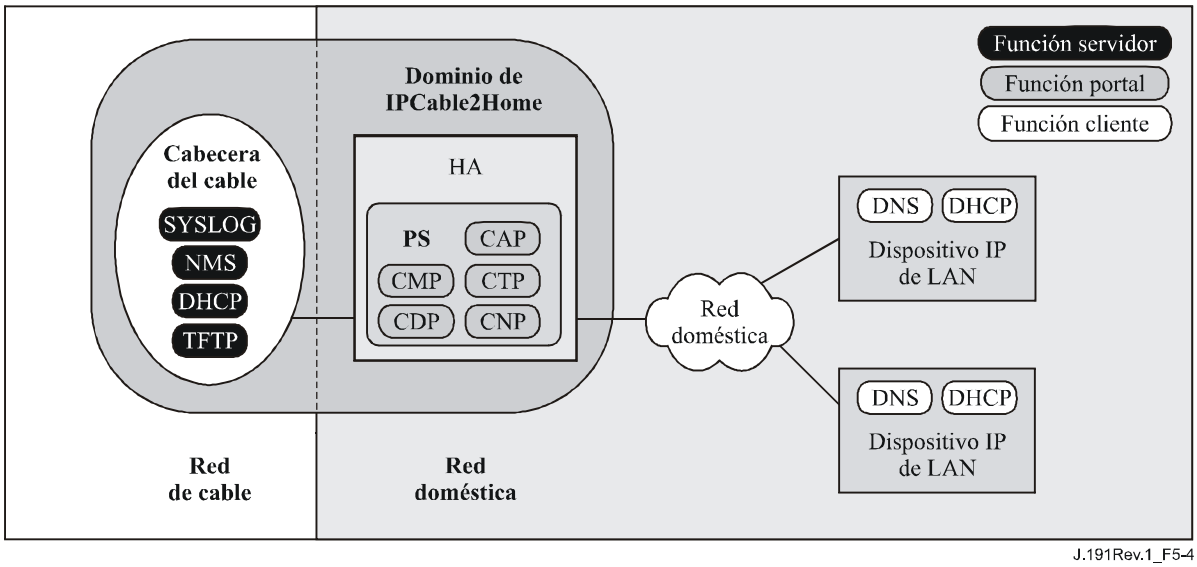


Figura 5-4/J.191 – Elementos de gestión

5.2.2 Funciones de seguridad

Para soportar los requisitos de seguridad de IPCable2Home, se definen dos clases de funciones de seguridad:

- Funciones de servidor de seguridad (Kerberos, centro de distribución de claves).
- Funciones de portal de seguridad.

Las funciones del servidor de seguridad residen en la cabecera (HE), y las funciones de portal de seguridad consisten en funciones tipo cliente que residen en el PS. En los cuadros 5-4 y 5-5 se introducen ejemplos de funciones de servidor de seguridad y de portal de seguridad, mismos que se ilustran en la figura 5-5.

Cuadro 5-4/J.191 –Descripción de la función portal de seguridad

Funciones portal de seguridad	Descripción
Portal de seguridad del cable (CSP, *cable security portal*)	El CSP se comunica con los servidores de seguridad de la cabecera, e incluye funciones que permiten la participación del lado cliente en los procesos de autenticación, intercambio de claves y gestión de certificados que se definen en IPCable2Home. Otras funciones de seguridad incluyen procesos de seguridad de mensajes de gestión, participación en la descarga asegurada, y gestión de barreras contra fuegos distantes.
Barrera contra fuegos (FW, *firewall*)	La barrera contra fuegos ofrece la funcionalidad que protege la red doméstica contra ataques malintencionados.

Cuadro 5-5/J.191 – Descripción de la función servidor de seguridad

Funciones servidor de seguridad	Descripción
Servidores de centro de distribución de cables (KDC, *key distribution center*) de la cabecera	Los servidores KDC de la cabecera ofrecen servicios de seguridad al CSP e incluyen funciones que intervienen en los procesos de autenticación y de intercambio de claves definidos por IPCable2Home.

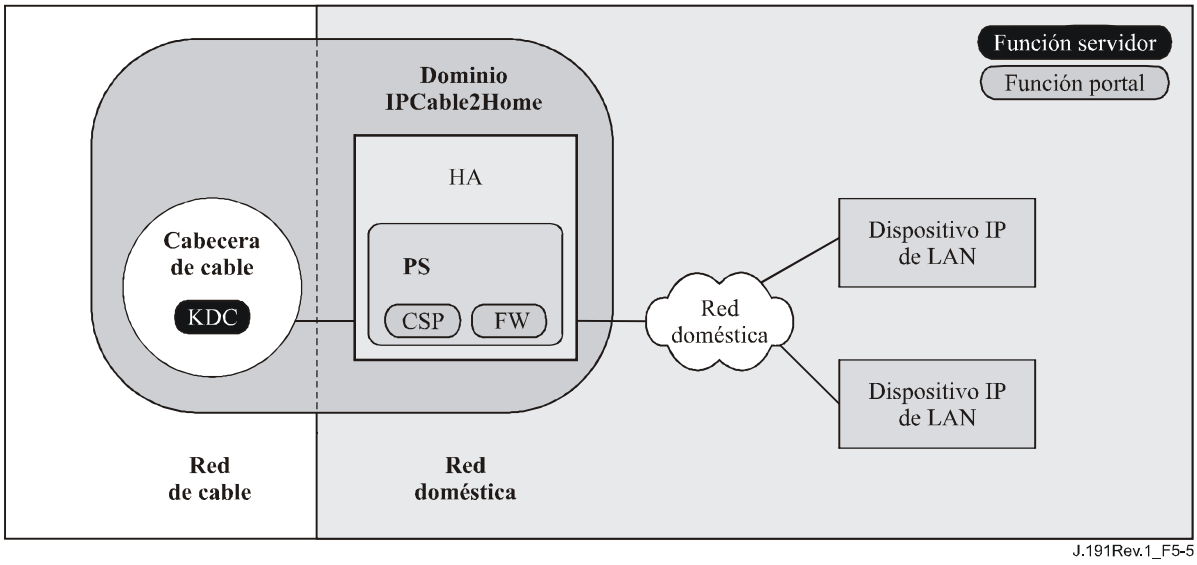


Figura 5-5/J.191 – Elementos de seguridad

5.2.3 Funciones QoS

La arquitectura QoS se compone de una sola entidad funcional basada en el PS denominada portal QoS de IPCable2Home (CQP, *cable QoS portal*). El CQP proporciona puenteo transparente para la mensajería QoS entre las aplicaciones IPCablecom y la infraestructura QoS IPCablecom de la red de cable.

5.3 Modelo de la interfaz de mensajería de IPCable2Home

La comunicación entre las funciones de los elementos de red de IPCable2Home y de los dispositivos IP de LAN se produce a través de interfaces de mensajería. Los tipos de interfaz de mensajería se distinguen por los elementos que intervienen en la comunicación. Las interfaces de mensajería se ilustran en la figura 5-6.

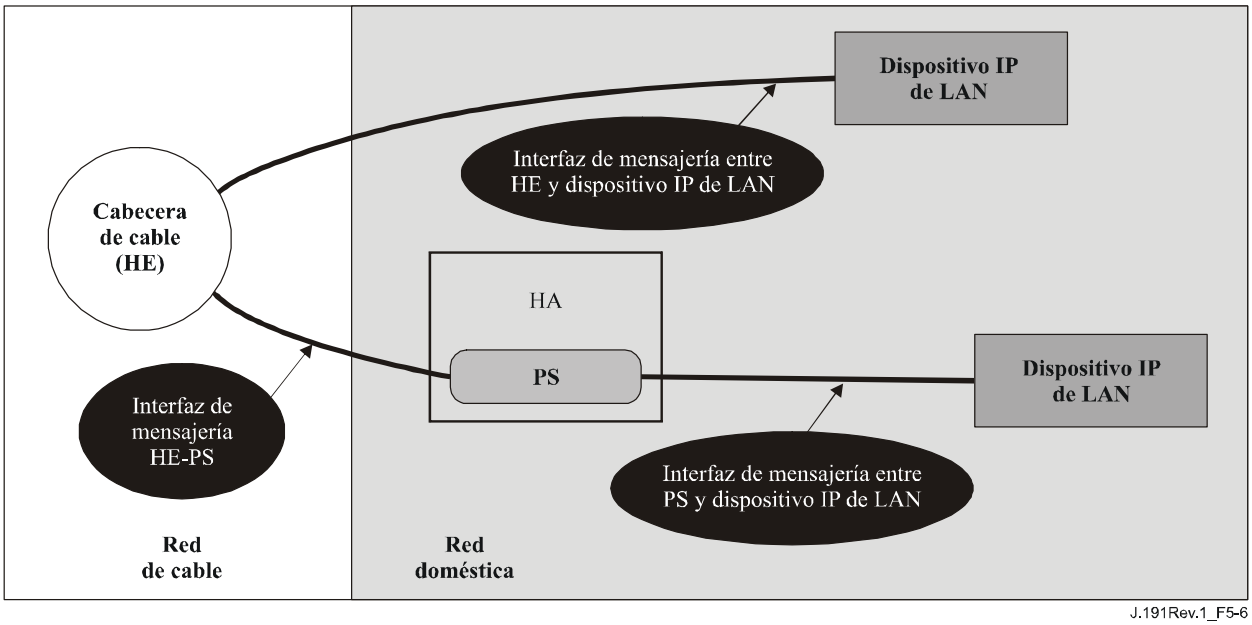


Figura 5-6/J.191 – Interfaces de referencia

Las interfaces de mensajería de IPCable2Home se resumen en el cuadro 5-6.

Cuadro 5-6/J.191 – Trayectos de interfaz válidos para cada funcionalidad

Funcionalidad	Protocolo	Interfaz		
		HE-PS	HE-Dispositivo IP de LAN	PS-Dispositivo IP de LAN
Nombre del servicio	DNS	Sin especificar	Sin especificar	Esta Recomendación
Descarga de soporte lógico	TFTP	Esta Recomendación	Sin especificar	Sin especificar
Adquisición de direcciones	DHCP	Esta Recomendación	Sin especificar	Esta Recomendación
Gestión (sencilla) (en bloque)	SNMP TFTP	Esta Recomendación Esta Recomendación	Sin especificar	Sin especificar
Notificación de eventos	SNMP SYSLOG	Esta Recomendación Esta Recomendación	Sin especificar	Sin especificar
QoS	Protocolos QoS IPCablecom	Sin especificar	IPCablecom	Sin especificar
Seguridad (distribución de claves)	Kerberos	Esta Recomendación	Sin especificar	Sin especificar
Seguridad (autenticación)	Kerberos	Esta Recomendación	Sin especificar	Sin especificar
Ping	ICMP	Esta Recomendación	Sin especificar	Esta Recomendación
Bucle/Eco	UDP/TCP	Sin especificar	Sin especificar	Esta Recomendación

5.4 Modelo de referencia de información de IPCable2Home

El funcionamiento del modelo de gestión se basa en la información almacenada en el PS por las diversas funciones PS (CAP, CDP, CMP, etc.). Dichas funciones deben poder interactuar a través del intercambio de información, representando la base de datos PS una entidad conceptual que almacena esta información. La base de datos PS no es propiamente una base de datos con especificaciones reales sino un instrumento auxiliar para explicar el significado de la información que se intercambian entre los diversos elementos.

La figura 5-7 muestra la relación entre la base de datos y las funciones PS, el cuadro 5-7 describe la información que suele asociarse a cada una de estas funciones. La figura 5-8 muestra un ejemplo detallado de implementación que indica el conjunto de información, las funciones que obtienen la información y las relaciones entre las funciones y la información.

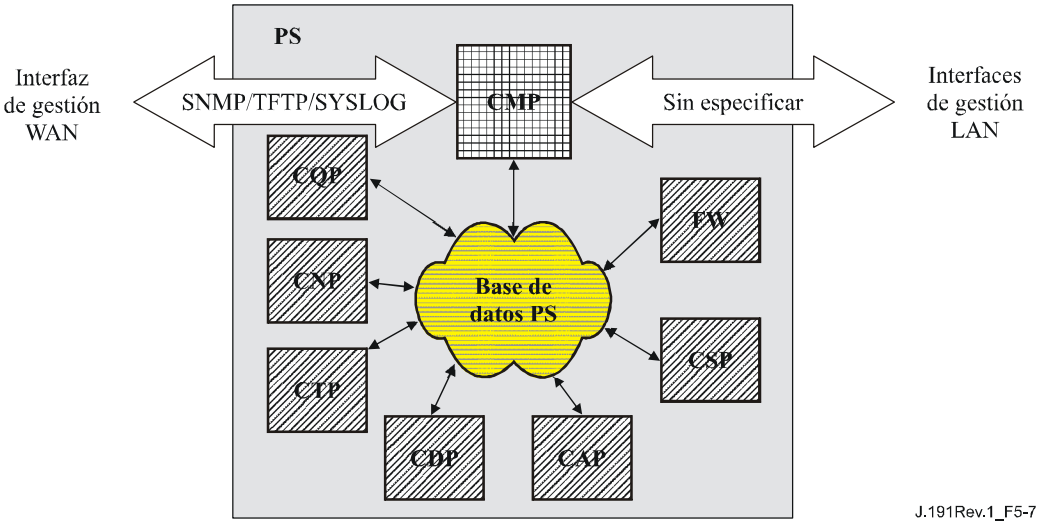


Figura 5-7/J.191 – Relación entre las funciones PS y la base de datos PS

La base de datos del PS almacena una gran cantidad de relaciones de datos. El CMP proporciona la interfaz de gestión de WAN (SNMP) con la base de datos PS. Las funciones del PS acceden en la base de datos del PS y revisan las relaciones entre los datos. Adicionalmente, las funciones del PS pueden recuperar información de la base de datos del PS que son mantenidas por otras funciones IPCable2Home en el PS.

Cuadro 5-7/J.191 – Ejemplos característicos de la información de la base de datos del PS

Nombre	Utilización (en general)
Información del CDP	Información asociada a direcciones adquiridas y asignadas mediante DHCP
Información del CAP	Información asociada a la correspondencia por traducción de direcciones de IPCable2Home
Información del CMP	Información asociada al estado de las funciones de gestión
Información del CTP	Información asociada a los resultados de las pruebas sobre la LAN efectuadas por el CMP
Información del CNP	Información asociada a la resolución del nombre del dispositivo IP de LAN
Información del USFS	Información asociada a la función de conmutación de entrega selectiva hacia el origen
Información del CSP	Información asociada a la autenticación, intercambio de claves, etc.
Información de la barrera contra fuegos	Información asociada al comportamiento de la barrera contra fuegos (conjunto de reglas) y al registro histórico de la barrera contra fuegos
Información de eventos	Información asociada al registro histórico local para todos los eventos, trampas, etc. de carácter general

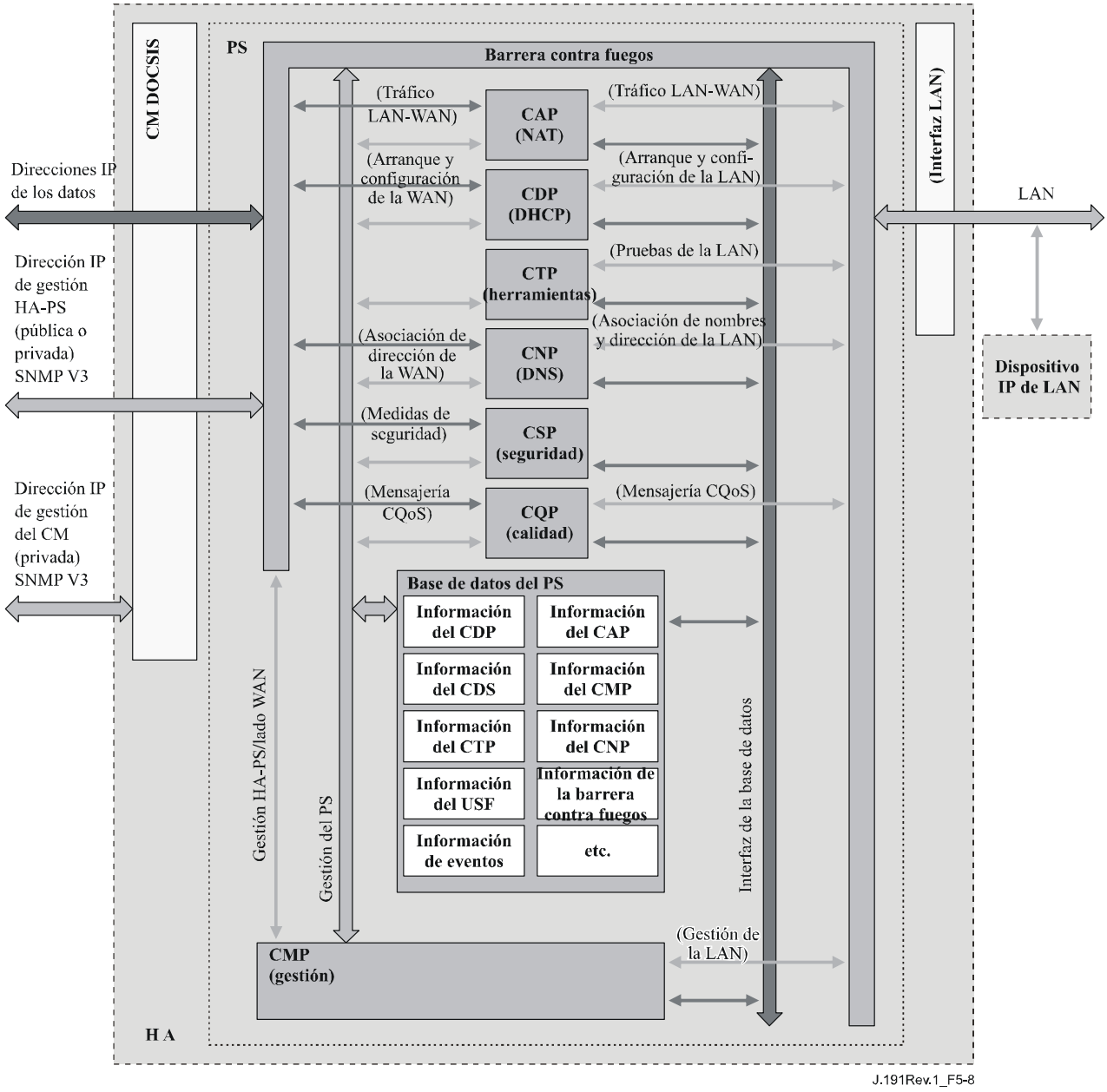


Figura 5-8/J.191 – Ejemplo detallado de implementación de la base de datos del PS

El PS se gestiona desde la WAN a través del CMP, lo que en gran medida supone el acceso a la información contenida en la base de datos del PS. La gestión tiene por objeto la inicialización y configuración de los elementos de la red del lado WAN por una parte, y de los diagnósticos y estado de la LAN de otra. Los diagnósticos pueden apoyarse en el CTP para conocer con más detalle el estado actual de la LAN. Se puede medir la conectividad y la calidad de funcionamiento elemental de la red.

El CNP es el gestor del sistema de nombres de dominio (DNS, *domain name system*) de la LAN. El CDP configura todos los dispositivos IP de LAN del sector LAN-Trans utilizando el CNP como servidor de nombres primario. El CNP resuelve los textos de los nombres de servidor de los dispositivos IP de LAN, y devuelve las correspondientes direcciones IP y además entrega a servidores DNS externos las peticiones de los dispositivos IP de LAN que no puedan satisfacerse a partir de la información local.

El CDP contiene las funciones de dirección que dan soporte al servidor DHCP en el sector LAN-Trans y a los clientes DHCP en los sectores de la WAN.

El CAP crea correspondencias de traducción de direcciones entre los sectores de direcciones WAN-Data y LAN-Trans. El CAP se encarga asimismo de las decisiones del conmutador de entrega selectiva hacia el origen orientadas a preservar la anchura de banda del canal HFC hacia el origen (WAN) frente al tráfico de la LAN exclusivamente local. Por último, el CAP contiene la función transferencia que actúa de puente para el tráfico entre los sectores de direcciones de la LAN y de la WAN.

El CSP provee al PS de capacidades de autenticación, así como de actividades de intercambio clave.

El CQP forma parte de un sistema que permite establecer la calidad de servicio (QoS) IPCablecom en el PS. El CQP actúa como un puente transparente que permite el paso de la mensajería QoS homologada con IPCablecom entre las aplicaciones IPCablecom y la infraestructura de QoS IPCablecom.

5.5 Modelos operacionales de IPCable2Home

La funcionalidad del elemento de servicios de portal es compatible con una diversidad de infraestructuras de red de cable, que se adaptan mediante distintos modos de operación del PS. Estos modos de operación permiten que el PS funcione adecuadamente en la infraestructura del módem de cable, y en la infraestructura del IPCable2Home ampliada. La infraestructura de IPCable2Home ampliada se construye sobre una infraestructura de módem de cable proporcionando servicios adicionales e incorporando capacidades semejantes a las de los sistemas de configuración IPCablecom.

A efectos de la configuración, el PS puede funcionar, en uno de los dos modos de configuración siguientes:

- El modo de configuración DHCP.
- El modo de configuración SNMP.

Si el PS no recibe la información necesaria para determinar el modo de configuración, operará con funcionalidad reducida en el modo CableHome aletargado.

Cuando el PS funciona en el modo de configuración DHCP, puede hacerlo en uno de los submodos de gestión de la red siguientes:

- Modo NmAccess.
- Modo de coexistencia.

La figura 5-9 muestra los diversos modos operacionales del PS junto con los activadores asociados a cada de uno de ellos. Véase 6.3.6.1.1.

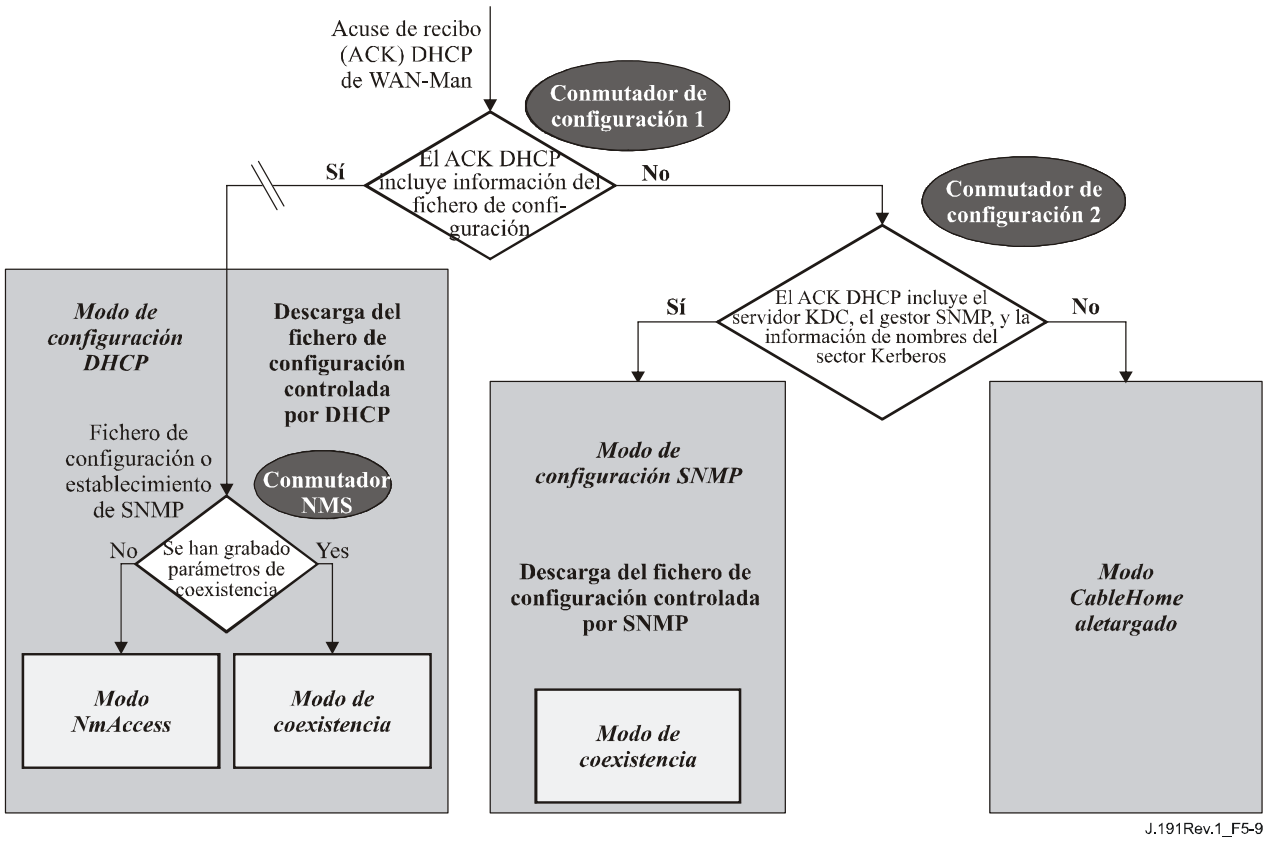


Figura 5-9/J.191 – Modos operacionales del PS

Si la información del fichero de configuración del PS (ubicación del servidor y nombre del fichero) se suministra al PS pero no se suministra información del servidor Kerberos, en el ACK DHCP emitido por el servidor DHCP de la red de cable, el PS funcionará en el modo de configuración DHCP. Cuando se encuentre en el modo de configuración DHCP, el PS podrá funcionar en uno de los dos modos de gestión de red (el NmAccess y la coexistencia). En el modo de configuración DHCP, el PS funcionará por defecto en el modo de gestión de red de NmAccess, aunque el NMS podrá configurarlo para funcionar en el modo de coexistencia.

Si se suministra información del servidor Kerberos y no se suministra información del fichero de configuración del PS a éste en el ACK DHCP emitido por el servidor DHCP de la red de cable, el PS funcionará en el modo de configuración SNMP. Cuando funcione en dicho modo, la información y los activadores de descarga del fichero de configuración del PS los suministrará el NMS por medio de mensaje SNMP. A diferencia del modo de configuración DHCP, en este modo no se modifica el comportamiento de la gestión de la red.

Si se suministra al PS la combinación errónea de información de servidor Kerberos y del fichero de configuración del PS en el ACK DHCP emitido por el servidor DHCP de la red de cable, el PS pasará a funcionar por defecto en el modo CableHome aletargado. Durante este modo, el PS utilizará parámetros de configuración almacenados localmente. Si el PS no ha sido aún configurado, funcionará con los parámetros de fábrica por defecto.

En el cuadro 5-8 se describen las infraestructuras en las que se pretende que funcione cada uno de los modos del PS.

Cuadro 5-8/J.191 – Infraestructuras del PS

Modo	Capacidad directamente afectada	Infraestructura que se pretende
Modo de configuración SNMP	Descarga del fichero de configuración	Infraestructura de IPCable2Home ampliada
Modo de configuración DHCP	Descarga del fichero de configuración	Infraestructuras DOCSIS 1.0 y 1.1
Modo de configuración DHCP: Modo NmAccess	Versión de SNMP utilizada entre el NMS y el PS	Infraestructura DOCSIS 1.0 (SNMPv1/v2)
Modo de configuración DHCP: Modo de coexistencia SNMP	Versión de SNMP utilizada entre el NMS y el PS	Infraestructuras DOCSIS 1.1 y de IPCable2Home ampliada (SNMPv3)
Modo CableHome aletargado	Gestión de SNMP desde la interfaz WAN	Cualquier infraestructura de red de cable que no soporte la configuración y la gestión de CableHome

5.6 Interfaces físicas de IPCable2Home

Hay diversos tipos de interfaces físicas que pueden aplicarse a un dispositivo que dispone de funcionalidad PS. Varios de éstos se describen en la siguiente relación:

- Interfaces de funcionamiento en red WAN, que incluyen la interfaz de radiofrecuencias (RFI, *radio frequency interface*) conforme a la Rec. UIT-T J.112 (o Rec. UIT-T J.122) para el caso del PS integrado y otras interfaces de funcionamiento en red WAN que se utilizarán para la conexión WAN en el caso de PS autónomo.
- Interfaces de funcionamiento en red LAN para conexión a dispositivos IP de LAN.
- Interfaces de prueba de soporte físico, como la del JTAG (*joint test action group*) y de otros métodos patentados, que forman parte de los equipos propiamente dichos y no siempre disponen de controles de soporte físico para desactivarlas. Esas interfaces son máquinas de estado de soporte físico que permanecen en un estado pasivo hasta que se registran datos en sus líneas de entrada. No obstante que estas interfaces pueden utilizarse para leer y escribir datos, se requiere un conocimiento detallado de los circuitos integrados y de la disposición de las tarjetas y, por consecuencia, es difícil que sufran "ataques". Las interfaces de prueba de soporte físico PUEDEN incluirse en un dispositivo con funcionalidad DPS. Estas interfaces NO DEBEN etiquetarse o documentarse para uso de los clientes.
- Interfaces de acceso a la gestión, también denominadas puertos de consola, que son trayectos de comunicaciones (por lo general RS-232, pero podría tratarse de Ethernet, etc.) y soporte lógico de depuración que interactúa con un usuario. El soporte lógico señala al usuario que puede introducir datos y acepta instrucciones para leer y escribir datos en el PS. Si el soporte lógico para esta interfaz se desactiva, igualmente se desactiva el trayecto físico de comunicaciones. Un PS NO DEBE dar acceso a funciones del PS a través de la interfaz de acceso a la gestión. El acceso a las funciones de PS sólo se permitirá a través de las interfaces prescritas específicamente para ese fin en esta Recomendación, por ejemplo, el acceso controlado por el operador mediante SNMP.
- Las interfaces de diagnóstico para lectura únicamente pueden aplicarse de muchas maneras y se utilizan para facilitar la depuración, la localización y reparación de averías, y proporcionar la información de estado del PS hacia los usuarios. Un PS PUEDE tener interfaces de diagnóstico de sólo lectura.
- Es posible que en algunos productos se decida implementar funciones de capa superior (como es el caso de las funciones de la red de datos en las instalaciones del cliente) que podrían requerir configuración a través del usuario. Un PS PUEDE ofrecer la capacidad para configurar funciones distintas de IPCable2Home. El acceso de la interfaz de gestión

(lectura/escritura) a las funciones del PS NO DEBE permitirse a través del mecanismo que se emplea para configurar las funciones que no pertenecen a IPCable2Home.

6 Herramientas de gestión

6.1 Introducción y presentación

Las herramientas de gestión dotan al operador de cable de la funcionalidad de supervisar y configurar el elemento de servicios de portal (PS) IP, así como de ejecutar diagnósticos a distancia sobre dispositivos IP de LAN. En esta cláusula se describen y especifican los requisitos para dichas capacidades.

6.1.1 Objetivos

Entre los objetivos de las herramientas de gestión se encuentran los siguientes:

- Dotar a los operadores de cable de visibilidad sobre los dispositivos IP de LAN.
- Dotar a los operadores de cable de un conjunto mínimo de herramientas de diagnóstico a distancia que le permitan verificar la conectividad entre el elemento de servicios de portal y cualquier dispositivo IP de LAN del sector de direcciones LAN-Trans.
- Dotar a los operadores de cable, a través las MIB, de acceso a los datos internos del elemento PS permitiéndole supervisar parámetros específicos y configurar, o reconfigurar, capacidades específicas cuando sea necesario.
- Ofrecer un medio de comunicación de excepciones y otros eventos en forma de trampas SNMP, mensajes a un registro histórico local o mensajes a un registro histórico del sistema (SYSLOG) de la red de cable.

6.1.2 Hipótesis

Entre las hipótesis definidas para el entorno de gestión de la red se encuentran las siguientes:

- Los dispositivos homologados de IPCable2Home implementan el conjunto de protocolos Internet (IPv4, *Internet protocol*).
- Para el intercambio de mensajes de gestión entre el NMS de la red de cable y el PS en el dispositivo HA se utiliza SNMP. El SNMP permite observar al NMS las interfaces del PS, mediante el acceso a datos internos del PS, a través de las MIB necesarias.
- Se puede utilizar SNMPv1/v2c/v3 como protocolo de gestión entre el NMS y el elemento servicios de portal.
- Los dispositivos IP de LAN implementan un cliente DHCP.
- La información obtenida gracias al intercambio de los mensajes DHCP DISCOVER, DHCP REQUEST y DHCP OFFER, intercambiados entre el PS y los dispositivos IP de LAN, y la información disponible en la base de datos del PS (véase 5.4) a través de la MIB del grupo de interfaces son suficientes para ofrecer al operador de cable los conocimientos necesarios sobre los dispositivos IP de LAN.
- El elemento PS y los dispositivos IP de LAN soportan ICMP.
- La utilidad PING ofrece la funcionalidad suficiente para proporcionar al operador de cable la información necesaria sobre conectividad entre el elemento PS y los dispositivos IP de LAN.

6.2 Arquitectura de gestión

6.2.1 Directrices de diseño del sistema

El cuadro 6-1 contiene las directrices del diseño del sistema de herramientas de gestión de IPCable2Home. Esta relación sirve de orientación para el desarrollo de las especificaciones de las herramientas de gestión.

Cuadro 6-1/J.191 – Directrices de diseño del sistema de herramientas de gestión

Referencia	Directrices de diseño del sistema de herramientas de gestión
Mgmt 1	El PS implementará SNMPv1/v2c/v3 para facilitar el acceso a los datos internos de los servicios de portal.
Mgmt 2	El PS deberá ser capaz de emitir un mandato Ping ICMP destinado a cualquier dispositivo IP de LAN específico del sector LAN-Trans en la dirección del NMS de la red de cable y de almacenar los resultados en la base de datos PS. Los resultados de las pruebas de Ping distante deberán ser accesibles a través de los objetos de la MIB del CTP cabhCtpPingStatus, cabhCtpPingNumSent, y cabhCtpPingNumRecv.
Mgmt 3	El PS deberá ser capaz de ejecutar una prueba de velocidad de conexión con un dispositivo IP de LAN específico en el sector de direcciones LAN-Trans en la dirección del NMS de la red de cable y almacenar los resultados en la base de datos del PS.
Mgmt 4	El elemento PS deberá ser capaz de comunicar los eventos que se produzcan.

6.2.2 Descripción del sistema de herramientas de gestión

De acuerdo con lo representado en la figura 6-1, la arquitectura de las herramientas de gestión consta de los siguientes componentes:

1) el portal de gestión del cable (CMP);
2) el portal de prueba del cable (CTP);
3) un mecanismo de comunicación de eventos dentro del CMP; y
4) un sistema de gestión de la red (NMS) SNMP que forme parte de la red de cable.

El NMS de la red de cable supervisa y configura el PS accediendo a la base de datos del PS a través de las MIB especificadas en 6.3.7. Asimismo, el NMS puede comunicarse directamente con dispositivos IP de LAN del sector de direcciones LAN-Pass.

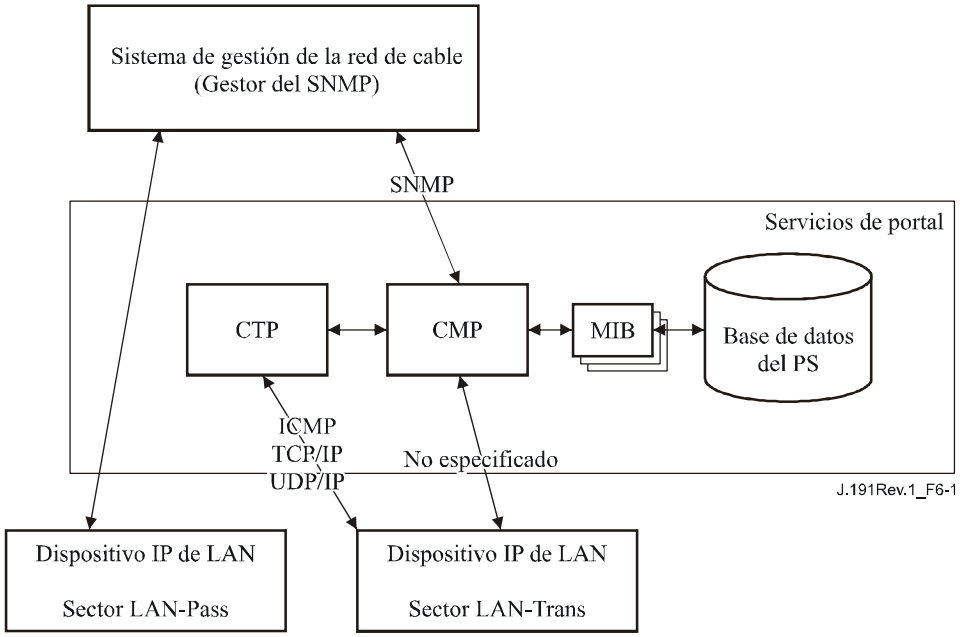


Figura 6-1/J.191 – Arquitectura de gestión

Los elementos funcionales CMP y CTP se encuentran en el interior del PS. El elemento lógico PS puede incorporarse o ser autónomo, con relación a la funcionalidad del módem de cable, conforme a la cláusula 5.

En ambos casos, desde el punto de vista de la gestión, el CM y el PS son entidades separadas e independientes, y no existe forzosamente la compartición de datos entre el CM y PS excepto en el caso de descarga de una imagen de soporte lógico en un PS incorporado. En este último caso, se accede a los objetos docsDevSoporte lógico del módem de cable para preparar la descarga de una única imagen de soporte lógico combinado, iniciarla y supervisarla. Gracias a la independencia de la gestión, el CM y el PS DEBEN responder a direcciones IP de gestión diferentes e independientes. Los objetos MIB del CM sólo son visibles cuando el gestor accede a ellos a través de la dirección IP de gestión del CM, pero no son visibles a través de la dirección IP de gestión del PS (y viceversa). Los derechos de acceso del SMNP a las entidades PS y CM DEBEN fijarse independientemente. El caso del PS incorporado no impide la utilización de un único agente SNMP.

El elemento de servicios de portal soporta los protocolos SNMPv1, SNMPv2c y SNMPv3. En 5.5 se presentan los dos modos de configuración soportados por un elemento de servicios de portal, y la cláusula 7 contiene detalles adicionales de estos modos. El modo de configuración en el que funciona parcialmente el PS determina la versión de SNMP que utiliza el PS. La cláusula 6.3.3 contiene más detalles al respecto.

6.3 El portal de gestión del cable (CMP)

El portal de gestión de cable (CMP) está dentro del PS y sirve de centro de distribución del control de gestión para los accesos de gestión del lado WAN. El CMP agrega e interconecta la información de gestión en los sectores WAN-Man y LAN-Trans ya que éstos no son mutuamente accesibles de un modo directo.

6.3.1 Objetivos del CMP

Entre los objetivos del portal de gestión de cable se encuentran los siguientes:

- Permitir al NMS la observación y actualización de la información de configuración del portal de dirección del cable (CAP).

- Permitir al NMS la visualización y actualización de la información de configuración de la barrera contra fuegos.
- Permitir el ping distante para los dispositivos IP de LAN del sector de direcciones LAN-Trans, a través del portal de prueba del cable (CTP).
- Permitir la visualización de la información del dispositivo IP de LAN obtenida a través del portal DHCP del cable (CDP).
- Permitir la visualización de los resultados de la supervisión de la calidad de funcionamiento del dispositivo IP de LAN efectuada por el portal de pruebas del cable (CTP).
- Permitir al NMS el acceso a otros parámetros de configuración del PS.
- Procesar los bloques de mandatos SNMP contenidos en un fichero de configuración del PS recibido del NMS de la red de cable.
- Facilitar la seguridad al permitir el acceso a los parámetros de seguridad, y mediante el uso de SNMPv1/v2c/v3 en el modo de gestión de red adecuado.
- Ofrecer la capacidad de desactivar segmentos de la LAN.

6.3.2 Directrices de diseño del CMP

El cuadro 6-2 contiene las directrices de diseño del CMP. Esta relación sirvió de orientación para la especificación de la funcionalidad CMP.

Cuadro 6-2/J.191 – Directrices de diseño del sistema CMP

Referencia	Directrices de diseño del sistema CMP
CMP 1	Las interfaces soportarán las características de gestión y diagnóstico y las funciones necesarias para soportar los servicios propios del cable que hayan de ser prestados en la red doméstica.
CMP 2	La desconexión entre el proveedor, o proveedores, de servicios de banda ancha y la red doméstica no desactivará ni degradará el funcionamiento de las funciones internas de la red doméstica.
CMP 3	La red doméstica se recuperará automáticamente tras un corte de corriente, debiendo volver los dispositivos conectados a dicha red al estado operacional en que se encontraban antes del corte.
CMP 4	Los dispositivos de la red doméstica serán de fácil instalación y configuración, como cualquier otro electrodoméstico.

6.3.3 Descripción del sistema CMP

Como se ha expuesto anteriormente, el CMP actúa como centro de distribución del control de gestión para los accesos de gestión del lado WAN y agrega información e interconecta la gestión de los elementos de gestión de la WAN y de la red LAN.

El CMP opera en uno de los siguientes modos de gestión de red.

Como se describe en 5.5, durante el modo de configuración SNMP, el PS funciona por defecto en el modo de coexistencia SNMPv3 con SNMPv1 y SNMPv2 desactivados, y emplea Kerberos para distribuir las claves. El modelo de seguridad del usuario (USM, *user security model*) [RFC 3414] y el modelo de control de acceso basado en vistas (VACM, *view-based access control model*) [RFC 3415] se soportan para permitir que el operador de cable pueda implementar las políticas de gestión para el acceso a las MIB especificadas para IPCable2Home.

Como se describe en 5.5, durante el modo de configuración de DHCP, el PS funciona por defecto en el modo del cuadro NmAccess, pero el operador de cable puede configurarlo para que funcione en el modo de coexistencia SNMPv3. En el modo del cuadro NmAccess, el acceso a la gestión se

controla mediante el cuadro NmAccess de RFC 2669 y se soportan los protocolos SNMPv1/v2c. Si el PS se configura de modo que funcione en el modo de coexistencia SNMPv3, el acceso a la gestión se controla conforme a RFC 2576, y se soportan los protocolos SNMPv1/v2c/v3, además de USM y VACM, y se distribuyen claves de SNMPv3 utilizando RFC 2786 y TLV en el fichero de configuración del PS.

Si el PS no recibe parámetros de decisión del modo de configuración SNMP o del modo de configuración DHCP y retrocede al modo CableHome aletargado, desactivará el acceso SNMP de sus interfaces WAN y responderá a cualquier mensaje SNMPv1 o SNMPv2c recibido en cualquier interfaz LAN.

El cuadro 6-3 contiene las definiciones de los términos específicos del CMP.

Cuadro 6-3/J.191 – Definición de los términos

Control de gestión	Acceso de lectura o escritura a un conjunto de parámetros que controla o supervisa el comportamiento del PS.
Base de datos del PS	Conjunto de parámetros que controla o supervisa el comportamiento del elemento PS pudiendo ser leído exclusivamente por el sistema de gestión de WAN. Puede considerarse como un depósito de información que describe el estado del PS en cada instante.
Usuario	De acuerdo con lo definido en SNMP (sección 2.1 de RFC 3414), un usuario tiene un nombre asociado, definiciones de seguridad asociadas y acceso a una vista.
Vista	Una vista es un conjunto de objetos de la MIB y de los derechos de acceso a los mismos. Cada vista tiene un nombre y está asociada a un usuario (sección 2.4 de RFC 3415).
Autorización final	Única autoridad que establece, modifica o suprime identificadores de usuario, claves de autenticación, claves de criptación y derechos de acceso a la base de datos del PS. Este usuario es responsable de todas las operaciones de gestión de seguridad.
Usuario de mantenimiento	Un usuario suele realizar únicamente operaciones de sólo lectura en la base de datos del PS. Esto se suele utilizar para supervisión de la calidad de funcionamiento y para funciones de contabilidad.
Usuario administrador	Usuario que suele efectuar operaciones tanto de lectura como de escritura en la base de datos del PS. Estas operaciones se utilizan para la configuración y la gestión de averías.

Como ejemplo de los tipos de información que se manejan a través del control de gestión del cable se pueden citar los valores de la política de la barrera contra fuegos, las correspondencias NAT configuradas por el NMS, el inicio de las herramientas de diagnóstico a distancia y el acceso a sus resultados, el estado del PS y la configuración del intervalo de direcciones de la LAN. Como se explicará más adelante, las diversas interfaces de mensajería de gestión pueden tener derechos de acceso a conjuntos de parámetros diferentes. Aunque es posible acceder a la base de datos del PS tanto desde la WAN como desde la LAN, no se especifica el acceso de la LAN. La figura 6-2 muestra interfaces de mensajería de gestión:

- NMS-CMP: intercambio de mensajes de gestión entre el NMS de la red de cable y el CMP.
- CMP-Dispositivo IP de LAN: intercambio de mensajes de gestión entre el CMP y los dispositivos IP de LAN en el sector de direcciones LAN-Trans (no especificado por IPCable2Home).
- NMS-Dispositivo IP de LAN: intercambio de mensajes de gestión entre el NMS de la red de cable y dispositivos IP de LAN en el sector LAN-Pass (no especificado por IPCable2Home).

- NMS- Dispositivo IP de LAN: intercambio de mensajes de gestión entre el NMS de la red de cable y dispositivos IP de LAN en el sector LAN-Trans (proporcionado por la configuración del CAP – véase 8.3.2). Esta mensajería no está especificada por IPCable2Home.

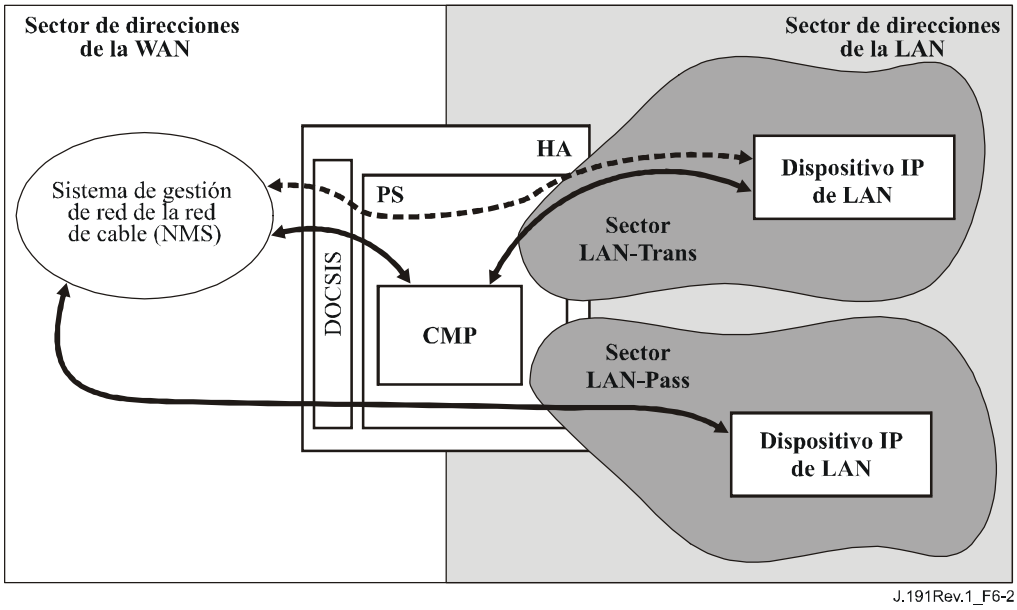


Figura 6-2/J.191 – Interfaces de los mensajes de gestión

El CMP es fundamentalmente una entidad a la que accede la WAN (NMS) y es controlada por ésta. Adicionalmente, se puede solicitar al CMP que informe al NMS de la red de cable de eventos o que transfiera ficheros históricos del sistema cuando sea necesario. La figura 6-3 muestra un ejemplo de implementación del CNP para ilustrar los conceptos de la funcionalidad CMP.

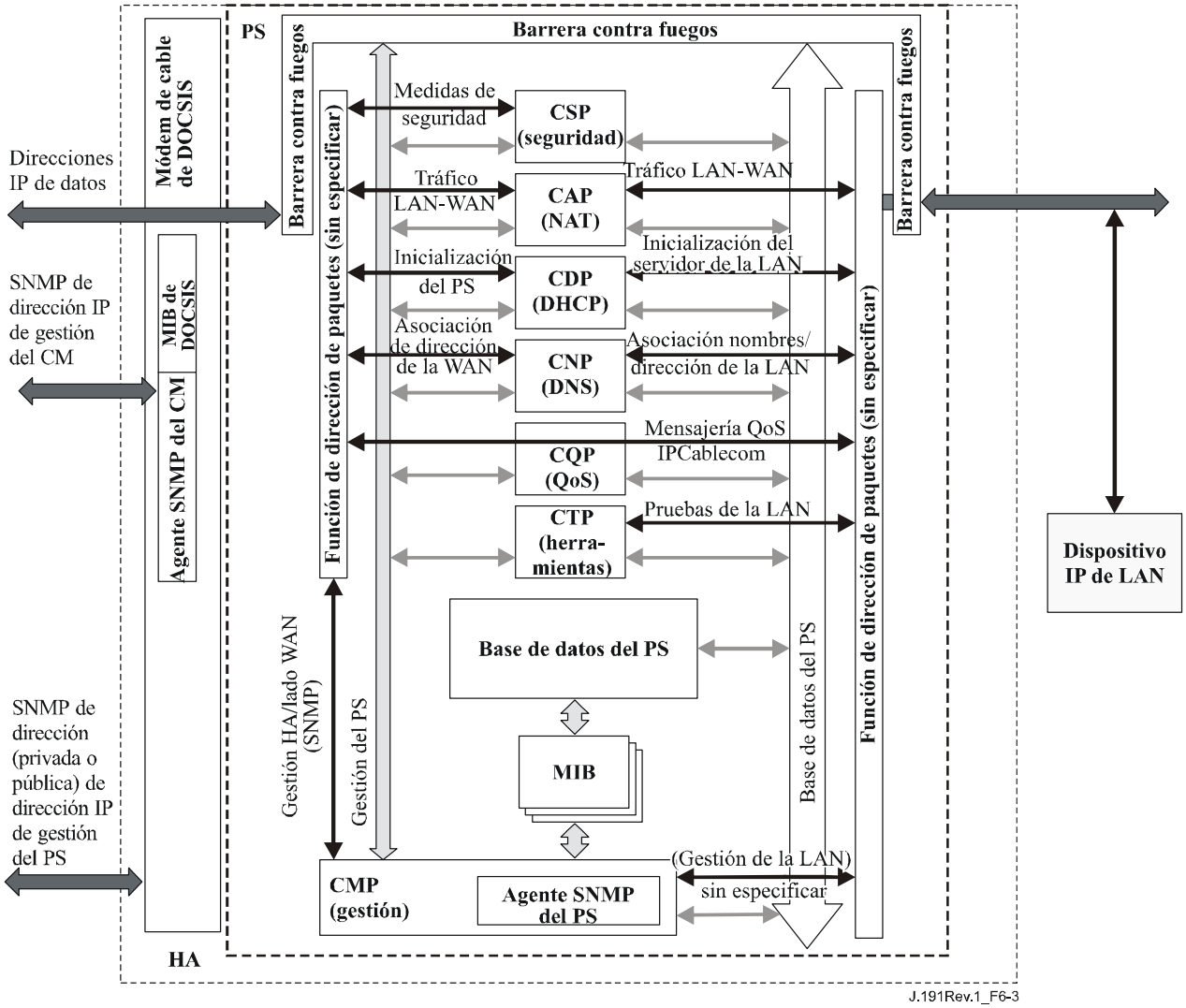


Figura 6-3/J.191 – Diagramas de bloque del PS

Las herramientas de gestión del NMS utilizan el SNMP para acceder a objetos del PS y gestionarlos. Si el PS está funcionando en el modo de coexistencia SNMPv3, el SNMPv3 otorga al operador del NMS autenticación de usuario del PS, acceso orientado a vistas de los objetos de la base de información de gestión (MIB) del PS y criptación de los mensajes de gestión cuando sea necesario.

Al CMP le corresponde la tarea de traducir el ID del objeto (OID, *object ID*) y el ejemplar del OID en todas las hojas de los bloques funcionales del PS, como por ejemplo el CAP o la memoria local tal como la base de datos del PS.

Además del CMP, un operador del NMS puede tener acceso o "gestionar" directamente dispositivos IP de LAN utilizando direccionamiento transferencia entre la cabecera y el dispositivo de LAN gestionado. No obstante, no es necesario que los dispositivos IP de LAN respondan a protocolos particulares, gestión o ninguna otra función concreta.

6.3.4 Requisitos generales del CMP

El PS DEBE aplicar tipos de mensajes de eco ICMP y de respuesta de eco (tipos 8 y 0) y tipos de mensajes de indicación de tiempo ICMP y de respuesta de indicación de tiempo (tipos 13 y 14) conforme a RFC 792, y responder adecuadamente a las solicitudes de verficaciones de direcciones de Internet (ping) recibidas en cualquier interfaz.

Si el PS está funcionando en el modo de configuración DHCP (indicado por el valor '1' de cabhPsDevProvMode) el CMP DEBE utilizar por defecto SNMPv1/v2c para la mensajería de gestión con el NMS y obedecer las reglas para el modo NmAccess y el de coexistencia descritas en 6.3.6.1.

Si el PS está funcionando en el modo de configuración SNMP (indicado por el valor '2' de cabhPsDevProvMode), el CMP DEBE utilizar SNMPv3 para la mensajería de gestión con el NMS, obedeciendo las reglas descritas en 6.3.6.2.

Cuando el PS funciona en el modo de coexistencia SNMP, el valor por defecto de la autorización final DEBE ser administrador WAN (administrador PS).

Cuando el PS funciona en el modo CableHome aletargado conforme a 5.5 y 7.2.3.3 y a lo indicado por el valor '3' de cabhPsDevProvMode, el PS NO DEBE aceptar o procesar ningún mensaje SNMP recibido en cualquier interfaz WAN.

Cuando el PS funciona en el modo CableHome aletargado conforme a 5.5 y 7.2.3.3 y a lo indicado por el valor '3' de cabhPsDevProvMode, el PS DEBE aceptar y procesar mensajes SNMP recibidos por cualquier interfaz LAN conforme a los valores de docsDevNmAccessTable (véase 6.3.6.1) o conforme a los valores del modelo de control de acceso basado en vistas (véase 6.3.6.3).

La raíz de las MIB (PSDev MIB, CAP MIB, CDP MIB, CTP MIB, y MIB de seguridad) DEBE ser (enterprises.4491.2.4).

El PS DEBE incluir – en el orden especificado a continuación – versión del soporte físico, nombre del fabricante, versión de imagen de la ROM de arranque, versión del soporte lógico y número de modelo en el objeto sysDescr (de [RFC 3418]). El formato de la información específica incluida en el sysDescr DEBE ser:

Informar	*Formato de cada campo*
Versión de soporte físico	HW_REV: <Soporte físico version>
Nombre del fabricante	VENDOR: <Vendor name>
ROM de arranque	BOOTR: <Boot ROM Version>
Versión de soporte lógico	SW_REV: <Soporte lógico version>
Número de modelo	MODEL: <Model number>

El sysDescr DEBE constar de una lista de cinco pares tipo/valor encerrados en corchetes angulares. La separación entre el tipo y el valor es ": " – un símbolo de dos puntos y un espacio en blanco. La separación entre dos pares tipo/valor es: "; " – un símbolo punto y coma y un espacio en blanco. Por ejemplo, un sysDescr de un PS del fabricante X, con versión de soporte físico 5.2, versión de ROM de arranque 1.4, versión de SW 2.2, y número de modelo X se verá como sigue:

cualquier texto<<HW_REV: 5.2; VENDOR: X; BOOTR: 1.4; SW_REV: 2.2; MODEL: X>>cualquier texto

El PS DEBE informar en el sysDescr por lo menos la información necesaria para determinar qué versiones de políticas de soporte lógico y de barrera contra fuegos puede cargar el PS. Si algunos campos del objeto sysDescr no se aplican, el PS DEBE informar "NINGUNO" ("NONE") como el valor. Por ejemplo, un PS sin BOOTR informará "BOOTR: NONE".

El valor del objeto MIB docsDevSwCurrentVers DEBE incluir la misma información de versión de soporte lógico que la contenida en la información de versión de soporte lógico del objeto sysDescr.

Cuando se incorporan en el mismo dispositivo un PS y un CM, los objetos sysDescr y docsDevSwCurrentVers del PS DEBEN informar los mismos valores que los del CM.

El objeto sysObjectID del grupo del sistema MIB-2 [RFC 3418] DEBE implementarse y DEBE conservarse en las reactivaciones de los dispositivos y ciclos de alimentación.

El objeto sysUpTime del grupo del sistema MIB-2 [RFC 3418] DEBE implementarse. Si SysUpTime es el periodo de tiempo transcurrido desde la última reactivación del sistema.

El objeto sysContact del grupo de sistema MIB-2 [RFC 3418] DEBE implementarse y DEBE mantenerse a pesar de las reactivaciones de dispositivos y ciclos de potencia. SysContact devuelve el nombre del usuario o el del administrador del sistema cuando se conoce.

El objeto sysLocation del grupo de sistema MIB-2 [RFC 3418] DEBE implementarse y DEBE conservarse en las reactivaciones de dispositivos y ciclos de alimentación.

El objeto sysServices del grupo de sistema MIB-2 [RFC 3418] DEBE implementarse y DEBE conservarse en las reactivaciones de dispositivos y ciclos de alimentación.

El objeto sysServices DEBE devolver el valor "3" (pasarela de Internet) cuando se le consulte en un elemento PS.

El objeto sysName del grupo de sistema MIB-2 [RFC 3418] DEBE implementarse y DEBE conservarse en la reactivación de dispositivos y ciclos de alimentación. La consulta de sysName devuelve el nombre de sistema.

Los objetos del grupo de sistema MIB-2 distintos de sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation y sysServices NO DEBERÍAN implementarse.

La MIB del grupo de interfaces [RFC 2863] DEBE implementarse, conforme al anexo A y los requisitos de 6.3.8.

El grupo SNMP de MIB-2 [RFC 3418] DEBE implementarse.

El objeto snmpSetSerialNo del grupo snmpSet [RFC 3418] DEBE implementarse. snmpSetSerialNo es un bloqueo consultivo para que varias entidades SNMPv2 cooperantes, actuando como gestoras, puedan coordinar su utilización de la operación del conjunto SNMPv2.

Los objetos del grupo snmpSet distintos de snmpSetSerialNo NO DEBERÍAN implementarse.

Cuando los objetos MIB del elemento PS se fijan a los valores de fábrica por defecto utilizando las MIB cabhCapSetToFactory, cabhCdpSetToFactory, cabhCTPSetToFactory o cabhPsDevSetToFactory, la funcionalidad PS correspondiente DEBE utilizar los mismos valores de fábrica por defecto para su funcionamiento sin tener que reaprovisionar el elemento PS.

6.3.5 Requisitos del protocolo SNMP

Las siguientes RFC del IETF DEBEN respetarse o implementarse según proceda:

1) Un protocolo de gestión de red simple [RFC 1157].
2) Introducción al SNMPv2 orientado a comunidades [RFC 1901].
3) Operaciones de protocolo para SNMPv2 [RFC 3416].
4) Correspondencias de transporte para SNMPv2 [RFC 3417].
5) Base de información de gestión para la versión 2 del protocolo de gestión de red simple (SNMPv2) [RFC 3418].
6) Introducción al SNMPv3 [RFC 3410].
7) MIB en el marco SNMP [RFC 2571].
8) Proceso y despacho de mensajes para SNMP [RFC 3412].
9) MIB de aplicaciones SNMP [RFC 3413].
10) Grupo de MIB SnmpUSM [RFC 3414].
11) Grupo de MIB SnmpVACM [RFC 3415].

12) MIB de comunidades SNMP [RFC 2576].

13) SNMPv2-CONF.

Para soportar el SMIv2, DEBEN implementarse las siguientes RFC del IETF:

1) Estructura de la información gestionada versión 2 (SMIv2) [RFC 2578].

2) Convenios textuales para el SMIv2 [RFC 2579].

3) Declaraciones de conformidad para SMIv2 [RFC 2580].

6.3.6 Requisitos del modo de gestión de red

En la cláusula 5.5 se describieron dos modos de configuración (modo de configuración DHCP y modo de configuración SNMP) y dos modos de gestión de red (modo NmAccessTable y modo de coexistencia SNMPv3) los cuales deberán ser soportados por el PS. En las cláusulas 7.2.3.3, 7.3.3.2 y 7.3.3.3 se proporcionan detalles adicionales relativos al funcionamiento del PS en cada uno de los dos modos de configuración.

En esta cláusula se describen las reglas para los modos de gestión de red que debe soportar el PS. En la cláusula 6.3.6.1 y en sus subcláusulas se describen los modos de gestión de red de un PS que funciona en el modo de configuración DHCP. De la misma manera, en la cláusula 6.3.6.2 y en sus subcláusulas se describen los modos de gestión de red de un PS funcionando en el modo de configuración SNMP.

6.3.6.1 Modos de gestión de red de un PS que funciona en el modo de configuración DHCP

El PS DEBE soportar SNMPv1, SNMPv2c y SNMPv3 y la coexistencia SNMP conforme a RFC 2576 y RFC 3414. Además, el PS DEBE soportar el modo NmAccessTable conforme a RFC 2669. El soporte de los modos de gestión de red de un PS que funciona en el modo de configuración DHCP queda sujeto a las siguientes directrices:

6.3.6.1.1 Principios de funcionamiento básico de un PS que funciona en el modo de configuración DHCP

Puede considerarse que el funcionamiento inicial del PS configurado según el modo de configuración DHCP tiene tres etapas:

1) comportamiento del PS después de haber sido configurado para el modo de configuración DHCP, pero antes de que se haya configurado su modo de gestión de red a través del fichero de configuración del PS;

2) determinación del modo de gestión de red; y

3) comportamiento del PS después de haber configurado su modo de gestión de red.

A continuación se presentan las reglas de funcionamiento para cada una de estas etapas:

1) Una vez configurado el PS para funcionar en el modo de configuración DHCP (indicado por un valor de cabhPsDevProvMode igual a '1' (DHCPmode)), pero antes de haberlo configurado para el modo de gestión de red, el PS DEBE funcionar de la siguiente manera:

   - Se descartan todos los paquetes SNMP.
   - El gestor SNMP no tiene acceso a ninguna de las MIB SNMPv3 (Community MIB, TARGET-MIB, VACM-MIB, USM-MIB, NOTIFICATION-MIB) en el NMS.
   - El gestor SNMP no tiene acceso a ninguno de los elementos en SNMP-USM-DH-OBJECTS-MIB en el NMS.
   - El fichero de configuración del PS especificado en la DHCP OFFER se descarga y se procesa.

- El proceso satisfactorio de todos los elementos MIB del fichero de configuración del PS DEBE llevarse a buen fin antes de iniciar el cálculo de los valores públicos del cuadro usmDHKickstart.

2) Si el PS está funcionando en el modo de configuración DHCP, el contenido del fichero de configuración del PS determina el modo de gestión de la red como se indica a continuación:
   - El PS se encuentra en el modo docsDevNmAccess SNMPv1/v2c si el fichero de configuración del PS SÓLO contiene valores del cuadro docsDevNmAccess para el control de acceso SNMP.
   - Si el fichero de configuración del PS no contiene elementos de control de acceso SNMP (docsDevNmAccessTable ni snmpCommunityTable ni TLV 34.1/34.2 ni TLV38), el PS se encuentra en el modo NmAccess.
   - Si el fichero de configuración del PS contiene el valor snmpCommunityTable y/o los tipos 34.1 y 34.2 de TLV y/o el tipo 38 de TLV, el PS se encuentra en el modo de coexistencia SNMP. En tal caso, se ignoran las entradas de docsDevNmAccessTable.

3) Tras completar el proceso de configuración descrito en 13.2 (indicado por el valor 'pass' (1) de cabhPsDevProvState), el PS funciona en uno de los dos modos de gestión de red. El modo de gestión de red viene determinado por el contenido del fichero de configuración del PS descrito anteriormente. A continuación se establecen las reglas para el funcionamiento del PS en cada uno de los dos modos de gestión de red:

Modo NmAccess con utilización de SNMPv1/v2c

- El PS DEBE procesar los paquetes SNMPv1/v2c y descartar los paquetes SNMPv3.
- docsDevNmAccessTable controla el acceso y los destinos de las trampas descritos en RFC 2669. El PS DEBE apegarse a la política de acceso de gestión, conforme al cuadro NmAccess, por lo que se refiere al acceso a los objetos MIB especificados, independientemente de la interfaz o del protocolo de acceso que se utilicen.
- No es accesible ninguna de las MIB SNMPv3 (Community MIB, TARGET-MIB, VACM-MIB, USM-MIB, NOTIFICATION-MIB).

Cuando el PS funciona en el modo NmAccess SNMPv1/v2c DEBE tener la capacidad para enviar trampas conforme al siguiente objeto MIB (extensión de MIB propuesta para el cuadro docsDevNmAccess):

DocsDevNmAccessTrapVersion OBJECT-TYPE

SYNTAX INTEGER {

DisableSNMPv2trap(1),

EnableSNMPv2trap(2),

}

MAX-ACCESS read-create

STATUS current

DESCRIPCIÓN

"Especifica la versión de TRAP (TRAMPA) que se envía a este NMS. La fijación de este objeto a disableSNMPv2trap(1) provoca que se envíe la trampa en el formato SNMPv1 a un NMS particular. La fijación de este objeto a EnableSNMPv2trap(2) provoca el envío de la trampa en el formato SNMPv2 a un NMS particular."

DEFVAL { Disable SNMPv2trap }

::={docsDevNmAcessEntry 8}

Modo de coexistencia utilizando SNMPv1/v2c/v3

Durante el modo de coexistencia SNMPv3, el PS DEBE soportar los requisitos de "inicialización de SNMPv3" y "modificaciones de clave DH" conforme a 11.3.3.1.2. Estos requisitos incluyen el cálculo de los parámetros públicos del cuadro de arranque USM Diffie-Hellman. Se aplican las siguientes reglas al funcionamiento del PS durante y después del cálculo de los parámetros públicos (valores) conforme se indica:

Durante el cálculo de los valores públicos de usmDHKickstartTable:

- El PS NO DEBE permitir ningún acceso SNMP desde la WAN.
- El PS PUEDE continuar permitiendo el acceso desde la LAN limitado de acuerdo con lo configurado por la USM-MIB de comunidad y la VACM-MIB.

Tras el cálculo de los valores públicos usmDHKickstartTable:

- El PS DEBE enviar la trampa arranque en frío o arranque en caliente para indicar que el PS ya admite sin reservas la gestión SNMPv3.
- Se procesan los paquetes SNMPv1/v2c/v3 descritos por RFC 2576, RFC 3412, RFC 3413, RFC 3414 y RFC 3415.
- No se puede acceder a docsDevNmAccessTable.
- El control de acceso y los destinos de las trampas vienen determinados por el snmpCommunityTable, la Notification-MIB, la Target-MIB, la VACM-MIB, y la USM-MIB. El PS DEBE hacer cumplir la política de acceso de gestión, tal como la define la vista VACM configurada por el operador de cable, para cualquier acceso a los objetos MIB especificados, sin importar cuál interfaz o protocolo de acceso se utilice.
- La MIB de comunidad controla la traducción de la cadena de comunidad de paquetes SNMPv1/v2c a un nombre de seguridad que seleccione entradas en la USM MIB. El control de acceso lo proporciona la VACM MIB.
- La USM MIB y la VACM MIB controlan los paquetes SNMPv3.
- Los destinos de las trampas se especifican en la Target-MIB y en la Notification-MIB.

Cuando no se pueda completar la inicialización SNMPv3 para un usuario (es decir, el NMS no puede acceder al PS a través de PDU SNMPv3), DEBE suprimirse el cuadro de usuarios USM correspondiente a dicho usuario, el PS se encuentra en el modo de coexistencia y el PS permitirá el acceso SNMPv1/v2c si y sólo si se configuran las entradas MIB de comunidad (y entradas relacionadas).

6.3.6.2 Modo de gestión de red para un PS que funciona en el modo de configuración SNMP

Si el PS está funcionando en el modo de configuración SNMP a continuación de un ACK DHCP (según el valor '2' (SNMPmode) de cabhPsDevProvMode), funcionará en el modo de coexistencia SNMPv3 utilizando SNMPv3 por defecto para intercambiar mensajes de gestión con el NMS, y empleará Kerberos para intercambiar claves con el KDC, siguiendo las reglas que se describen en esta cláusula.

6.3.6.2.1 Vista de gestión

Los controles de gestión definidos para IPCable2Home se ubican en la función CMP del PS. Los valores, basados en el modo de gestión, definen los derechos de acceso que se otorgan a un usuario para acceder a la base de datos de servicios de portal, a través de las MIB especificadas para IPCable2Home, mediante SNMP desde el NMS de la red de cable. La especificación de IPCable2Home define un solo usuario.

En la figura 6-4 se muestran algunas vistas de gestión posibles para el PS. IPCable2Home define una vista de administrador WAN (vista de administrador del PS) y un usuario de administrador WAN (usuario administrador del PS). Mediante la autorización final (administrador del PS) pueden establecerse otras vistas y usuarios, como es el caso de la vista de mantenimiento WAN, la vista de administrador LAN o la vista de usuario LAN, apegándose a las reglas definidas en RFC 3414 y RFC 3415.

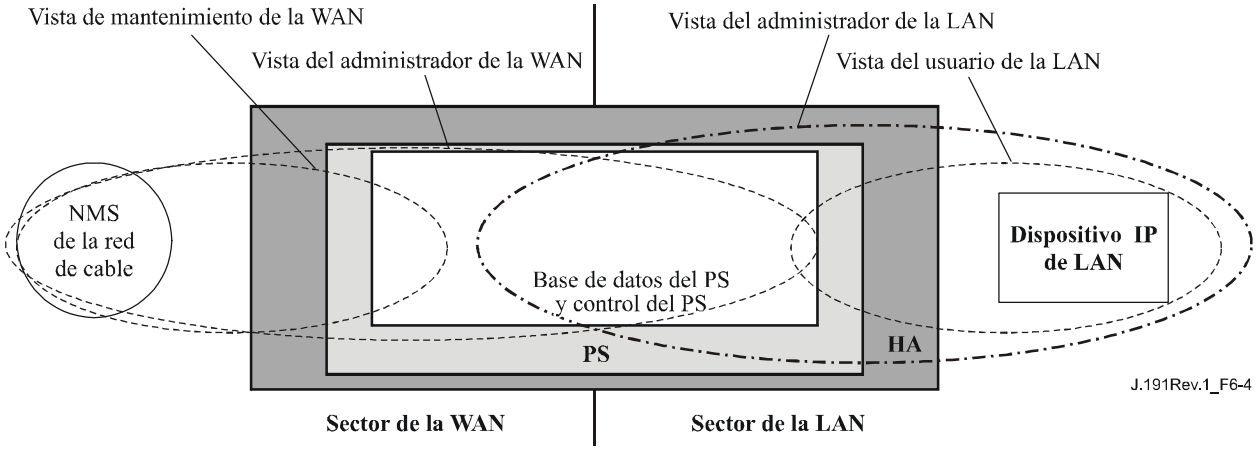


Figura 6-4/J.191 – Vistas de gestión

Los parámetros gestionados definidos por IPCable2Home se almacenan en la base de datos del PS. Como muestra la figura 6-4, hay un concepto de vistas de acceso introducido en la base de datos PS y en el control PS, que permite la gestión simultánea desde la LAN y desde la WAN, gracias a la definición de vistas de gestión en la base de datos del PS y el control del PS. Las vistas constituyen un mecanismo que proporciona privacidad y seguridad, de acuerdo con una política que puede establecerla por separado el usuario administrador del PS.

La autorización final (usuario administrador del PS) tiene su propio ID de usuario y sus propias claves, y tiene las responsabilidades que se indican a continuación:

- El establecimiento de todas las vistas de acceso en las interfaces de gestión de la LAN y de la WAN.
- La creación y gestión de todos los perfiles de usuario incluidos los ID de usuario, sus claves y los privilegios de acceso a la base de datos del PS.
- El establecimiento de la política de acceso desde el lado LAN y desde la WAN.

La implementación completa del VACM requiere un conjunto de actuaciones que vincule un "usuario" a un "grupo" y el "grupo" a una vista VACM, que define el acceso. La cláusula 6.3.6.3 describe la creación de estas relaciones.

El vacmSecurityName es el "User". Este nombre de seguridad está vinculado al vacmGroupName, por lo que el "User" queda vinculado a un grupo específico. A continuación se define el grupo para especificar el nivel de seguridad utilizado y las vistas de lectura, escritura y notificación permitidas para este grupo. A continuación las vistas se especifican mostrando cuáles son exactamente los objetos MIB accesibles.

El modelo de control de acceso basado en vistas determina los derechos de acceso de un grupo, que representa cero o más securityNames, con los mismos derechos de acceso. En un contexto determinado, identificado por contextName, al que un grupo, identificado por groupName, tiene acceso utilizando unos determinados securityModel y securityLevel, los derechos de acceso de dicho grupo se obtienen de una vista de lectura, una vista de escritura y una vista de notificación.

La vista de lectura representa el conjunto de ejemplares de objeto autorizados para el grupo cuando lee objetos. La lectura de objetos tiene lugar cuando se procesa una operación de recuperación (tratando PDU de la clase lectura).

La vista de escritura representa el conjunto de ejemplares de objeto autorizados al grupo cuando escribe objetos. La escritura de objetos tiene lugar cuando se procesa una operación de escritura (tratando PDU de la clase escritura).

La vista de notificación representa el conjunto de ejemplares de objeto autorizados a un grupo cuando envía objetos en una notificación, como cuando envía una notificación (cuando envía PDU de la clase notificación).

La vista del administrador PS otorga pleno acceso de lectura y escritura a todas las MIB especificadas.

Los requisitos de la vista de gestión se consignan en 6.3.6.3.

6.3.6.2.2 Control de acceso WAN

El control de acceso SNMP, de acuerdo con RFC 3415, se utilizará para controlar el acceso a los objetos MIB especificados, independientemente de la interfaz por la que llega la petición. El modelo de control de acceso basado en vistas (VACM) [RFC 3415] define un conjunto de servicios que pueden utilizarse para la comprobación de derechos de acceso. Los grupos VACM definen los derechos de acceso al CMP.

De acuerdo con lo definido en la sección 2.4 de RFC 3415, la "vista MIB" es un conjunto específico de tipos de objetos gestionados que pueden definirse, utilizándose este concepto en IPCable2Home para soportar la gestión del PS por parte de la WAN. La vista y el acceso del usuario administrador del PS se especifican en 11.3.3.2.2 y 6.3.6.3. La cláusula 12.3.1 contiene un ejemplo de la secuencia de acceso a la base de datos del PS desde la interfaz de la WAN.

6.3.6.2.3 Seguridad

La seguridad de la gestión de mensajes la proporciona el SNMPv3. Consúltese la cláusula 11 en relación con la descripción detallada del modo de utilización del SNMPv3. El CMP puede utilizar SNMPv3 para responder a las amenazas definidas en el anexo C.

Como protección contra los ataques de repetición de la reproducción, se utiliza un reloj que proporciona indicaciones de tiempo para los mensajes. Los requisitos de seguridad de los mensajes de gestión se especifican en 11.3.3.

6.3.6.3 Requisitos del modelo de control de acceso basado en vistas (VACM)

Para proporcionar acceso controlado a la información de gestión y la creación de sectores de gestión bien definidos para un PS que funciona en el modo de coexistencia SNMPv3, DEBE utilizarse el modelo de control de acceso basado en vistas (VACM) definido en RFC 3415.

CHAdministrator' es el nombre de usuario USM [RFC 3414] que se definió para el administrador WAN en 6.3.4, y 6.3.6.2.1, suponiendo que este administrador es el operador del sistema de cable. Como autorización final para un PS, el administrador de la WAN debe poder leer y escribir cualquier objeto MIB y tener la capacidad para crear nuevos usuarios. Las configuraciones de la vista para este usuario CHAdministrator se definen en esta cláusula.

La vista del administrador de la WAN DEBE implementarse en el elemento de servicios de portal. Las vistas por defecto distintas de la vista del administrador de la WAN, NO DEBEN estar disponibles en el PS.

PUEDEN crearse otras vistas mediante la autorización final a través del NMS de la red de cable configurando la MIB VACM.

La especificación de usuario para la vista del administrador de la WAN DEBE implementarse del siguiente modo:

vacmSecurityModel	3 (USM)
vacmSecurityName	'PS Administrator'
vacmGroupName	'PS Administrator'
vacmSecurityToGroupStorageType	permanente
vacmSecurityToGroupStatus	activo

La especificación de grupo de la vista del administrador del PS DEBE implementarse del siguiente modo:

PS Administrator Group	
vacmGroupName	'PS Administrator'
vacmAccessContextPrefix	''
vacmAccessSecurityModel	3 (USM)
vacmAccessSecurityLevel	AuthPriv
vacmAccessContextMatch	exacta
vacmAccessReadViewName	'PS AdministratorView'
vacmAccessWriteViewName	'PS AdministratorView'
vacmAccessNotifyViewName	'PS AdministratorView'
vacmAccessStorageType	permanente
vacmAccessStatus	activo

La vista VACM para la vista del administrador PS DEBE implementarse del siguiente modo:

PS AdministratorView subárbol 1.3.6.1 (MIB completa).

6.3.6.4 Correspondencia de los campos TLV con las filas del cuadro creado para SNMPv3

En esta cláusula y en las siguientes se proporcionan los detalles para hacer corresponder el elemento del fichero de configuración del *receptor de notificación docsisV3* (TLV tipo 38) con los cuadros funcionales de SNMPv3.

Cuando se recibe un elemento de fichero de configuración tipo 38, el PS DEBE efectuar asientos en los siguientes cuadros para provocar la transmisión de la trampa deseada.

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

Un fichero de configuración PS PUEDE incluir elementos MIB TLV (tipo 28) que efectúan asientos en cualquiera de los 11 cuadros relacionados anteriormente. Se prevé que estos elementos MIB TLV no tendrán columnas de índice que comiencen con los caracteres "@config" o "@PSconfig".

Los cuadros de esta cláusula muestran cómo se colocan los campos del elemento TLV del fichero de configuración PS (las etiquetas entre corchetes angulares < >) en los cuadros de SNMPv3.

La correspondencia entre los campos TLV y las etiquetas <TAG> del cuadro es la siguiente:

PS<IP Address> TLV 38.1

<Port> – TLV 38.2

<Trap type> TLV 38.3

<Timeout> TLV 38.4

<Retries> TLV 38.5

<Filter OID> TLV 38.6

<Security Name> TLV 38.7

Estos cuadros se representan en el mismo orden en que el agente efectuará la búsqueda en ellos cuando se genere una notificación para determinar a quién se debe enviar la misma y cómo rellenar el contenido del paquete de notificación.

6.3.6.4.1 snmpNotifyTable

Si hay uno o más elementos TLV se deben crear dos filas con valores fijos.

Cuadro 6-4/J.191 – snmpNotifyTable

snmpNotifyTable [RFC 2573] SNMP-NOTIFICATION-MIB	**Primera fila**	**Segunda fila**
Nombre de columna (* = Parte del índice)	Valor de columna	Valor de columna
* snmpNotifyName	"@PSconfig_inform"	"@PSconfig_trap"
snmpNotifyTag	"@PSconfig_inform"	"@PSconfig_trap"
snmpNotifyType	inform(2)	trap(1)
snmpNotifyStorageType	volátil	volátil
snmpNotifyRowStatus	Active(1)	Active(1)

6.3.6.4.2 snmpTargetAddrTable

Se debe crear una fila para cada elemento TLV en el fichero de configuración del PS.

Cuadro 6-5/J.191 – snmpTargetAddrTable

snmpTargetAddrTable [RFC 2573] SNMP-TARGET-MIB	Nueva fila
Nombre de columna (* = parte del índice)	Valor de columna
* snmpTargetAddrName	"@PSconfig_n", donde n va de 0 a m–1, y m es el número de elementos TLV del receptor de notificación en el fichero de configuración del PS
snmpTargetAddrTDomain	snmpUDPDomain – snmpDomains.1
snmpTargetAddrTAddress (dirección IP y puerto UDP del receptor de notificación)	CADENA DE OCTETOS (6) Octetos 1-4: <IP Address> Octetos 5-6: <Port>
snmpTargetAddrTimeout	<Timeout> desde el TLV
snmpTargetAddrRetryCount	<Retries> desde el TLV
snmpTargetAddrTagList	Si <Trap type> == 1, 2 ó 4 "@PSconfig_trap" Para el resto, si <Trap type> = 3 ó 5 "@PSconfig_inform"
snmpTargetAddrParams	"@PSconfig_n" (el mismo valor de snmpTargetAddrName)
snmpTargetAddrStorageType	volátil
snmpTargetAddrRowStatus	active(1)

6.3.6.4.3 snmpTargetAddrExtTable

Se debe crear una fila para cada uno de los elementos TLV en el fichero de configuración del PS.

Cuadro 6-6/J.191 – snmpTargetAddrExtTable

snmpTargetAddrExtTable [RFC 2576] SNMP-COMMUNITY-MIB	Nueva fila
Nombre de columna (* = Parte del índice)	Valor de columna
*snmpTargetAddrName	"@PSconfig_n", donde n va de 0 a m – 1, y m es el número de elementos TLV del receptor de notificación en el fichero de configuración del PS
snmpTargetAddrMask	<zero length octet string>
snmpTargetAddrMMS	0

6.3.6.4.4 snmpTargetParamsTable

Se debe crear una fila para cada elemento TLV en el fichero de configuración. Si <Trap type> es 1, 2 ó 3, o si el campo <Security Name> tiene una longitud cero, se debe crear el cuadro conforme a lo siguiente:

Cuadro 6-7/J.191 – snmpTargetParamsTable para <Trap type> 1, 2 ó 3

snmpTargetParamsTable [RFC 2573] SNMP-TARGET-MIB	**Nueva fila**
Nombre de columna (* = Parte del índice)	Valor de columna
* snmpTargetParamsName	"@PSconfig_n", donde n va de 0 a m – 1, y m es el número de elementos TLV del receptor de notificación en el fichero de configuración del PS
snmpTargetParamsMPModel SYNTAX: SnmpMessageProcessingModel	Si <Trap type> = 1 SNMPv1(0) De lo contrario, si <Trap type> = 2 ó 3 SNMPv2c(1) De lo contrario, si <Trap type> = 4 ó 5 SNMPv3(3)
snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	Si <Trap type> = 1 SNMPv1(1) De lo contrario, si <Trap type> = 2 ó 3 SNMPv2c(2) De lo contrario, si <Trap type> = 4 ó 5 USM(3) NOTA – La correspondencia de los tipos de protocolo SNMP con el valor en este cuadro es distinta de snmpTargetParamsMPModel.
snmpTargetParamsSecurityName	"@PSconfig"
snmpTargetParamsSecurityLevel	noAuthNoPriv
snmpTargetParamsStorageType	volátil
snmpTargetParamsRowStatus	active(1)

Si <Trap type> es 4 ó 5, y el campo <Security Name> no tiene longitud cero, se debe crear el cuadro de la siguiente manera:

Cuadro 6-8/J.191 – snmpTargetParamsTable para <Trap type> 4 ó 5

snmpTargetParamsTable [RFC 2573] SNMP-TARGET-MIB	**Nueva fila**
Nombre de columna (* = Parte del índice)	Valor de columna
* snmpTargetParamsName	"@PSconfig_n", donde n va de 0 a m – 1, y m es el número de elementos TLV del receptor de notificación en el fichero de configuración del PS
snmpTargetParamsMPModel SYNTAX: SnmpMessageProcessingModel	Si <Trap type> = 1 SNMPv1(0) De lo contrario, si <Trap type> = 2 ó 3 SNMPv2c(1) De lo contrario, si <Trap type> = 4 ó 5 SNMPv3(3)
snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	Si <Trap type> = 1 SNMPv1(1) De lo contrario, si <Trap type> = 2 ó 3 SNMPv2c(2) De lo contrario, si <Trap type> = 4 ó 5 USM(3) NOTA – La correspondencia de los tipos de protocolo SNMP con el valor en este cuadro es diferente de snmpTargetParamsMPModel.
snmpTargetParamsSecurityName	<Security Name>
snmpTargetParamsSecurityLevel	El nivel de seguridad de <Security Name>
snmpTargetParamsStorageType	volátil
snmpTargetParamsRowStatus	active(1)

6.3.6.4.5 snmpNotifyFilterProfileTable

Se debe crear una fila para cada elemento TLV que tenga una longitud diferente de cero <Filter Length>.

Cuadro 6-9/J.191 – snmpNotifyFilterProfileTable

snmpNotifyFilterProfileTable [RFC 2573] SNMP-NOTIFICATION-MIB	**Nueva fila**
Nombre de columna (* = Parte del índice)	Valor de columna
* snmpTargetParamsName	"@PSconfig_n", donde n va de 0 a m – 1, y m es el número de elementos TLV del receptor de notificación en el fichero de configuración del PS
snmpNotifyFilterProfileName	"@PSconfig_n", donde n va de 0 a m – 1, y m es el número de elementos TLV del receptor de notificación en el fichero de configuración del PS
snmpNotifyFilterProfileStorType	volátil
snmpNotifyFilterProfileRowStatus	active(1)

6.3.6.4.6 snmpNotifyFilterTable

Se debe crear una fila para cada elemento TLV que tenga una longitud diferente de cero <Filter Length>.

Cuadro 6-10/J.191 – snmpNotifyFilterTable

snmpNotifyFilterTable [RFC 2573] SNMP-NOTIFICATION-MIB	Nueva fila
Nombre de columna (* = Parte del índice)	Valor de columna
* snmpNotifyFilterProfileName	"@PSconfig_n", donde n va de 0 a m – 1, y m es el número de elementos TLV del receptor de notificación en el fichero de configuración del PS
* snmpNotifyFilterSubtree	<Filter OID> desde el TLV
snmpNotifyFilterMask	<Zero length octet string>
snmpNotifyFilterType	included(1)
snmpNotifyFilterStorageType	volátil
snmpNotifyFilterRowStatus	active(1)

6.3.6.4.7 snmpCommunityTable

Se debe crear una fila con valores fijos si hay uno o más TLV. Esto provoca que las notificaciones SNMPV1 y V2c incluyan la cadena de la comunidad en snmpCommunityName.

Cuadro 6-11/J.191 – snmpCommunityTable

snmpCommunityTable [RFC 2576] SNMP-COMMUNITY-MIB	Primera fila
Nombre de columna (* = Parte del índice)	Valor de columna
* snmpCommunityIndex	"@PSconfig"
snmpCommunityName	"public"
snmpCommunitySecurityName	"@PSconfig"
snmpCommunityContextEngineID	<The PS engineID>
snmpCommunityContextName	<Zero length octet string>
snmpCommunityTransportTag	<Zero length octet string>
snmpCommunityStorageType	volátil
snmpCommunityStatus	active(1)

6.3.6.4.8 usmUserTable

Se debe crear una fila con valores fijos, si hay uno o más elementos TLV. Se debe crear otra fila cada vez que se determine el ID de la máquina de un receptor de trampas. Esto permite especificar el nombre del usuario en los receptores de notificación distantes a los que se deben enviar las notificaciones.

Se debe crear una fila en usmUserTable. A continuación, cuando se determine el ID de la máquina de cada receptor de notificación, el agente copia esta fila en una nueva y sustituye el valor 0x00 con el valor recién determinado en la columna usmUserEngineID.

Cuadro 6-12/J.191 – usmUserTable

usmUserTable [RFC 2574] SNMP-USER-BASED-SM-MIB	Primera fila
Nombre de columna (* = Parte del índice)	Valor de columna
* usmUserEngineID	0
* usmUserName	"@PSconfig" Cuando se crean otras filas, ésta se sustituye con el campo <Security Name> de elemento TLV
usmUserSecurityName	"@PSconfig" Cuando se crean otras filas, ésta se sustituye con el campo <Security Name> de elemento TLV
usmUserCloneFrom	<don't care> – no se puede copiar esta fila
usmUserAuthProtocol	Ninguna. Cuando se crean otras filas, ésta se sustituye con Ninguno (None) o MD5, en función del nivel de seguridad del usuario v3
usmUserAuthKeyChange	<don't care> – sólo escritura
usmUserOwnAuthKeyChange	<don't care> – sólo escritura
usmUserPrivProtocol	Ninguna. Cuando se crean otras filas, ésta se sustituye con Ninguno o DES, en función del nivel de seguridad del usuario v3
usmUserPrivKeyChange	<don't care> – sólo escritura
usmUserOwnPrivKeyChange	<don't care> – sólo escritura
usmUserPublic	<zero length string>
usmUserStorageType	volátil
usmUserStatus	active(1)

6.3.6.4.9 vacmSecurityToGroupTable

Se deben crear tres filas con valores fijos, si hay uno o más elementos TLV.

Se trata de las tres filas con valores fijos que se utilizan para los asientos TLV con <Trap Type> fijado a 1, 2 ó 3 o con un <Security Name> de longitud cero.

Cuadro 6-13/J.191 – vacmSecurityToGroupTable

vacmSecurityToGroupTable [RFC 2575] SNMP-VIEW-BASED-ACM-MIB	Primera fila	Segunda fila	Tercera fila
Nombre de columna (* = Parte del índice)	Valor de columna	Valor de columna	Valor de columna
* vacmSecurityModel	SNMPv1(1)	SNMPv2c(2)	USM(3)
* vacmSecurityName	"@PSconfig"	"@PSconfig"	"@PSconfig"
vacmGroupName	"@PSconfigv1"	"@PSconfigv2"	"@PSconfigUSM"
vacmSecurityToGroupStorageType	volátil	volátil	volátil
vacmSecurityToGroupStatus	active(1)	active(1)	active(1)

6.3.6.4.10 vacmAccessTable

Se deben crear tres filas con valores fijos, si hay uno o más elementos TLV.

Se trata de las tres filas con valores fijos que se utilizan para los asientos TLV con <Trap Type> fijado a 1, 2 ó 3 o con un <Security Name> de longitud cero.

Cuadro 6-14/J.191 – vacmAccessTable

vacmAccessTable [RFC 2575] SNMP-VIEW-BASED-ACM-MIB	Primera fila	Segunda fila	Tercera fila
Nombre de columna (* = Parte del índice)	Valor de columna	Valor de columna	Valor de columna
* vacmGroupName	"@PSconfigV1"	"@PSconfigV2"	"@PSconfigUSM"
* vacmAccessContextPrefix	<Zero length string>	<Zero length string>	<Zero length string>
* vacmAccessSecurityModel	SNMPv1(1)	SNMPv2c(2)	USM(3)
* vacmAccessSecurityLevel	noAuthNoPriv(1)	noAuthNoPriv(1)	noAuthNoPriv(1)
vacmAccessContextMatch	exact(1)	exact(1)	exact(1)
vacmAccessReadViewName	<Zero length octet string>	<Zero length octet string>	<Zero length octet string>
vacmAccessWriteViewName	<Zero length octet string>	<Zero length octet string>	<Zero length octet string>
vacmAccessNotifyViewName	"@PSconfig"	"@PSconfig"	"@PSconfig"
vacmAccessStorageType	volátil	volátil	volátil
vacmAccessStatus	active(1)	active(1)	active(1)

Los asientos TLV con <Trap Type> fijado a 4 ó 5 y un <Security Name> de longitud diferente de cero utilizarán las filas creadas en el cuadro vacmAccessTable mediante el proceso de arranque DH.

6.3.6.4.11 vacmViewTreeFamilyTable

Se debe crear una fila con valores fijos si hay uno o más elementos TLV.

Esta fila se utiliza para los asientos TLV con <Trap Type> fijado a 1, 2 ó 3 o con un <Security Name> de longitud cero.

Cuadro 6-15/J.191 – vacmViewTreeFamilyTable

vacmViewTreeFamilyTable [RFC 2575] SNMP-VIEW-BASED-ACM-MIB	Primera fila
Nombre de columna (* = Parte del índice)	Valor de columna
* vacmViewTreeFamilyViewName	"@PSconfig"
* vacmViewTreeFamilySubtree	1.3
vacmViewTreeFamilyMask	<Default from MIB>
vacmViewTreeFamilyType	included(1)
vacmViewTreeFamilyStorageType	volátil
vacmViewTreeFamilyStatus	active(1)

Los asientos TLV con <Trap Type> fijado a 4 ó 5 y un <Security Name> de longitud diferente de cero utilizarán las filas creadas en el cuadro vacmViewTreeFamilyTable mediante el proceso de arranque DH.

6.3.7 Requisitos de la MIB

Los objetos de la MIB que se relacionan en el anexo A DEBEN implementarse en un elemento PS de IPCable2Home PS. Los objetos MIB necesarios proceden de los siguientes documentos MIB:

1) MIB del grupo de interfaces [RFC 2863].
2) MIB del dispositivo de cable DOCSIS [RFC 2669].
3) MIB de definición [E.4].
4) MIB PSDev de cable [E.1].
5) MIB CAP de cable [E.6].
6) MIB CDP de cable [E.5].
7) MIB CTP de cable [E.2].
8) MIB de seguridad de cable [E.3].
9) draft-ietf-ipcdn-bpiplus-mib-12.
10) MIB de IP (SNMPv2) [RFC 2011].
11) MIB de UDP (SNMPv2) [RFC 2013].
12) Clave USM de Diffie-Hellman [RFC 2786].
13) MIB de dirección INET [RFC 3291].
14) MIB de IF DOCS [RFC 2670].
15) MIB ifType IANA.

En el caso del PS integrado, la entidad de gestión del módem de cable y la entidad de gestión del PS (CMP) DEBEN responder a distintas direcciones IP de gestión independientes. El módem de cable e IPCable2Home especifican algunos de los mismos objetos MIB pero si un módem de cable conforme y un elemento PS conforme con IPCable2Home se integran en el mismo dispositivo, es necesario que cada uno conserve su propio ejemplar independiente de objetos MIB específicos, a los que se podrá acceder a través de distintas direcciones IP de gestión, con excepción de: subárbol snmpV2 de RFC 2578, grupo SNMP de RFC 3418, contadores de grupo IP e ICMP de RFC 2011 y los contadores de grupo UDP de RFC 2013, que PODRÍAN ser comunes entre el módem de cable y el elemento de servicios de portal y compartirse entre estos últimos, y PODRÍA accederse a ellos a través de la dirección IP de gestión del módem de cable o de la dirección IP de gestión del PS.

En el PS integrado, la descarga de la imagen única del soporte lógico combinado del módem de cable y de los servicios de portal, se controla mediante el módem de cable. El grupo de objetos docsDevSoporte lógico [RFC 2669] NO DEBE implementarse en el PS integrado, salvo para el objeto de sólo lectura docsDevSwCurrentVers, es decir, únicamente se puede acceder al resto de este grupo de objetos a través de la dirección IP de gestión del módem de cable.

- docsDevSwServer;
- docsDevSwFilename;
- docsDevSwAdminStatus;
- docsDevSwOperStatus.

El grupo de objetos docsDevSoporte lógico DEBE implementarse en un PS autónomo. La modificación de estos objetos (según la especificación en 11.3.7) por el operador de cable a los efectos de la descarga de la imagen del soporte lógico del PS autónomo DEBE dar por resultado una operación de descarga de soporte lógico segura y apropiada.

En el caso del PS integrado, los objetos MIB del módem de cable sólo son visibles y accesibles cuando el gestor accede a los mismos a través de la dirección IP de gestión del módem de cable y NO DEBEN ser visibles o accesibles a través de ninguna dirección IP del PS, con excepción de: subárbol snmpV2 de RFC 2578, grupo SNMP de RFC 3418, contadores de grupo IP e ICMP de RFC 2011, y contadores de grupo UDP de RFC 2013 que podrán compartirse entre las entidades de gestión CM y PS.

En el caso de PS integrado, los objetos MIB específicos de IPCable2Home sólo DEBEN estar visibles y accesibles cuando el gestor accede a los mismos desde la red WAN a través de la dirección IP WAN-Man del PS, o desde la red LAN a través de la dirección IP cabhCdpServerRouter, y no son visibles o accesibles a través de la dirección IP de gestión del módem de cable, con excepción de: subárbol snmpV2 de RFC 2578, grupo SNMP de RFC 3418, contadores de grupo IP e ICMP de RFC 2011 y contadores de grupo UDP de RFC 2013 que podrán compartirse entre las entidades de gestión CM y PS.

En la figura 6-5 se ilustra la jerarquía general de la MIB de IPCable2Home. En el anexo A se enumeran los OID específicos necesarios para las MIB particulares.

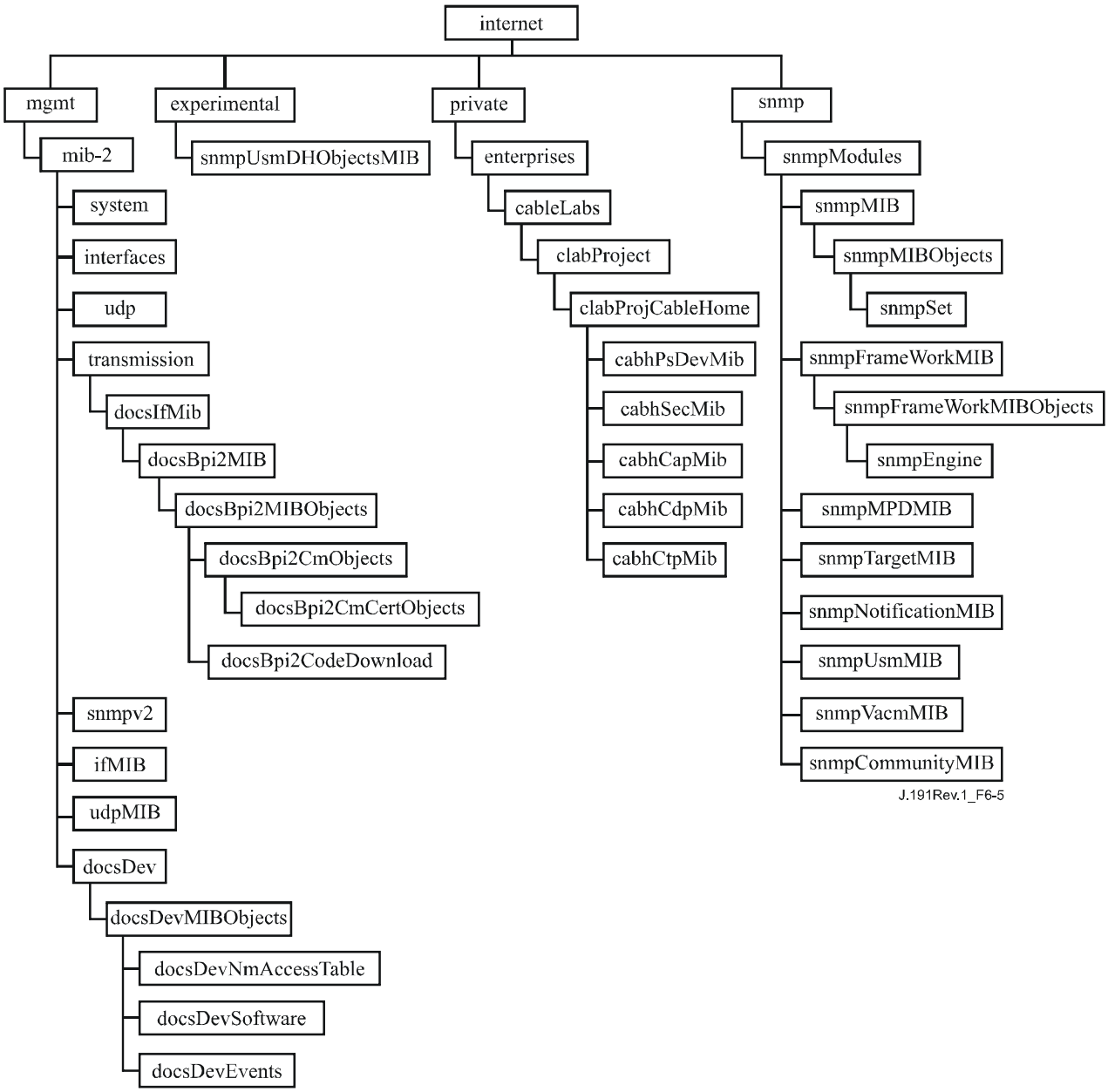


Figura 6-5/J.191 – Jerarquía MIB

6.3.8 Requisitos de la MIB del grupo de interfaces

La MIB del grupo de interfaces constituye una potente herramienta que permite a los operadores de cable averiguar el estado de todas las interfaces físicas del elemento servicio de portal y consultar sus estadísticas. Para la utilización inteligente de esta MIB, es indispensable un esquema de numeración de la interfaz. Por consiguiente los elementos del PS necesitan cumplir los siguientes requisitos:

DEBE existir un ejemplar IfEntry para la interfaz WAN-Man del elemento PS, aunque dicha interfaz sea interna – como existe en el caso de los PS integrados diseñados con circuitos integrados.

DEBE existir un ejemplar ifEntry para la interfaz WAN-Datos del elemento PS siempre que esta interfaz sea parte de la configuración activa del PS e independientemente de que la interfaz sea externa o interna como sucede en el caso de un PS integrado que plantea un diseño basado en un circuito integrado incorporado.

DEBE existir un ejemplar IfEntry para cada interfaz LAN física del elemento PS. DEBE existir un ejemplar ifEntry para una interfaz de 'Interfaces LAN agregadas', que se identifica mediante el valor 255 de ifIndex.

Las interfaces DEBEN numerarse como se indica en el cuadro 6-16.

Cuadro 6-16/J.191 – Numeración de las interfaces en ifTable

Interfaz	Descripción
1	Interfaz WAN-Man
2	Interfaz WAN-Data
2+n	Cada interfaz LAN
255	Interfaz LAN agregada

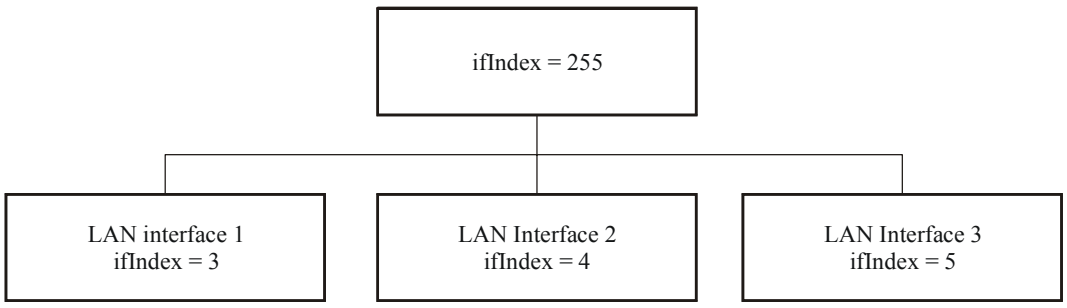
Si ifAdminStatus = down de una interfaz determinada, la misma NO DEBE aceptar o retransmitir ningún tráfico. El objeto ifAdminStatus correspondiente al valor 255 de ifIndex DEBE proporcionar control administrativo de todas las interfaces LAN y DEBE implementarse como RW.

Los valores ifType de ifTable correspondientes a ifIndex 255 DEBEN ser 'Otro' (other). En el caso de PS integrados los valores ifType de ifTable correspondientes a los valores 1 y 2 de ifIndex DEBEN ser 'Otro'. En el caso de PS autónomos el valor ifType de ifTable correspondiente a los valores 1 y 2 de ifIndex DEBEN ser el valor ifType de IANA apropiado.

El valor ifPhysAddress de ifTable correspondiente a ifIndex 255 DEBE ser una cadena de octetos de longitud cero.

Los contadores ifTable de las interfaces WAN de los valores 1 y 2 de ifIndex DEBEN compartirse entre las dos interfaces. Es POSIBLE que se implementen los contadores ifTable para el valor 255 de ifIndex.

El grupo ifStack DEBE implementarse para identificar las relaciones entre la interfaz 'Interfaces LAN agregadas' de capa superior y las subinterfaces LAN de capa inferior. En la figura 6-6 se ilustra la utilización del grupo ifStack para un PS con tres interfaces LAN:



Implementation of ifStack for this example:

ifStackHigherLayer	ifStackLowerLayer
255	3
255	4
255	5

Figura 6-6/J.191 – Ejemplo de implementación de ifStack

6.3.9 Requisitos de ipNetToMediaTable

El ipNetToMediaTable (RFC 2011) hace corresponder las direcciones IP y las direcciones físicas, y su utilización es simple si cada dirección IP se asocia a una interfaz física y si ésta se asocia a una dirección física. No obstante, el PS utiliza distintas direcciones IP que pueden aplicarse a varias interfaces físicas, y asocia la interfaz WAN física con dos direcciones de soporte físico. El PS DEBE relacionar en el cuadro ipNetToMediaTable cada una de las direcciones IP que integran su configuración activa, creando un asiento por cada valor IP[1] distinto y apegándose al cuadro 6-17.

Cuadro 6-17/J.191 – ipNetToMediaTable del PS

ipNetToMediaNetAddress	ipNetToMediaPhysAddress	ipNetToMediaIfIndex
Dirección IP de WAN-Man	Dirección de soporte físico de Wan-Man	1
Direcciones IP de WAN-Datos	Dirección de soporte físico de Wan-Datos	2
Dirección IP de servidor DHCP	Cadena de octetos de longitud cero	255
Dirección IP de servidor DNS	Cadena de octetos de longitud cero	255
Dirección IP de encaminador de servidor	Cadena de octetos de longitud cero	255

6.4 El portal de prueba del cable (CTP)

6.4.1 Objetivos del CTP

Entre los objetivos del portal de prueba del cable se encuentran los siguientes:

- Permitir el diagnóstico de averías del dispositivo IP de LAN.
- Proporcionar visibilidad a los dispositivos IP de LAN, así como acceso al número y tipos de dispositivos IP de LAN.
- Permitir la supervisión de la calidad de funcionamiento de los dispositivos IP de LAN.

6.4.2 Directrices para el diseño del CTP

Las directrices de diseño para el sistema de herramientas de gestión de IPCable2Home se relacionan en el cuadro 6-18. Algunas de estas directrices coinciden con las de diseño del CMP. Esta relación proporciona orientaciones para la especificación de la funcionalidad CTP.

[1] Se creará un asiento por cada una de las direcciones IP de los servidores DHCP, DNS y encaminador sólo si las tres direcciones son distintas. En la configuración LAN del PS más convencional, cuando la misma dirección IP se comparte entre los tres servidores, sólo se visualizará un asiento en ipNetToMediaTable.

Cuadro 6-18/J.191 – Directrices de diseño del sistema CMP

Referencia	Directrices de diseño del sistema CMP
CTP 1	Necesidad de que las interfaces soporten las características y funciones de gestión y diagnóstico necesarias para soportar los servicios basados en cable prestados en la red doméstica.
CTP 2	Se necesitan capacidades de supervisión locales y distantes que puedan controlar el funcionamiento de la red doméstica y ayudar al consumidor y al operador de cable a identificar áreas problemáticas.
CTP 3	El NMS de la red de cable requiere un método de captura de información de identificación de cada dispositivo IP conectado a la red doméstica.
CTP 4	El NMS de la red de cable requiere un método que le permita detectar si un dispositivo conectado se encuentra en un estado operacional.

6.4.3 Descripción del sistema CTP

El CTP (portal de prueba del cable) contiene las "herramientas distantes" mediante las cuales el NMS puede recoger más información de los dispositivos de la LAN. Las pruebas deben efectuarse a distancia, ya que puede resultar problemático atravesar una función de traducción de dirección de red (NAT, *network address translation*) de un direccionador. Por ejemplo, un ping de la WAN a la LAN no atravesará un PS, salvo que el CAP haya sido configurado previamente para cursar este tráfico. El CTP es un apoderado local destinado a interpretar y ejecutar la clase de avería/diagnóstico a distancia de mensajes SNMP que recibe del operador NMS. Estas pruebas de los dispositivos IP de LAN se definen en base a problemas de probable aparición de las redes doméstica de tipo IPCable2Home: conectividad y diagnósticos de caudal.

Estas funciones reciben el nombre de herramienta de velocidad de la conexión CTP y herramienta de ping a distancia del CTP. Las herramientas de velocidad de conexión y de ping a distancia permiten al centro de soporte al cliente del operador de cable y al centro de operaciones de la red obtener más información acerca de la conexión entre el elemento PS y los dispositivos IP de LAN domésticos.

6.4.3.1 Herramienta de velocidad de conexión del CTP

Esta función se utiliza para obtener una medida aproximada de la calidad de funcionamiento del caudal a través del enlace entre el PS y un dispositivo IP de LAN. Envía una ráfaga de paquetes entre el PS y el dispositivo IP de LAN sometido a prueba midiéndose el tiempo de ida y vuelta de la ráfaga. En líneas generales, se puede decir que el operador del NMS otorga valores a algunos parámetros y arranca la función, almacenándose los resultados en la base de datos PS pudiendo recuperarse posteriormente mediante la MIB del CTP.

La función de velocidad de conexión se apoya en los dispositivos IP de LAN para disponer de una "función de establecimiento de bucle" o de un "servicio de eco" integrado. La autoridad de asignación de números Internet (IANA, *Internet assigned numbers authority*) ha asignado el puerto 7 de servicio de eco tanto para el protocolo TCP como para el UDP [RFC 347]. El valor por defecto de la dirección IP de origen (cabhCtpConnSrcIp) es el mismo del valor de la pasarela por defecto de la LAN del PS (cabhCdpServerRouter). El valor de cabhCtpConnSrcIp podrá fijarse a cualquier dirección IP WAN-Data del PS válida o a cualquier dirección IP de interfaz LAN del PS válida. La dirección IP WAN-Man del PS no se utiliza como dirección IP de origen para una herramienta CTP ya que cuando está presente una dirección de este tipo mientras que la dirección IP WAN-Data no lo está, el PS funciona en el modo de manejo de paquetes fundamental de transferencia y el operador de cable puede probar los dispositivos IP de LAN directamente desde la consola del NMS si lo desea. Esta característica de prueba funciona únicamente en los dispositivos

IP de LAN en el sector de direcciones LAN-Trans que implementa la función de servicio de eco conforme a la norma RFC 347.

La cláusula sobre requisitos verificables del CTP, que figura más adelante en este texto, enumera los parámetros y respuestas correspondientes a la herramienta de velocidad de conexión. La cláusula 12.2.1.1 detalla el funcionamiento de la herramienta de velocidad de conexión.

6.4.3.2 Herramienta ping del CTP

Se invoca esta función para verificar la conectividad entre el PS y los dispositivos IP de LAN individuales. El NMS puede reunir los resultados obtenidos tras utilizar varias veces la herramienta ping para crear un barrido de red de los dispositivos IP de LAN. El cuadro DHCP del CDP contiene una relación de dispositivos históricos, aunque sólo figuran los dispositivos que utilizan el DHCP. El ping puede captar el estado actual incluso de los clientes no DHCP. Para mayor sencillez del PS, cabe esperar que el NMS incremente la dirección y almacene los resultados en la herramienta NMS para ejecutar el barrido de una subred de la LAN.

La herramienta ping se inicia por medio de una serie de mensajes SNMP Set-Request emitidos por la consola del NMS de la red de cable a la dirección de gestión del PS.

La herramienta ping del CTP DEBE implementarse utilizando la facilidad "Echo" del protocolo de mensajes de control Internet (ICMP, *Internet control message protocol*). El CTP emitirá una petición de eco ICMP y el dispositivo IP de LAN debería devolver una respuesta de eco ICMP.

El CTP DEBE ignorar, y excluir del contador cabhCtpPingNumRecv, cualquier respuesta de eco que se reciba después de que expire cabhCtpPingTimeOut.

En la cláusula 6.4.4 se relacionan los parámetros y las respuestas de la herramienta ping.

En la cláusula 12.2.1.2 se proporcionan los detalles del funcionamiento de la herramienta ping.

6.4.4 Requisitos del CTP

6.4.4.1 Herramienta de velocidad de la conexión

El CTP DEBE implementar la herramienta de velocidad de conexión, Y DEBE cumplir con los valores por defecto y las gamas de valores definidas para los objetos específicos de la herramienta de velocidad de la conexión de la MIB de CTP de cable.

El CTP TRANSMITIRÁ los bytes de los datos de prueba tan rápido como sea posible cuando esté funcionando la herramienta de velocidad de conexión.

El CTP UTILIZARÁ el puerto 7 como puerto de destino cuando esté funcionando la herramienta de velocidad de la conexión.

Esta herramienta NO DEBE generar paquetes a través de ninguna interfaz WAN.

Cuando el NMS activa el CTP para arrancar la herramienta de velocidad de la conexión fijando cabhConnControl = start(1), el CTP DEBE ejecutar lo siguiente:

- reactivar el temporizador;
- fijar cabhCtpConnStatus = running(2);
- transmitir el número de paquetes igual al valor de cabhCtpConnNumPkts, cada uno con un tamaño igual al valor de cabhCtpConnPktSize, a la dirección IP igual al valor de cabhCtpConnDestIp y al puerto número 7, utilizando el protocolo determinado por cabhCtpConnProto;
- arrancar el temporizador con el primer bit transmitido;
- detener el temporizador cuando se recibe el último bit del dispositivo IP de LAN objetivo O cuando el valor del temporizador es igual al valor de cabhCtpConnTimeOut, lo que suceda primero;

- cuando se detiene el temporizador, fijar cabhCtpConnStatus = complete(3), Y notificar el evento apropiado (véase el anexo B – Eventos del CTP);
- almacenar el valor del temporizador (en milisegundos) en cabhCtpConnRTT;
- si el valor del temporizador es igual al valor de cabhCtpConnTimeOut antes de que se reciba el último bit del dispositivo IP de LAN objetivo, notificar el evento apropiado (véase el anexo B – Eventos del CTP);
- calcular el caudal que se define en el requisito a continuación y almacenar el valor en cabhCtpConnThroughput.

Si la herramienta de velocidad de la conexión se detiene cuando el NMS fija el objeto cabhCtpConnControl = abort(2) o por cualquier otro motivo antes de que se reciba el último bit del dispositivo IP de LAN objetivo O antes de que se detenga el temporizador, el CTP DEBE fijar cabhCtpConnStatus = aborted(4) Y notificar el evento apropiado (véase el anexo B – Eventos del CTP).

Cuando el CTP hace funcionar la herramienta de velocidad de conexión, DEBE determinar el caudal de ida y vuelta promedio entre el PS y el dispositivo IP de LAN cuya dirección se transfirió en cabhCtpConnDestIp (dispositivo IP de LAN objetivo) en kilobits por segundo, redondear el número al entero más próximo, Y almacenar el resultado en cabhCtpConnThroughput.

La cabida útil de los paquetes transmitidos cuando está funcionando la herramienta de velocidad de conexión NO DEBERÍA ser ni todos ceros ni todos unos.

El CTP DEBE reiniciar cabhCtpConnPktsSent, cabhCtpConnPktsRecv, cabhCtpConnRTT y cabhCtpConnThroughput al valor 0 cuando arranca la herramienta de velocidad de conexión (es decir, cuando el valor de cabhCtpConnControl se fija a start(1)).

El tiempo de ida y vuelta (RTT, *round trip time*) de la herramienta de velocidad de la conexión se mide en el PS como el tiempo transcurrido desde el primer bit del primer paquete transmitido hasta el último bit del último paquete recibido. El RTT es válido únicamente si el número de paquetes recibidos es igual al número de paquetes transmitidos.

El CTP DEBE permitir que la dirección IP de destino de la herramienta de velocidad de la conexión (cabhCtpConnDestIp) pueda ser cualquier dirección IPv4 válida de cualquier dispositivo IP de LAN al que se pueda acceder a través de cualquier interfaz LAN del PS que hace funcionar la herramienta de velocidad de conexión del CTP.

Al fijar el objeto de control de la herramienta de velocidad de la conexión, cabhCtpConnControl, con el valor start(1) DEBE dar por resultado la ejecución de esa herramienta.

Al fijar el objeto de control de la herramienta de velocidad de conexión, cabhCtpConnControl, con el valor abort(2) DEBE dar por resultado la terminación de la herramienta.

El valor por defecto de cabhCtpConnStatus es notRun(1), que indica que la herramienta de velocidad de conexión no se ha utilizado aún.

El CTP DEBE fijar el valor de cabhCtpConnStatus a running(2) si la herramienta ha recibido la instrucción de arrancar, no se ha detenido, y el temporizador de velocidad de conexión no ha expirado.

El CTP DEBE fijar el valor de cabhCtpConnStatus a complete(3) cuando recibe el último paquete enviado por la herramienta de velocidad de la conexión.

El CTP DEBE fijar el valor de cabhCtpConnStatus a aborted(4) si la herramienta de velocidad de la conexión se detiene después de su arranque, mediante una fijación SNMP del valor abort(2) al objeto cabhCtpConnControl o si por el contrario la prueba termina antes de que se reciba el último paquete enviado por la herramienta de velocidad de la conexión Y antes de que expire el temporizador (cabhCtpConnTimeOut) de la herramienta de velocidad de la conexión.

El CTP DEBE fijar el valor de cabhCtpConnStatus a timedOut(5) si el temporizador (cabhCtpConnTimeOut) de la herramienta de velocidad de conexión expira antes de que el CTP reciba el último paquete enviado por la herramienta de velocidad de la conexión.

El CTP NO DEBE utilizar ninguna dirección IP de la dirección IP de origen de la herramienta de velocidad de conexión (cabhCtpConnSrcIp) excepto una dirección IP válida actual WAN-Data del PS (es decir, un valor de objeto cabhCdpWanDataAddrIp activo) O una dirección IP válida actual de interfaz LAN del PS. Si se configura un valor no válido para cabhCtpConnSrcIp, el CTP DEBE tratar la ejecución de la prueba como un caso abortado y fijar el objeto cabhCtpConnStatus de estado de la herramienta de velocidad de la conexión a "abortado" notificando el evento apropiado (véase el cuadro B.1).

6.4.4.2 Herramienta Ping

El CTP DEBE implementar la herramienta Ping de CTP, Y DEBE aceptar los valores por defecto y las gamas de valores definidos para los objetos específicos de la herramienta Ping de la MIB de CTP de Cable.

Cuando el NMS activa el CTP para iniciar la herramienta Ping al fijar cabhCtpPingControl = start(1), el CTP DEBE efectuar lo siguiente:

- fijar cabhCtpPingStatus = running(2);
- enviar tantos mensajes Ping (peticiones ICMP) como especifique el valor cabhCtpPingNumPkts a la dirección IP definida por el valor de cabhCtpPingDestIp, utilizando el valor de cabhCtpPingSrcIp como la dirección de origen de cada mensaje. El tamaño de cada trama de prueba emitida es el valor de cabhCtpPingPktSize. El valor de cabhCtpPingTimeOut es el fin de temporización de cada petición Ping,
- si el valor de cabhCtpPingNumPkts es mayor que 1, debe esperar el tiempo necesario definido por el valor de cabhCtpPingTimeBetween entre cada petición Ping transmitida por el CTP.

Si el CTP recibe todas las respuestas Ping antes de la expiración de cualquier temporizador, el CTP DEBE fijar cabhCtpPingStatus = complete(3) Y notificar el evento apropiado (véase el anexo B – Eventos del CTP).

Si el NMS detiene la herramienta Ping fijando el objeto cabhCtpPingControl = abort(2) o por cualquier otro motivo antes de que se reciba el último bit del dispositivo IP de LAN objetivo Y antes de que expire el temporizador, el CTP DEBE fijar cabhCtpPingStatus = aborted(4) Y notificar el evento apropiado (véase el anexo B – Eventos del CTP).

Si el temporizador expira para al menos una de las peticiones Ping, antes de que se reciba su respuesta desde el dispositivo IP de LAN objetivo, el CTP DEBE fijar cabhCtpPingStatus = timedOut(5) Y notificar el evento apropiado (véase el anexo B – Eventos del CTP).

Cuando el CTP hace funcionar la herramienta Ping, DEBE determinar el tiempo de ida y vuelta promedio transcurrido entre el PS y el dispositivo IP de LAN cuya dirección se transfirió en cabhCtpPingDestIp (dispositivo IP de LAN objetivo), por el número de peticiones Ping definidas por cabhCtpPingNumPkts, Y almacenar el resultado en cabhCtpPingAvgRTT. Asimismo, cuando el CTP hace funcionar esta herramienta, DEBE determinar los tiempos de ida y vuelta mínimos y máximos transcurridos entre el PS y el dispositivo IP de LAN objetivo, del conjunto de peticiones Ping definidas por cabhCtpPingNumPkts, y almacenar los valores en cabhCtpPingMinRTT y en cabhCtpPingMaxRTT, respectivamente.

Si se produce un error ICMP durante la ejecución de la herramienta Ping, el CTP DEBE aumentar el valor de cabhCtpPingNumIcmpError Y registrar el error en cabhCtpPingIcmpError. El último error ICMP que se produce suprimirá el registro anterior.

La cabida útil de los paquetes transmitidos durante el funcionamiento de la herramienta Ping NO DEBERÍA ser ni todos ceros ni todos unos.

Cuando se arranca la herramienta Ping (es decir, cuando el valor de cabhCtpPingControl se fija a start(1)) el CTP DEBE reactivar cabhCtpPingNumSent, cabhCtpPingNumRecv, cabhCtpPingAvgRTT, cabhCtpPingMaxRTT, cabhCtpPingMinRTT, cabhCtpPingNumIcmpError y cabhCtpPingIcmpError cada uno al valor 0.

El RTT de la herramienta Ping se mide en el PS como el tiempo transcurrido desde el último bit de cada paquete transmitido por la herramienta Ping de CTP, al instante en que se recibe el último bit de ese paquete.

El CTP DEBE permitir que la dirección IP de destino de la herramienta Ping (cabhCtpPingDestIp) pueda fijarse a cualquier dirección IPv4 válida de cualquier dispositivo IP de LAN al que se pueda acceder a través de cualquier interfaz LAN del PS que hace funcionar la herramienta Ping CTP.

La herramienta Ping NO DEBE generar paquetes por ninguna interfaz WAN.

El CTP NO DEBE utilizar ninguna dirección IP para la dirección IP de origen de la herramienta Ping (cabhCtpPingSrcIp) excepto una dirección IP válida actual WAN-Data del PS (es decir, un valor de objeto cabhCdpWanDataAddrIp activo) O una dirección IP válida actual de interfaz LAN del PS. Si se configura un valor no válido para cabhCtpPingSrcIp, el CTP DEBE tratar la ejecución de la prueba como un caso abortado y fijar el objeto cabhCtpPingStatus de estado de la herramienta Ping a "abortado" y notificar el evento apropiado (véase el cuadro B.1).

6.5 Comunicación de eventos

El mecanismo de comunicación y control de eventos utilizado es RFC 2669, que define un formato normalizado para la comunicación de la información de eventos, independientemente del tipo de mensaje, e incluye un cuadro local de registro histórico de eventos, de cuyos elementos se conservarán tras el rearranque del PS. Obsérvese que los eventos puede generarlos cualquier parte del PS, pero el CMP efectúa las anotaciones históricas y/o comunica el evento o bien localmente o a un servidor de registro histórico del sistema (Syslog) o de trampas (Trap).

6.5.1 Notificación de eventos

El PS DEBE generar eventos asíncronos correspondientes a los eventos y situaciones de importancia especificados (véase el anexo B). Los eventos pueden almacenarse en un registro histórico de eventos interno (LOG), en memoria no volátil, comunicarse a otras entidades SNMP (en forma de mensajes TRAP o INFORMES SNMP), o enviarse como mensaje de evento SYSLOG a un servidor SYSLOG cuya dirección IP se transfiera en la opción 7 de DHCP OFFER que se recibe del servidor DHCP de cabecera a través de la interfaz WAN-Man del PS.

El PS DEBE soportar los siguientes mecanismos de notificación de eventos:

- Registro histórico local de eventos del que ciertas anotaciones pueden conservarse tras un rearranque del PS.
- SNMP TRAP y SNMP INFORM.
- SYSLOG.

La notificación de eventos por parte del PS es totalmente configurable. El PS DEBE implementar docsDevEvControlTable de RFC 2669 a fin de controlar la comunicación de eventos. El PS DEBE soportar los siguientes valores BIT para el objeto RFC 2669 docsDevEvReporting:

- 1: local-no volátil(0)
- 2: trampas(1)
- 3: syslog(2)
- 4: local-volátil(3)

Los mensajes de petición SNMP SET dirigidos al objeto RFC 2669 docsDevEvReporting utilizando los valores siguientes DEBEN provocar un error 'Wrong Value' para las PDU SNMP:

- 0x20 = sólo registro de sistema
- 0x40 = sólo trampa
- 0x60 = sólo (trampa + registro de sistema)

Un evento comunicado por trampa, histórico del sistema o informativo DEBE generar asimismo una anotación histórica en el registro local ya sea volátil o no volátil conforme al cuadro 6-19, y como se describe en 6.5.1.1.

6.5.1.1 Registro histórico local de eventos

El PS DEBE mantener un cuadro de eventos de registro histórico local que almacene los eventos ya sea como locales volátiles o como locales no volátiles. Los eventos almacenados como locales no volátiles DEBEN conservarse tras los rearranques del PS. El cuadro de eventos del histórico local DEBE organizarse como una memoria intermedia cíclica con una capacidad mínima de 10 entradas. El cuadro de eventos del histórico local DEBE ser accesible a través de docsDevEventTable definido en RFC 2669.

La descripción de los eventos DEBE estar en inglés. Las descripciones de los eventos NO DEBEN superar los 255 bytes de longitud, que es el máximo definido para SnmpAdminString.

El EventId es un entero de 32 bits sin signo. Los EventIds comprendidos entre 0 y $(2^{31} – 1)$ están reservados. El EventId DEBE convertirse con arreglo a los códigos de error definidos en el anexo B. Los EventId que van de 2^{31} a $(2^{32} – 1)$ DEBEN utilizarse como específicos del fabricante de acuerdo con el siguiente formato:

- El bit 31 estará activado para indicar un evento específico del fabricante.
- Los bits 30-16 contendrán los 15 bits finales del número de fabricante del SNMP.
- Los bits 15-0 están destinados a la numeración de eventos del fabricante.

El objeto RFC 2669 docsDevEvIndex permite la ordenación relativa de los eventos en el registro histórico. La calificación de los eventos del registro histórico local como volátiles locales y no volátiles locales exige un método de sincronizar los valores docsDevEvIndex entre ambos tipos de eventos tras un rearranque del PS. Tras éste, DEBE utilizarse el siguiente procedimiento para sincronizar los valores docsDevEvIndex correspondientes a los elementos volátiles y no volátiles:

- Los valores de docsDevEvIndex correspondientes a los eventos del registro histórico local calificados como no volátiles locales DEBEN renumerarse desde 1.
- El registro histórico local DEBE inicializarse, acto seguido, con los eventos calificados como no volátiles locales en el mismo orden que tenían antes del rearranque.
- Los eventos subsiguientes anotados en el histórico local, calificados como volátiles locales o bien como no volátiles locales, DEBEN utilizar valores de incremento de docsDevEvIndex.

La reactivación del registro histórico local iniciada por medio de un SNMP SET del objeto docsDevEvControl RFC 2669 DEBE suprimir todos los eventos del histórico local, incluidos los eventos del histórico calificados como volátiles locales o como no volátiles locales.

6.5.1.2 SNMP TRAP y SNMP INFORM

El PS DEBE soportar la PDU SNMP Trap descrita en RFC 2576. El PS DEBE soportar la PDU SNMP INFORM descrita en RFC 2576. INFORM es una variante de trampa y exige que el servidor receptor acuse recibo de la llegada de una PDU InformRequest con una PDU InformResponse.

Cuando se activa en el PS una trampa SNMP normal, DEBE enviar notificaciones para cualquier evento de dicha categoría cuya prioridad sea "error" o "notice".

El PS PUEDE soportar eventos específicos del fabricante. Caso de soportarse, los eventos PS específicos del fabricante que puedan comunicarse mediante SNMP TRAP DEBEN describirse en una MIB privada distribuida con el PS. En la definición de las trampas del SNMP específicas del fabricante, la declaración de OBJECTS de la definición de la trampa privada DEBERÍA contener como mínimo los objetos indicados a continuación:

- EvLevel
- EvIdText
- Umbral de eventos (de haberlos en la trampa)
- IfPhysAddress (dirección física asociada a la dirección IP WAN-Man del PS)

Se pueden incluir más objetos en la sentencia OBJECTS si así se desea.

6.5.1.3 Syslog

Los mensajes SYSLOG emitidos por el PS DEBEN adoptar el siguiente formato:

<nivel>PortalServicesElement[fabricante]: <eventId> texto

siendo:

nivel – presentación en ASCII de la prioridad del evento, encerrada entre paréntesis angulares, interpretada como el OR binario o la facilidad por defecto (128) y la prioridad del evento (0-7). El nivel obtenido puede estar comprendido entre 128 y 135.

fabricante – nombre del fabricante correspondiente a los mensajes SYSLOG específicos del fabricante o "IPCABLE2HOME" para los mensajes de IPCable2Home normales.

eventId – presentación en ASCII del número INTEGER en formato decimal, encerrado entre paréntesis angulares, que identifica de modo exclusivo el tipo de evento. Este EventID DEBE ser el mismo número almacenado en el objeto docsDevEvId de docsDevEventTable. Para los eventos de IPCable2Home normales, este número se convierte utilizando el código de errores de acuerdo con las siguientes reglas:

- El número es un decimal de ocho dígitos.
- Los dos primeros dígitos (los situados más a la izquierda) son el código ASCII (decimal) correspondiente a la letra del código de error.
- Los cuatro dígitos siguientes están ocupados por los dos o tres dígitos existentes entre la letra y el punto del código de error relleno a ceros por la izquierda.
- Los dos últimos dígitos se rellenan con el número que hay tras el punto del código de error relleno a ceros por la izquierda.

Por ejemplo, el evento D04.2 se convierte en 68000402 y el evento I114.1 se convierte en 73011401.

Obsérvese que de este modo sólo se utiliza una pequeña fracción del espacio numérico disponible reservado al IPCable2Home (0 a $2^{31} - 1$). La primera letra de un código de error siempre va en mayúsculas.

texto – para los mensajes de IPCable2Home normales, esta cadena DEBE contener la descripción textual definida en el anexo B.

Ejemplo del evento Syslog correspondiente al evento D04.2: "Time of the day received in invalid format":

<132>Portal ServicesElement[IPCABLE2HOME]: <68000402> Time of the day received in invalid format.

El número 68000402 del ejemplo anterior es el asignado por IPCable2Home a este evento concreto.

6.5.2 Formato de los eventos

Los mensajes de eventos de gestión de IPCable2Home PUEDEN contener las informaciones siguientes:

- Contador de eventos – indicador de la secuencia de eventos.
- Hora del evento – momento de la ocurrencia del evento.
- Prioridad del evento – gravedad de la situación. [RFC 2669] define ocho niveles de gravedad. La gravedad del evento por defecto puede modificarse a un valor distinto para cada evento específico a través de la interfaz SNMP.
- Número de empresa del evento – este número identifica el evento como evento normal o bien como evento definido por el fabricante.
- ID del evento – identifica exactamente el evento cuando está combinado con el número de empresa del evento. Los fabricantes definen sus propios ID de eventos. Los eventos de gestión normal de IPCable2Home se definen en el anexo B. Cada evento de gestión descrito en este anexo tiene asignado un ID de evento de IPCable2Home.
- Texto del evento – describe el evento de manera inteligible.
- Dirección MAC-WAN-Man de PS – describe la dirección MAC del elemento PS que se utiliza para la gestión del dispositivo.
- Dirección MAC-WAN-Datos de PS – describe la dirección MAC del elemento PS que se emplea facultativamente para datos.

El formato exacto de esta información para las trampas e informativos se define en el anexo B. El formato para los mensajes SYSLOG se define en la sección de requisitos de esta cláusula.

6.5.2.1 Prioridad de los eventos

La norma RFC 2669 define ocho niveles de prioridad distintos y los mecanismos de información correspondientes a cada nivel. Los eventos normales especificados en esta Recomendación utilizan los siguientes niveles de prioridad.

Evento de emergencia (prioridad 1)

Se reserva para errores de tipo 'fatal' del equipo físico o de los programas específicos del fabricante que impiden el funcionamiento normal del sistema y provocan el rearranque del sistema informador. Los fabricantes pueden definir sus propios conjuntos de eventos de emergencia. Como ejemplos de estos eventos se pueden citar 'no memory buffers available (no hay memoria intermedia disponible)', 'memory test failure (prueba de memoria fallida)' etc.

Evento de alerta (prioridad 2)

Avería grave que provoca el rearranque del sistema informador a pesar de no ser provocado por un mal funcionamiento del equipo físico ni del soporte lógico. Tras recuperarse del evento, el sistema DEBE enviar la notificación de arranque en frío o caliente.

Evento crítico (prioridad 3)

Avería grave que impide que el dispositivo transmita datos aunque puede recuperarse sin necesidad de rearrancar el sistema. Tras recuperarse de un evento crítico, el PS DEBE enviar la notificación Link Up (enlace activo). Como ejemplos de estos eventos se pueden citar los problemas del fichero de configuración del PS o la incapacidad de obtener una dirección IP a través del DHCP.

Evento de error (prioridad 4)

Avería que podría interrumpir el flujo normal de datos pero que no provoca el rearranque del dispositivo. Los eventos de error pueden comunicarse en tiempo real utilizando el mecanismo TRAP o el SYSLOG.

Evento de alarma (prioridad 5)

Avería que podría interrumpir el flujo normal de datos. Los informes de Syslog y Trap están activados por defecto para este nivel.

Evento de notificación (prioridad 6)

Evento de importancia que no constituye una avería y que puede comunicarse en tiempo real utilizando el mecanismo TRAP o el SYSLOG. Como ejemplo de eventos NOTICE se pueden citar 'Cold Start', 'Warm Start', 'Link Up' y 'SW upgrade successful'.

Evento informativo (prioridad 7)

Evento de importancia que no constituye una avería pero que puede ser útil para el seguimiento del funcionamiento normal del dispositivo.

Evento de depuración (prioridad 8)

Reservado para eventos no críticos específicos del fabricante.

La prioridad asociada a los eventos normales NO DEBE modificarse.

El cuadro 6-19 muestra los tipos de notificación por defecto correspondientes a las diversas prioridades de evento. El PS DEBE implementar los tipos de notificación por defecto para las ocho prioridades de evento. Por ejemplo, el tipo de notificación por defecto para los eventos de emergencia y alerta consiste en inscribirlos en el registro histórico local como entradas no volátiles.

Cuadro 6-19/J.191 – Tipos de notificación por defecto de las prioridades de eventos del PS

Prioridad del evento	No volátil local (bit-0)	Trampa SNMP (bit-1)	SYSLOG (bit-2)	Volátil local (bit-3)	Nota
1) Emergencia	Sí	No	No	No	Específico del fabricante
2) Alerta	Sí	No	No	No	Normal
3) Crítico	Sí	No	No	No	Normal
4) Error	Sí	Sí	Sí	No	Normal
5) Alarma	Sí	Sí	Sí	No	Normal
6) Notificación	No	Sí	Sí	Sí	Normal
7) Informativo	No	No	No	No	Normal y específico del fabricante
8) Depuración	No	No	No	No	Específico del fabricante

El PS DEBE tener la capacidad para poderlo configurar de modo que genere todos los tipos de notificación para cada nivel de prioridad de evento relacionado en el cuadro 6-19.

Cuadro 6-20/J.191 – Nivel mínimo de soporte del tipo de notificación por prioridad del evento en el PS

Prioridad del evento	No volátil local (bit-0)	Trampa SNMP (bit-1)	SYSLOG (bit-2)	Volátil local (bit-3)	Nota
1) Emergencia	Sí	Sí	Sí	Sí	Específico del fabricante
2) Alerta	Sí	Sí	Sí	Sí	Normal
3) Crítico	Sí	Sí	Sí	Sí	Normal
4) Error		Sí	Sí	Sí	Normal
5) Alarma		Sí	Sí	Sí	Normal
6) Notificación		Sí	Sí	Sí	Normal
7) Informativo		Sí	Sí	Sí	Normal y específico del fabricante
8) Depuración		Sí	Sí	Sí	Específico del fabricante

6.5.2.2 Eventos normales

El PS DEBE enviar las siguientes trampas SNMP genéricas, definidas en RFC 3418 y RFC 2863:

- coldStart [RFC 3418];
- linkUp [RFC 2863];
- linkDown [RFC 2863];
- SNMP authentication-Failure [RFC 3418].

El PS DEBE poder generar notificaciones de eventos correspondientes a los eventos normales relacionados en el anexo B.

6.5.3 Estrangulamiento y limitación de eventos

El PS DEBE soportar el estrangulamiento y la limitación de SNMP TRAP/INFORM y SYSLOG descritos en RFC 2669.

El PS DEBE considerar que dos eventos son idénticos si sus EventId son idénticos.

RFC 2669 especifica cuatro estados de estrangulamiento:

- unconstrained(1) (sin restricciones) hace que los mensajes trap y syslog se transmitan sin tener en cuenta los valores umbral.
- maintainBelowThreshold(2) (mantener por debajo del umbral) hace que la transmisión de trap y los mensajes syslog se supriman si el número de trampas sobrepasa el umbral.
- stopAtThreshold(3) (detenerse en el umbral) provoca el cese de la transmisión de las trampas cuando se alcanza el umbral, no reanudándose hasta que se le indique.
- inhibited(4) (inhibido) provoca la supresión de todas las transmisiones de mensajes trap y syslog.

Un evento sencillo DEBE tratarse como tal a efectos del cómputo del umbral, o sea un evento que provoca un mensaje trap y un mensaje syslog sigue tratándose como un único evento.

6.5.4 Notificación de eventos de descarga segura de soporte lógico

En el cuadro B-1, Formato y contenido de las trampas de eventos, SYSLOG y SNMP, se describen los eventos asociados con las actualizaciones del soporte lógico de los servicios de portal, para lo cual se determinan tres categorías: inicialización de la actualización del soporte lógico (SW UPGRADE INIT), fallo general de actualización del soporte lógico y éxito de actualización

del soporte lógico. Estos eventos tienen aplicación únicamente en los PS autónomos, ya que la actualización de soporte lógico (al que se hace referencia también como descarga segura de soporte lógico) de un PS integrado la controla y gestiona el módem de cable. En 11.3.7.1, se definen los requisitos para la descarga segura de soporte lógico de las dos clases de elementos de servicios de portal. El PS integrado, según se define en 5.1.3.1, PS integrado y PS autónomo, NO DEBE generar eventos que estén categorizados en el cuadro B-1, como eventos de "Inicio de actualización de soporte lógico" (SW UPGRADE INIT), eventos de "Fallo general de actualización de soporte lógico" (SW UPGRADE GENERAL FAILURE) o eventos de "Éxito de actualización de soporte lógico" (SW UPGRADE SUCCESS).

7 Herramientas de configuración

7.1 Introducción y presentación

El elemento de servicios de portal y los dispositivos IP de LAN deben inicializarse y configurarse convenientemente a fin de intercambiar información inteligible entre sí, con los elementos conectados a la red de cable y con Internet. Las herramientas de configuración de IPCable2Home permiten realizar esta inicialización y configuración sin interrupciones y con una intervención mínima por parte del usuario. Los operadores de cable pueden asimismo ofrecer a los abonados servicios de datos de alta velocidad de valor añadido mediante la definición de procesos gracias a los cuales aquellos pueden facilitar y adaptar la inicialización y configuración del PS y el dispositivo IP de LAN. Las tres herramientas de configuración definidas para acometer estas tareas son las siguientes:

- La función portal DHCP de cable (CDP) del elemento de servicios de portal.
- La herramienta de configuración de servicios de portal en bloque (BPSC, *bulk PS configuration*).
- El cliente de hora del día del elemento de servicios de portal.

7.1.1 Modos de configuración

Se soportan dos modos de configuración, a saber el modo de configuración DHCP (modo DHCP) y el modo de configuración SNMP (modo SNMP). El cuadro 7-1 compara los dos modos de configuración.

Cuadro 7-1/J.191 – Modos de configuración

	Modo DHCP	**Modo SNMP**
Activador del fichero de configuración del PS	Activado por la presencia de información del servidor TFTP en el mensaje DHCP	Activado por el NMS por medio del mensaje SNMP
Requisito del fichero de configuración del PS	Es necesaria la descarga del fichero de configuración del PS	No es necesaria la descarga del fichero de configuración del PS

El comportamiento específico de las herramientas de configuración depende del modo de configuración en el que funcione el PS.

La cláusula 13, procesos de configuración describe la secuencia de eventos correspondiente a cada uno de los modos de configuración.

7.1.2 Arquitectura de configuración

La figura 7-1 ilustra la arquitectura de configuración. Los elementos de servicio de portal interactúan con las funciones del servidor en la red de cable a través de la interfaz HFC, o con los dispositivos IP de LAN para satisfacer las directrices de diseño del sistema consignadas en 7.2.1.

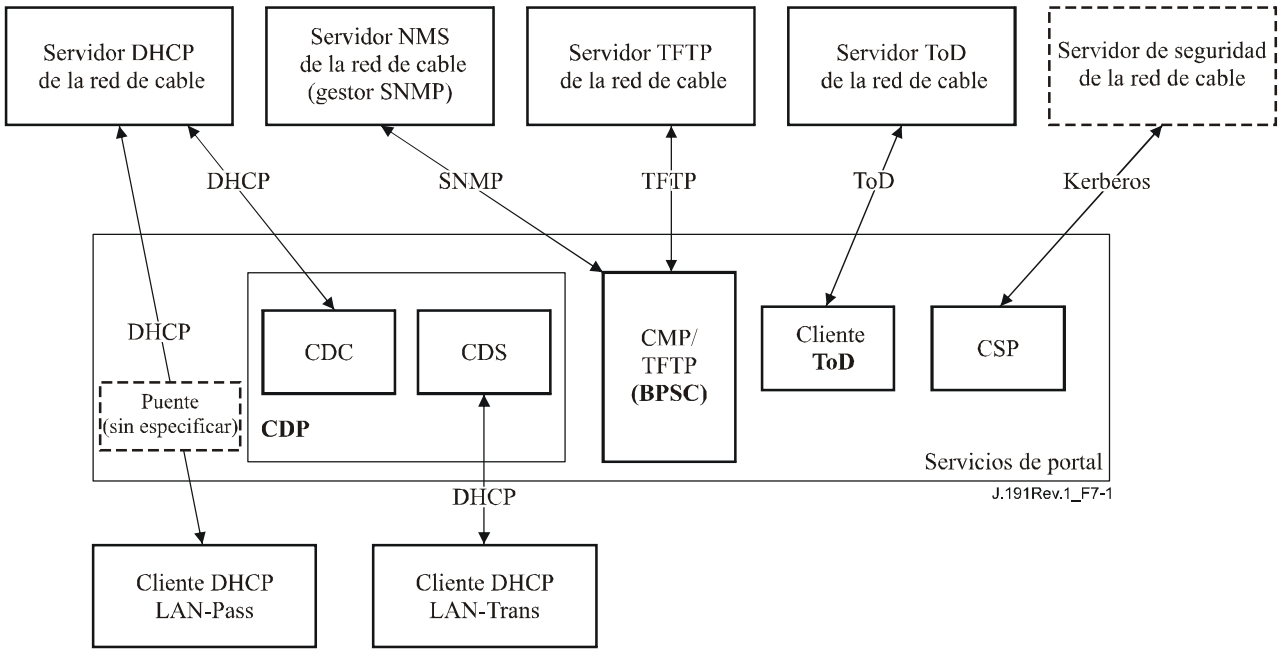


Figura 7-1/J.191 – Arquitectura de configuración

7.1.3 Objetivos

Entre los objetivos del portal DHCP de cable se encuentran:

- La asignación, mediante DHCP, de direcciones IP a los dispositivos IP de LAN de acuerdo con las reglas especificadas en esta cláusula.
- La adquisición, mediante DHCP, de direcciones IP para las interfaces WAN del elemento de servicios de portal de acuerdo con las reglas especificadas en esta cláusula.

Entre los objetivos de la configuración del PS en bloque se encuentra:

- La descarga y procesamiento de los ficheros de configuración.

Entre los objetivos de la hora del día del cliente se encuentra:

- La sincronización del reloj del elemento PS con el de la red de cabecera.

7.1.4 Hipótesis

Entre la hipótesis de funcionamiento del portal DHCP de cable se encuentran las siguientes:

1) Los dispositivos IP de LAN implementan un cliente DHCP definido por RFC 2131.
2) El sistema de configuración de la red de cable implementa un servidor DHCP definido por RFC 2131.
3) Si el servidor DHCP del sistema de configuración de la red de cable soporta la opción 61 de DHCP (opción de identificador de cliente), las interfaces IP WAN-Man y todas las WAN-Data pueden compartir una dirección MAC común.
4) Los dispositivos IP de LAN pueden soportar diversas opciones DHCP y extensiones de fabricante BOOTP permitidas por RFC 2132.

Entre las hipótesis de funcionamiento de la herramienta de configuración del PS en bloque se encuentra:

- La configuración del PS en bloque se llevará a cabo por medio de la descarga de un fichero de configuración del PS que contenga uno o varios parámetros.

Entre las hipótesis de funcionamiento de la hora del día cliente se encuentra la siguiente:

- El servidor DHCP de cabecera proporcionará una opción DHCP a la interfaz WAN-gestión que señale a un servidor de hora del día que funcione dentro de la red de cabecera.

7.2 Arquitectura del portal DHCP de cable

El portal DHCP de IPCable2Home (CDP) es una de las tres herramientas de configuración presentadas en 7.1. En dicha cláusula se describen las directrices de diseño del sistema, la descripción del sistema y los requisitos correspondientes al CDP.

7.2.1 Directrices de diseño del sistema del portal DHCP de cable

Las siguientes directrices de diseño (cuadro 7-2) permiten obtener las capacidades definidas para el CDP:

Cuadro 7-2/J.191 – Directrices de diseño del sistema CDP

Número	Directrices de diseño del sistema CDP
CDP 1	Los mecanismos de direccionamiento los controlará el operador y facilitará al operador conocimiento de los elementos de red IPCable2Home y de los dispositivos IP de LAN, y el acceso a éstos.
CDP 2	Los procesos de adquisición y gestión de direcciones no exigirán la intervención humana (suponiendo que ya se haya establecido una cuenta de usuario u hogar).
CDP 3	La adquisición y gestión de direcciones serán escalables a fin de soportar el aumento previsto del número de dispositivos IP de LAN.
CDP 4	Es preferible que las direcciones de los dispositivos IP de LAN permanezcan inalteradas tras eventos tales como un ciclo de alimentación o un cambio de proveedor de servicios de Internet.
CDP 5	Se suministrará un mecanismo de supervisión y control del número de dispositivos IP de LAN del sector LAN-Trans.
CDP 6	En el hogar, la comunicación continuará funcionando como se proveyó durante las caídas del servidor de direcciones de la cabecera. Se prestará soporte de direccionamiento a los dispositivos IP de LAN recién añadidos y a las direcciones cuya validez haya expirado durante las caídas del servidor de direcciones remoto.
CDP 7	Se conservarán las direcciones IP siempre que sea posible (esto afecta tanto a las direcciones encaminables mundialmente como a las direcciones de gestión de la red de cable privada).

7.2.2 Descripción del sistema del portal DHCP de cable

El portal DHCP de cable (CDP) es la entidad lógica encargada de las actividades de direccionamiento de IPCable2Home. Entre las responsabilidades de petición y atribución de direcciones del CDP dentro del entorno de IPCable2Home se encuentran las siguientes:

- Asignación de direcciones IP, mantenimiento de direcciones IP y entrega de parámetros de configuración (a través del DHCP) a los dispositivos IP de LAN del sector de direcciones LAN-Trans.
- Adquisición de una dirección WAN-Man y de alguna o ninguna dirección IP WAN-Data y de los parámetros de configuración DHCP asociados para el elemento de servicios de portal (PS).
- Información al portal de nombres de cable (CNP) como soporte de los servicios de nombre de servidor del dispositivo IP de LAN.

El PS utiliza dos direcciones de soporte físico, una para obtener una dirección IP para fines de gestión y la otra podría utilizarse para obtener una o más direcciones para los datos. Para evitar la simulación de la dirección de soporte físico, el PS no permite la modificación de ninguna de las dos direcciones de soporte físico.

El elemento de servicios de portal necesita una dirección IP en la LAN doméstica para poder funcionar como encaminador de tráfico (véase la cláusula 8), servidor DHCP (CDS), y servidor DNS (véase la cláusula 9). Para cada una de estas tres funciones de servidor y encaminador del elemento del servicio de portal se salva una dirección IP de LAN en la base de datos del PS. Puede accederse a cada una de ellas a través de un objeto MIB diferente, de los relacionados a continuación y en el cuadro 7-2.

Dirección del encaminador (pasarela por defecto)	cabhCdpServerRouter
Dirección del servidor de nombres de dominio (DNS)	cabhCdpServerDnsAddress
Dirección del servidor del protocolo dinámico de configuración del anfitrión (DHCP) (CDS)	cabhCdpServerDhcpAddress

El valor por defecto de cabhCdpServerRouter es 192.168.0.1. Los valores por defecto de cabhCdpServerDnsAddress y cabhCdpServerDhcpAddress son iguales al valor de cabhCdpServerRouter.

Como muestra la figura 7-2, las capacidades CDP están constituidas por dos elementos funcionales que residen en el interior del CDP: el servidor de DHCP de cable (CDS) y el cliente de DHCP de cable (CDC, *cable DHCP client*).

La figura 7-2 ilustra asimismo la interacción entre los componentes del CDP y los sectores de direcciones presentados en la cláusula 5. El CDC intercambia mensajes DHCP con el servidor DHCP de la red de cable (sector de direcciones de gestión de la WAN) para obtener una dirección IP y opciones de DHCP para el PS, a efectos de gestión. El CDC podría intercambiar asimismo mensajes de DHCP con el servidor de DHCP de la red de cable (sector de direcciones WAN-Data) para obtener alguna o ninguna dirección IP en representación de los dispositivos IP de LAN del sector LAN-Trans. El CDS intercambia mensajes DHCP con los dispositivos IP de LAN en el sector LAN-Trans, asigna direcciones IP privadas, otorga licencias y puede ofrecer opciones DHCP a los clientes DHCP de dichos dispositivos IP de LAN. Los dispositivos IP de LAN del sector LAN-Pass reciben sus direcciones IP, sus licencias y las opciones DHCP directamente del servidor DHCP de la red de cable. El CDP se limita a hacer de puente para los mensajes DHCP entre el servidor DHCP de la red de cable y los dispositivos IP de LAN del sector LAN-Pass.

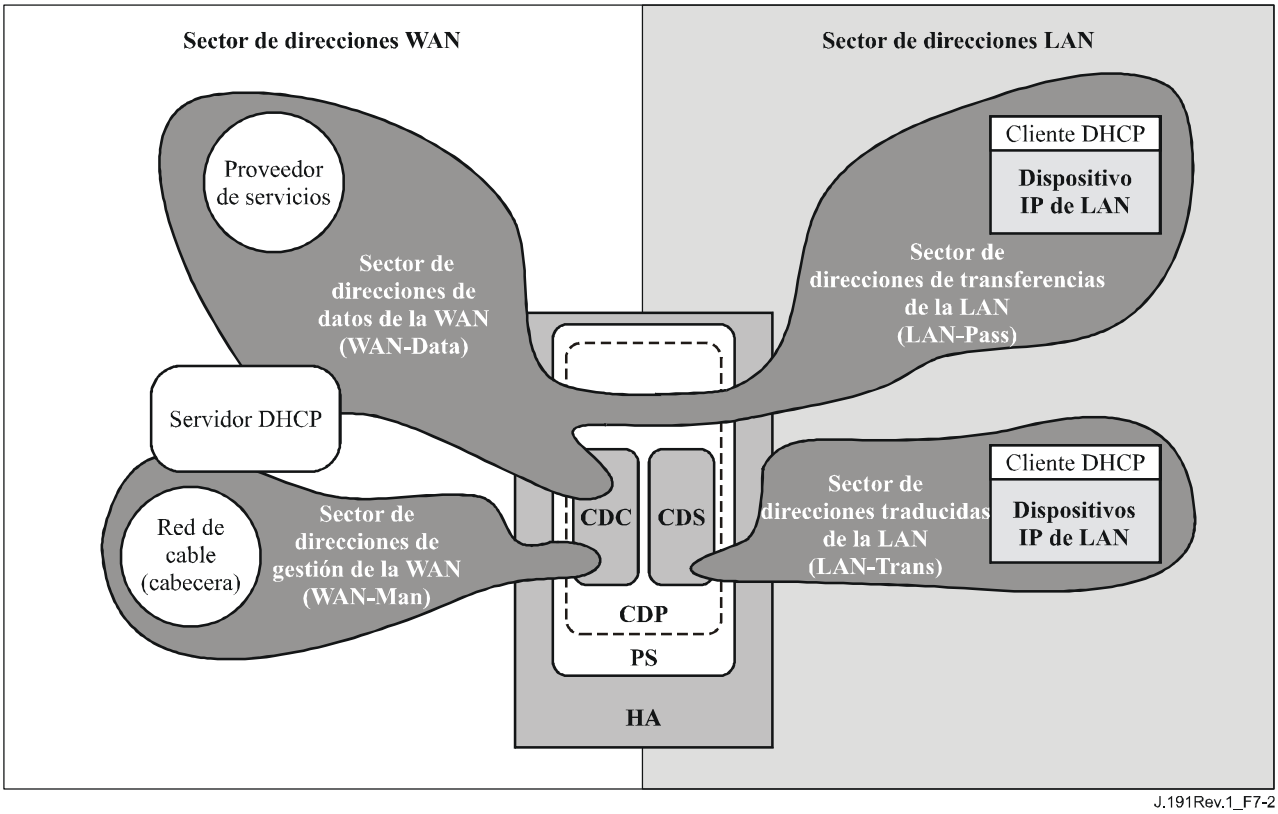


Figura 7-2/J.191 – Funciones del CDP

7.2.2.1 Descripción del sistema CDS

El CDS es un servidor DHCP normal definido en RFC 2131, incluyéndose entre sus fines los siguientes:

- El CDS asigna direcciones y entrega parámetros de configuración del DHCP a los dispositivos IP de LAN que reciben una dirección del sector de direcciones LAN-Trans. El CDS se entera de las opciones DHCP por el sistema NMS y proporciona estas opciones DHCP a los dispositivos IP de LAN. Si las opciones DHCP no hubieran sido proporcionadas por el sistema NMS (por ejemplo, cuando el PS arranca o durante una desconexión del cable), el CDS utilizaría los valores por defecto integrados (DefVals) de las opciones requeridas.
- El CDS es capaz de proporcionar servicios de direccionamiento DHCP a los dispositivos IP de LAN, con independencia del estado de conectividad de la WAN.
- El número de direcciones que el CDS suministra a los dispositivos IP de LAN se puede controlar por medio del sistema NMS. El comportamiento del CDS cuando se sobrepasa el límite, ajustable por el operador de cable, también puede configurarse mediante el NMS. Entre las posibles acciones del CDS cuando se supera dicho límite se encuentran:

  1) asignar una dirección IP LAN-Trans y tratar la interconexión CAT de la WAN a la LAN como se haría normalmente si no se hubiera superado el límite; y

  2) no asignar direcciones a los dispositivos IP de LAN solicitantes.

  El ajuste a 0 del umbral de dirección indica el umbral máximo posible para el grupo de direcciones IP LAN-Trans definido mediante los valores "start" (cabhCdpLanPoolStart) y "end" (cabhCdpLanPoolEnd) del grupo.
- A falta de información horaria procedente del servidor de hora del día (ToD, *time of day*), el CDS utiliza la hora GMT 00:00:0 (medianoche) del 1 de enero de 1970 de arranque

del PS por defecto, actualiza los plazos de expiración de las licencias activas en el sector LAN-Trans para volver a sincronizarse con los clientes DHCP en los dispositivos IP de LAN y mantiene las licencias basadas en dicho instante de arranque hasta que el PS se sincronice con el servidor de hora del día de la red de cable.

- Al rearrancarse el PS, el CDS se mantiene inactivo hasta ser activado por el PS.
- Si el modo de tratamiento de paquetes primario del PS (cabhCapPrimaryMode) tuviera el valor Pass-through (transferencia) y se ha completado el proceso de configuración del PS (indicado mediante cabhPsDevProvState = pass(1)), se desactivaría el CDS.

Los dispositivos IP de LAN pueden recibir direcciones que residan en el sector LAN-Pass. Como muestra la figura 7-2, las peticiones de direcciones LAN-Pass son atendidas por la infraestructura de direccionamiento de la WAN, no por el PS. Los procesos de direccionamiento LAN-Pass tendrán lugar cuando el PS esté configurado para funcionar en modo transparencia o en modo mixto puenteo/encaminamiento (véanse más detalles en 8.2.2.2). En dichos casos, las interacciones DHCP tendrán lugar directamente entre los dispositivos IP de LAN y los servidores de la cabecera, no especificándose el proceso en la presente Recomendación.

En la presente Recomendación, los términos asignación dinámica y asignación manual se utilizan con arreglo a la definición de RFC 2131. Las opciones DHCP proporcionadas por el CDS, objetos cabhCdpServer de la MIB del CDP, son opciones que pueden ser suministradas por el NMS, y las ofrece el CDS a los dispositivos IP LAN que tienen asignada una dirección LAN-Trans. Las opciones DHCP proporcionadas por el CDS, objetos cabhCdpServer, se conservan tras un ciclo de alimentación del PS, pudiendo el sistema NMS establecer, leer, escribir y borrar dichos objetos. Las opciones DHCP proporcionadas por el CDS, objetos cabhCdpServer, se conservan durante los periodos de desconexión del cable, ofreciéndose estos objetos a los dispositivos IP de LAN con una dirección LAN-Trans asignada durante los periodos de desconexión del cable. La conservación en el almacenamiento del CDC de las opciones DHCP es congruente con la sección 2.1 de RFC 2131. Los valores por defecto de las opciones DHCP proporcionadas por el CDS, objetos cabhCdpServer, se definen (cuadro 7-2) pudiendo el NMS restaurar los valores por defecto de las opciones DHCP proporcionadas por el CDS, objetos cabhCdpServer, escribiendo en el objeto de la MIB cabhCdpSetToFactory.

Los objetos del umbral de direcciones del CDS (cabhCdpLanTrans) contienen los parámetros de control de eventos utilizados por el CDS para indicar al CMP que genere una notificación al sistema de gestión de cabecera cuando el número de direcciones LAN-Trans asignadas por el CDS supere el umbral preestablecido.

El objeto contador de direcciones (cabhCdpLanTransCurCount) es un valor que indica el número de direcciones LAN-Trans asignadas por el CDS con licencias DHCP activas.

El objeto umbral de direcciones (cabhCdpLanTransThreshold) es un valor que indica al sistema de gestión de la cabecera la generación de una notificación. La notificación se genera cuando el CDS asigna una dirección al dispositivo IP de LAN que provoca que el contador de direcciones (cabhCdpLanTransCurCount) sobrepase el umbral de direcciones (cabhCdpLanTransThreshold).

La acción de umbral sobrepasado (cabhCdpLanTransAction) es la emprendida por el CDS cuando el contador de direcciones (cabhCdpLanTransCurCount) sobrepasa el umbral de direcciones (cabhCdpLanTransThreshold). Si la acción de umbral sobrepasado (cabhCdpLanTransAction) permite que se asignen direcciones una vez sobrepasado el contador, se genera una notificación cada vez que se asigna una dirección. Las acciones definidas son las siguientes:

a) asignar una dirección LAN-Trans con normalidad; y

b) no asignar dirección alguna al siguiente dispositivo IP de LAN que efectúe una petición.

El contador de direcciones (cabhCdpLanTransCurCount) continúa actualizándose durante los periodos de desconexión del cable.

La MIB del CDS contiene asimismo los parámetros comienzo del grupo de direcciones (cabhCdpLanPoolStart) y final del grupo de direcciones (cabhCdpLanPoolEnd). Estos parámetros indican el intervalo de direcciones del sector LAN-Trans que el CDS puede asignar a dispositivos IP de LAN.

El cuadro de direcciones LAN del CDP (cabhCdpLanAddrTable) contiene la lista de parámetros asociados a las direcciones asignadas a los dispositivos IP de LAN con direcciones LAN-Trans. Entre estos parámetros se encuentran:

1) Los identificadores de cliente mencionados en la sección 9.14 de RFC 2132 (cabhCdpLanAddrClientID).
2) Las direcciones IP de LAN asignadas al cliente (cabhCdpLanAddrIp).
3) Una indicación de si la dirección se asignó manualmente (a través del CMP) o dinámicamente (a través del CDP) (cabhCdpLanAddrConfig).

El CDS almacena información de identificación de dispositivos IP LAN en el objeto MIB cabhCdpLanAddrClientID. Además utiliza el valor transferido en el campo chaddr del mensaje de petición DHCP enviado por el dispositivo IP LAN para este efecto.

El CDS crea una anotación en el cuadro CDP (cabhCdpLanAddrTable) cuando asigna una dirección IP a un dispositivo IP de LAN. El CDS puede crear anotaciones en el cuadro CDP (cabhCdpLanAddrTable) durante los periodos de desconexión del cable.

El cuadro CDP (cabhCdpLanAddrTable) mantiene un tiempo de licencia DHCP para cada uno de los dispositivos IP de LAN.

Las anotaciones del cuadro CDP (cabhCdpLanAddrTable) proporcionadas por el NMS se conservan durante los periodos de desconexión del cable y se mantienen tras un ciclo de alimentación del PS.

7.2.2.2 Descripción del sistema CDC

El CDC es un cliente DHCP normal definido en RFC 2131, incluyéndose entre sus fines los siguientes:

- El CDC lanza peticiones a los servidores DHCP de cabecera para la adquisición de direcciones del sector WAN-Man pudiendo lanzar peticiones a los servidores DHCP de cabecera para la adquisición de direcciones en los sectores de direcciones WAN-Data. El CDC entiende asimismo ciertos parámetros de configuración DHCP del cable y actúa sobre ellos.
- El CDC soporta la adquisición de una dirección IP WAN-Man y de ninguna o alguna dirección IP WAN-Data.
- El CDC soporta la opción de identificador de clase de fabricante (opción 60 del DHCP), la opción de información específica del fabricante (opción 43 del DHCP), y la opción de identificador del cliente (opción 61 del DHCP).
- Por defecto, el CDC adquirirá una única dirección IP para ser utilizada simultáneamente por las interfaces WAN-Man y WAN-Data a fin de reducir al mínimo las modificaciones necesarias de los servidores DHCP de cabecera existentes. En esta situación por defecto no se exige la utilización de un identificador de cliente (opción 61 del DHCP) por parte del CDC.

El CDP soporta diversas opciones DHCP y extensiones de fabricante BOOTP, contempladas en RFC 2132.

La opción de identificador de la clase de fabricante (opción 60 del DHCP) define una clase de dispositivo específica. En el caso de IPCable2Home la opción de identificador de la clase de fabricante contendrá la cadena IPCable2Home para identificar un elemento lógico de servicios de

portal (PS) de IPCable2Home, siempre que un CDC solicite una dirección WAN-Man o WAN-Data.

La opción de información específica del fabricante (opción 43 del DHCP) identifica además el tipo de dispositivo y sus capacidades. Describe el tipo de componente que lanza la petición (integrado o autónomo, CM o PS), los componentes que contiene el dispositivo (CM, MTA, PS, etc.), el número de serie del dispositivo y permite asimismo parámetros específicos del dispositivo. En 7.2.3.3 se definen la opción 43 de DHCP y sus subopciones.

Los cuadros 7-4 y 7-5 contienen detalles de los requisitos para soportar las opciones 60 y 43 del DHCP. El cuadro 7-6 contiene los detalles relativos a otras opciones DHCP facultativas y obligatorias.

El parámetro de recuento de direcciones IP WAN-Data de la MIB del CDP (cabhCdpWanDataIpAddrCount) es el número de licencias de direcciones IP que el CDC debe tratar de conseguir para el lado WAN de las correspondencias entre NAT y NAPT. El valor por defecto de cabhCdpWanDataIpAddrCount es cero, y significa que, por defecto, el CDC conseguirá sólo una dirección IP WAN-Man.

7.2.2.2.1 Opción 61 de cliente de DHCP del cable

El elemento PS puede tener una o varias dirección IP de WAN asociadas a una o varias interfaces de la capa de enlace (por ejemplo, la MAC). Por consiguiente, el CDC no puede depender exclusivamente de una dirección MAC como único valor identificativo del cliente.

Esta Recomendación permite la utilización de la opción de identificador del cliente (opción 61 del DHCP), sección 9.14 de [RFC 2132], para identificar de modo único la interfaz WAN lógica asociada a una dirección IP determinada.

Es necesario que el PS tenga dos direcciones de soporte físico: una que se utilizará para identificar de modo exclusivo la interfaz WAN lógica asociada con la dirección IP WAN-Man (dirección de soporte físico WAN-Man) y la otra que se empleará para identificar de modo exclusivo la interfaz WAN lógica asociada con las direcciones IP WAN-Data (dirección de soporte físico WAN-Data).

7.2.2.2.2 Modos de direccionamiento WAN

Para lograr la compatibilidad con tantos sistemas de configuración de los operadores de cable como sea posible, el CDC debe soportar los siguientes modos configurables de direccionamiento de la WAN:

Modo 0 de direccionamiento de la WAN: El elemento PS utiliza una sola dirección IP WAN, obtenida a través del DHCP utilizando la dirección de soporte físico WAN-Man. El elemento PS tiene una interfaz IP WAN-Man y ninguna interfaz IP WAN-Data IP. Este modo de direccionamiento se aplica únicamente cuando el modo de manejo de paquetes primario del PS (cabhCapPrimaryMode) se fija a transferencia (véase 8.3.2). El servidor de DHCP de cabecera del operador de cable normalmente no necesita efectuar modificaciones del soporte lógico para soportar este modo de direccionamiento. En el modo 0 de direccionamiento de la WAN, el valor de cabhCdpWanDataIpAddrCount es cero.

Modo 1 de direccionamiento de la WAN: El elemento PS utiliza una sola dirección IP de la WAN, obtenida a través de DHCP utilizando la dirección de soporte físico de WAN-Man. El elemento PS tiene una interfaz IP WAN-Man y otra IP WAN-Data y ambas comparten una sola dirección IP común. Este modo de direccionamiento se aplica únicamente cuando el modo de manejo de paquetes primario del PS (cabhCapPrimaryMode) se fija a NAPT. El servidor de DHCP de la cabecera del operador de cable normalmente no necesita efectuar modificaciones del soporte lógico para soportar este modo de direccionamiento. En el modo 1 de direccionamiento de la WAN el valor de cabhCdpWanDataIpAddrCount es cero.

Modo 2 de direccionamiento WAN: El elemento PS consigue una dirección IP WAN-Man utilizando la dirección única de soporte físico WAN-Man y a continuación el NMS lo configura para solicitar una o más direcciones únicas IP WAN-Data. El elemento PS tendrá una interfaz IP WAN-Man y una o varias interfaces IP WAN-Data. Todas las direcciones IP WAN-Data compartirán una dirección de soporte físico común que es única a partir de la dirección de soporte físico WAN-Man. Cada una de las dos o más interfaces (una interfaz WAN-Man y una o varias WAN-Data) tienen su propia dirección IP no compartida. El operador de cable configura el CDP para funcionar en el modo 2 de direccionamiento de la WAN escribiendo un valor distinto de cero en cabhCdpWanDataIpAddrCount, a través del fichero de configuración del PS o de una petición de establecimiento SNMP. Este modo de direccionamiento se aplica cuando el modo de manejo de paquetes primario del PS (cabhCapPrimaryMode) se fija a NAPT o NAT. Es posible que el servidor DHCP de la cabecera del operador de cable necesite modificar el soporte lógico para incluir el soporte de los identificadores de clientes (opción 61 de DHCP) de modo que pueda asignar múltiples direcciones IP a la dirección única del soporte físico WAN-Data.

Existen cuatro casos posibles para el direccionamiento IP de WAN-Data:

1) El PS se configura de modo que no solicite ninguna dirección IP WAN-Data. En este caso no son necesarios los ID de cliente WAN-Data.

2) El PS se configura de modo que solicite una o más direcciones IP WAN-Data y sin anotaciones cabhCdpWanDataAddrClientId configuradas por el operador en la MIB del CDP. El PS deberá autogenerar tantos ID únicos de cliente WAN-Data como el valor de cabhCdpWanDataIpAddrCount.

3) El PS se configura de modo que solicite una o varias direcciones IP WAN-Data y habrá por lo menos tantas anotaciones cabhCdpWanDataAddrClientId configuradas por el operador como el valor de cabhCdpWanDataIpAddrCount, es decir, el operador habrá previsto suficientes valores de ID de cliente WAN-Data. El PS no autogenera ningún ID de cliente.

4) El PS se configura de modo que solicite una o más direcciones IP WAN-Data y habrá menos anotaciones cabhCdpWanDataAddrClientId configuradas por el operador que el valor de cabhCdpWanDataIpAddrCount, es decir, el operador habrá previsto algunos valores ID de cliente WAN-Data pero no los suficientes. El PS tendrá que autogenerar suficientes ID únicos de cliente WAN-Data adicionales hasta alcanzar el número total de ID únicos de cliente WAN-Data igual al valor de cabhCdpWanDataIpAddrCount.

Si el operador de cable desea que el PS consiga una o varias direcciones IP WAN-Data, que sean distintas de la dirección IP WAN-Man, se deberá seguir el siguiente procedimiento. Para todos los modos de direccionamiento de la WAN, en primer lugar el PS solicita una dirección IP WAN-Man utilizando la dirección de soporte físico WAN-Man. En el procedimiento que se describe más adelante se supone que el PS ya ha conseguido una dirección IP WAN-Man:

1) El operador de cable facultativamente suministra al PS algunos ID únicos de cliente particulares, al escribir valores en las anotaciones cabhCdpWanDataAddrClientId del cuadro cabhCdpWanDataAddrTable de la MIB del CDP, a través del fichero de configuración de PS o de mensajes de petición de establecimiento de SNMP.

2) El operador de cable configura el CDP de modo que funcione en el modo 2 de direccionamiento de la WAN al escribir en cabhCdpWanDataIpAddrCount un valor distinto de cero a través del fichero de configuración del PS o de un mensaje de petición de establecimiento de SNMP.

3) Después de que el CDP se configura para que funcione en el modo 2 de direccionamiento de la WAN conforme a la descripción en el paso 2), el PS verifica si el NMS ha proporcionado valores de ID de cliente como se describe en el paso 1). Si se ha proporcionado un determinado número de valores de ID de cliente mayor que o igual al valor de cabhCdpWanDataIpAddrCount, el PS emplea esos valores en la opción 61 de

DHCP cuando solicita direcciones IP WAN-Data. Si los valores de ID de cliente no han sido suministrados, es decir, no existen las anotaciones cabhCdpWanDataAddrClientId, o el número de los valores de ID de cliente proporcionados es menor que el valor de cabhCdpWanDataIpAddrCount, el PS genera varios valores únicos de ID de cliente de manera que en combinación con los ID de cliente suministrados, el número total de ID de cliente únicos será igual al valor de cabhCdpWanDataIpAddrCount. El PS genera valores de ID de cliente utilizando la dirección de soporte físico de WAN-Data sólo para la primera dirección IP WAN-Data solicitada, y concatenando la dirección de soporte físico WAN-Data con un contador de 8 bits de longitud para la segunda y todas las direcciones IP WAN-Data subsiguientes. Si el NMS no ha suministrado ID de cliente, el primer valor del contador de 8 bits es 0x02 (que indica la segunda dirección IP WAN-Data solicitada), el segundo valor del contador es 0x03, etc.

Ejemplo para el caso cuando el NMS no ha suministrado los ID de cliente:

Dirección de soporte físico WAN-Data asignada 0xCDCDCDCDCDCD

ID de cliente generado por el PS para la primera dirección IP WAN-Data solicitada: 0xCDCDCDCDCDCD

ID de cliente generado por el PS para la segunda dirección IP WAN-Data solicitada: 0xCDCDCDCDCDCD02

ID de cliente generado por el PS para la tercera dirección IP WAN-Data solicitada: 0xCDCDCDCDCDCD03

ID de cliente generado por el PS para la enésima dirección IP WAN-Data solicitada: 0xCDCDCDCDCDCDn ($n \leq 0xFF$)

Si el NMS ha suministrado algunos ID de cliente pero el número es menor que el valor de cabhCdpWanDataIpAddrCount, el PS genera los ID de cliente adicionales que resulten necesarios para llevar el número total de ID de cliente al valor de cabhCdpWanDataIpAddrCount. El PS genera estos valores de ID de cliente adicionales agregando un valor de recuento de 8 bits a la dirección de soporte físico WAN-Data, iniciando con 0x02, a menos que este valor duplique un ID de cliente ya suministrado. Si los ID de cliente proporcionados por el NMS utilizan el mismo formato (dirección de soporte físico con valor de recuento de 8 bits), el PS debe utilizar un valor de recuento único para no duplicar un ID de cliente ya suministrado.

Ejemplo para el caso cuando el NMS ha suministrado los ID de cliente (tres valores de ID de cliente suministrados, cabhCdpWanDataIpAddrCount = 5):

Dirección de soporte físico WAN-Data asignada 0xCDCDCDCDCDCD

Primer ID de cliente suministrado para la primera dirección IP WAN-Data: 0x0A0A0A0A0A1A

Segundo ID de cliente suministrado para la segunda dirección IP WAN-Data: 0x0A0A0A0A0A2A

Tercer ID de cliente suministrado para la tercera dirección IP WAN-Data: 0x0A0A0A0A0A3A

Primer ID de cliente generado por el PS para la cuarta dirección IP WAN-Data solicitada: 0xCDCDCDCDCDCD02

Segundo ID de cliente generado por el PS para la quinta dirección IP WAN-Data solicitada: 0xCDCDCDCDCDCD03

4) El PS añade los valores de ID de cliente que genera como anotaciones cabhCdpWanDataAddrClientId al final de cabhCdpWanDataAddrTable.

5) El PS (CDC) solicita (repitiendo el proceso DHCP DISCOVER según proceda) tantas direcciones IP WAN Data únicas según especifique el valor de cabhCdpWanDataIpAddrCount, utilizando la dirección de soporte físico WAN-Data en el campo chaddr del mensaje DHCP y el valor o valores de ID de cliente del paso 3) en la opción 61 de DHCP, iniciando con la primera anotación cabhCdpWanDataAddrClientId de cabhCdpWanDataAddrTable. El CDC no deberá solicitar más direcciones IP WAN-Data que el valor de cabhCdpWanDataIpAddrCount, aun si el número de ID de cliente suministrado es mayor que el valor de cabhCdpWanDataAddrTable.

7.2.3 Requisitos del portal DHCP de cable

7.2.3.1 Requisitos del CDP

Tanto en la configuración integrada como en la autónoma, el PS DEBE implementar dos direcciones de soporte físico WAN únicas: la dirección de soporte físico WAN-Man del PS y la dirección de soporte físico WAN-Data del PS. El valor numérico de esta última dirección DEBE seguir la secuencia del valor numérico de la primera dirección. Las dos direcciones DEBEN permanecer una vez fijadas en la fábrica. El PS NO DEBE permitir la modificación de estas dos direcciones fijadas en la fábrica.

En ambos casos, PS integrado y PS autónomo, el elemento PS DEBE tener direcciones de soporte físico de interfaz WAN distintas de la dirección de soporte físico del módem de cable.

7.2.3.2 Requisitos del CDS

El comportamiento del CDS DEBE ajustarse a los requisitos del servidor consignados en la sección 4.3 de RFC 2131.

El CDS DEBE soportar la asignación dinámica y manual de direcciones conforme a la sección 1 de RFC 2131.

DEBERÁ soportarse la asignación manual de dirección IP del CDS utilizando las anotaciones cabhCdpLanAddrTable de la MIB del CDP que se crean a través del sistema NMS o del fichero de configuración del PS.

Para soportar la asignación dinámica de la dirección IP, el CDS DEBE tener la capacidad de crear, modificar y suprimir anotaciones cabhCdpLanAddrTable para los dispositivos asignados a la dirección LAN-Trans.

Durante una interrupción del cable se DEBEN mantener las anotaciones del cuadro (cabhCdpLanAddrTable) de gestión de direcciones LAN del CDP suministradas y DEBERÁN continuar después de un ciclo de alimentación de energía del PS. El CDS DEBE ser capaz de proporcionar servicios de direccionamiento DHCP a los dispositivos IP de LAN cuando el PS habilite esta función, independientemente de la condición de conectividad de la red WAN.

Durante una reactivación o rearranque del PS, el CDS NO DEBE intercambiar mensajes DHCP con dispositivos IP LAN hasta que el PS active el CDS.

El PS DEBE activar el CDS, es decir, el CDS COMENZARÁ respondiendo a los mensajes DHCP DISCOVER y DHCP REQUEST que se reciben a través de la interfaz LAN del PS, bajo cualquiera de las siguientes condiciones (véase también la figura 13-2):

- Cuando el PS está funcionando en el modo de configuración DHCP, a partir de que el CDC recibe una licencia de dirección IP WAN-Man del PS y el PS ha recibido y procesado adecuadamente un fichero de configuración PS.
- Cuando el PS está funcionando en el modo de configuración SNMP, a partir de que el CDC ha recibido una licencia de dirección IP WAN-Man del PS, ha realizado la autenticación con el servidor del centro de distribución de claves (KDC), y ha sido admitido satisfactoriamente en el NMS.

- Cuando fracasa el primer intento del CDC para conseguir una licencia de dirección IP WAN-Man del PS.
- Cuando el PS está funcionando en el modo de configuración DHCP y fracasa el primer intento para descargar o procesar el fichero de configuración del PS.
- Cuando el PS está funcionando en el modo de configuración SNMP y fracasa el intento de autenticación con el servidor KDC.
- Cuando el PS está funcionando en el modo de configuración SNMP y recibe una señal de activación para descargar un fichero de configuración del PS antes de que se inicie el funcionamiento del CDS, y fracasa el primer intento para descargar o procesar el fichero de configuración del PS.

El CDS DEBE asignar una dirección IP única disponible a partir de la gama de direcciones que comienza con cabhCdpLanPoolStart y termina con cabhCdpLanPoolEnd, a cada uno de los dispositivos IP de LAN en el sector LAN-Trans que solicita una dirección IP utilizando DHCP, si el número de direcciones IP que ya han sido asignadas por el CDS es menor que el valor de cabhCdpLanTransThreshold.

Si el valor de cabhCdpLanTransThreshold es 0, el CDS DEBE tratar el umbral como si se le hubiese asignado el valor más grande posible del tamaño del grupo de direcciones IP LAN-Trans actual (que se define mediante los valores de arranque del grupo de direcciones IP LAN-Trans (cabhCdpLanPoolStart) y de terminación del mismo grupo (cabhCdpLanPoolEnd)).

El CDS DEBE mantener el parámetro del contador de direcciones (cabhCdpLanTransCurCount) indicando el número de licencias de dirección LAN-Trans activas otorgadas a los dispositivos IP LAN.

El contador de direcciones DEBE incrementarse cada vez que se otorga licencia para una dirección LAN-Trans a un dispositivo IP de LAN y DEBE disminuirse cada vez que se libera una dirección LAN-Trans o expira una licencia de la misma.

El CDS DEBE comparar el parámetro contador de direcciones (cabhCdpLanTransCurCount) con el parámetro umbral de direcciones (cabhCdpLanTransThreshold) tras asignar direcciones LAN-Trans. Si el parámetro contador de direcciones (cabhCdpLanTransCurCount) es mayor que el parámetro umbral de direcciones (cabhCdpLanTransThreshold), DEBE generarse una notificación conforme al mecanismo de comunicación de eventos definido en 6.5 y en el anexo B. Cuando el parámetro contador de direcciones (cabhCdpLanTransCurCount) sea mayor que el parámetro umbral de direcciones (cabhCdpLanTransThreshold), el CDS DEBERÁ poder emprender las siguientes acciones de superación de umbral para el siguiente DHCP DISCOVER desde la LAN: asignar las direcciones LAN-Trans con normalidad o no asignar direcciones en absoluto.

Si cabhCdpLanTransCurCount iguala o excede a cabhCdpLanTransThreshold Y un dispositivo IP de LAN solicita una licencia de dirección IP adicional, la acción específica que tome el CDS DEBE ser la indicada por el parámetro suministrado por la acción de umbral sobrepasado (cabhCdpLanTransAction).

El CDS DEBE asignar direcciones IP y entregar los parámetros de configuración DHCP enumerados en el cuadro 7-3 para los cuales el CDS tiene un valor válido, únicamente a los dispositivos IP de LAN que reciben una dirección en el sector de direcciones LAN-Trans.

Si el operador de cable aporta valores para una fila en el cuadro cabhCdpLanAddrTable, el PS (CDS) DEBE ofrecer una licencia (es decir, debe intentar asignarla) para la dirección IP cabhCdpLanAddrIp proporcionada, al dispositivo IP de LAN cuya dirección de soporte físico corresponde al identificador cabhCdpLanAddrClientID proporcionado, en respuesta a un DCHP DISCOVER recibido del dispositivo IP de LAN.

Cuando el CDS asigna una licencia activa para una dirección IP a un dispositivo IP de LAN, el CDP DEBE suprimir esa dirección del grupo de direcciones IP disponibles para su asignación a los dispositivos IP de LAN.

Si el CDS recibe una petición de licencia de un dispositivo IP de LAN y no puede atenderla debido a la falta de direcciones en el grupo de direcciones IP (definido por cabhCdpLanPoolStart y CabhCdpLanPoolEnd), deberá notificar el evento conforme al anexo B y al mecanismo de notificación de eventos que se define en 6.5.

El CDS DEBE almacenar el valor transferido en el campo chaddr del mensaje de petición DHCP enviado por el dispositivo IP de LAN cuando se crea una licencia activa para dicho dispositivo.

El PS DEBE soportar todos los objetos MIB de CDP de CableHome, incluidos todos los objetos en cabhCdpLanAddrTable, cabhCdpLanPool, cabhCdpServer, y cabhCdpLanTrans.

El CDS DEBE soportar las opciones de DHCP indicadas como obligatorias en la columna de soporte del protocolo CDS del cuadro 7-3.

El CDS DEBE soportar la oferta de valores por defecto indicados en la columna de valores por defecto de fábrica para el CDS en el cuadro 7-3, si no se ha proporcionado la opción DHCP con otros valores.

Si se ha fijado el modo de manejo de paquetes primario del PS (cabhCapPrimaryMode) a transferencia Y se ha completado el proceso de configuración del PS (indicado por cabhPsDevProvState = pass(1)), en ese caso se DEBE deshabilitar el CDS.

El CDS NO DEBE responder a los mensajes DHCP que se reciben a través de cualquier interfaz WAN, ni originar mensajes DHCP de ninguna interfaz WAN.

El CDS NO DEBE entregar ninguna opción DHCP con un valor nulo a ningún dispositivo IP de LAN.

Cuadro 7-3/J.191 – Opciones DHCP del CDS

Número de la opción	Función de la opción	Soporte del protocolo CDS (M) obligatorio u (O) opcional	Datos por defecto de fábrica del CDS	Nombre del objeto de la MIB
0	Rellenar	M	N/A	N/A
255	Terminar	M	N/A	N/A
1	Máscara de subred	M	255.255.255.0	cabhCdpServerSubnetMask
2	Diferencia horaria	M	0	cabhCdpServerTimeOffset
3	Opción del encaminador	M	192.168.0.1	cabhCdpServerRouter
6	Servidor de nombres de dominio	M	192.168.0.1	cabhCdpServerDnsAddress
7	Servidor de anotaciones históricas	M	0.0.0.0	cabhCdpServerSyslogAddress
12	Nombre del servidor	M	N/A	N/A
15	Nombre de dominio	M	Cadena nula	cabhCdpServerDomainName
23	Tiempo de vida por defecto	M	64	cabhCdpServerTTL
26	MTU de la interfaz	M	N/A	cabhCdpServerInterfaceMTU
43	Información específica del fabricante	M	Seleccionado por el fabricante	cabhCdpServerVendorSpecific
50	Dirección IP solicitada	M	N/A	N/A
51	Tiempo de licencia de la dirección IP	M	3600 segundos	cabhCdpServerLeaseTime
54	Identificador del servidor	M	192.168.0.1	cabhCdpServerDhcpAddress
55	Lista de petición de parámetros	M	N/A	N/A
60	Identificador de la clase de fabricante	M	N/A	N/A

7.2.3.3 Requisitos del CDC

El comportamiento del CDC DEBE ajustarse a los requisitos del cliente especificados en RFC 2131.

El PS DEBE difundir el mensaje DHCP DISCOVER conforme a los requisitos del cliente de RFC 2131 y tratar de conseguir una licencia de dirección IP WAN-Man de PS durante el proceso de rearranque del PS.

El PS DEBE fijar cabhPsDevProvState a inProgress (2) cuando el PS difunde el mensaje DHCP DISCOVER por primera vez después del rearranque del dispositivo o la reactivación del PS.

En el cuadro 13-1 se describe el comportamiento completo de configuración del PS para el modo de configuración DHCP y en el cuadro 13-2 para el modo de configuración SNMP.

El CDC DEBE utilizar la dirección de soporte físico WAN-Man del PS en el campo *chaddr* Y en la opción 61 del DHCP, en los mensajes DHCP DISCOVER y DHCP REQUEST, cuando solicite una dirección IP de la WAN-Man al servidor DHCP de cabecera.

Si el valor de cabhCdpWanDataIpAddrCount es cero, el PS DEBE utilizar la dirección IP de WAN-Man para las interfaces de WAN-Man y WAN-Data.

Si el valor de cabhCdpWanDataIpAddrCount es mayor que cero, el PS DEBE solicitar el mismo número de direcciones IP únicas de WAN-Data del servidor DHCP de cabecera que el valor de cabhCdpWanDataIpAddrCount.

El PS (CDC) NO DEBE tratar de conseguir más direcciones IP de WAN-Data que el valor de cabhCdpWanDataIpAddrCount.

El CDC DEBE utilizar un identificador cabhCdpWanDataAddrClientId único en la opción 61 del DHCP por cada dirección IP de WAN-Data solicitada al servidor DHCP de la cabecera.

El CDC DEBE utilizar la dirección de soporte físico de WAN-Data como el valor del campo *chaddr* del mensaje DHCP por cada dirección IP de WAN-Data solicitada al servidor DHCP de la cabecera.

Cuando el CDC solicita direcciones IP de WAN-Data del servidor DHCP de la cabecera, el CDC DEBE utilizar anotaciones cabhCdpWanDataAddrClientId para la opción 61 de DHCP en el orden en que aparecen las anotaciones en el cuadro cabhCdpWanDataAddrTable, comenzando con la primera anotación.

Si se configura un valor diferente de cero para cabhCdpWanDataIpAddrCount, y si el número de anotaciones cabhCdpWanDataAddrClientId es menor que el valor de cabhCdpWanDataIpAddrCount, el PS DEBE generar tantos ID de cliente de WAN-Data únicos como resulte necesario para llevar el número total de anotaciones cabhCdpWanDataAddrClientId al valor de cabhCdpWanDataIpAddrCount, y añadir cada anotación generada al final de cabhCdpWanDataAddrTable.

Si el PS genera varios ID de cliente de WAN-Data, la primera anotación cabhCdpWanDataAddrClientId de cabhCdpWanDataAddrTable DEBE ser la dirección de soporte físico de WAN-Data.

Si el PS genera varios ID de cliente de WAN-Data, cualquier anotación cabhCdpWanDataAddrClientId generada por el PS que sea distinta de la primera anotación de cabhCdpWanDataAddrTable DEBE ser la dirección de soporte físico de WAN-Data con un valor de contador de 8 bits añadido al final, comenzando con 0x02, a menos que ya exista el valor como una anotación cabhCdpWanDataAddrClientId, en cuyo caso el PS DEBE generar el ID de cliente como la dirección de soporte físico de WAN-Data añadida al siguiente valor del contador de 8 bits disponible.

El PS DEBE implementar la opción de información específica de fabricante (opción 43 de DHCP) que se indica en los cuadros 7-5 y 7-6. Más adelante se describen con mayor amplitud los detalles de la opción 43 de DHCP y de sus subopciones para CableHome 1.0. Las definiciones de las subopciones de la opción 43 de DHCP DEBEN ser conformes a los requisitos propuestos en RFC 2132.

La opción comienza con un octeto de tipo con el valor 43 seguido por un octeto de longitud, el cual a su vez es seguido por el número de octetos de datos igual al valor del octeto de longitud. El valor de este último no incluye los dos octetos que especifican la etiqueta y la longitud.

La opción 43 de DHCP en el sistema CableHome 1.0 es una opción compuesta. El contenido de la opción 43 se compone de una o más subopciones. Las subopciones de la opción 43 de DHCP que soporta CableHome 1.0 son: 1, 2, 3, 4, 5, 6, 11, 12, 13 y 14. Una subopción comienza con un octeto de etiqueta que incluye el código de subopción, seguido de un octeto de longitud que indica el

número total de octetos de datos. El valor del octeto de longitud no se incluye a sí mismo ni al octeto de etiqueta. El octeto de longitud es seguido por octetos de "longitud" de los datos de la subopción.

Más adelante se define la codificación de cada subopción de la opción 43. En los cuadros 7-5 y 7-6 se puede encontrar el objetivo previsto para cada subopción.

El PS DEBE codificar la subopción 1 de la opción 43 de DHCP mediante el número de octetos igual al valor del octeto de longitud de esta subopción, y cada octeto codifica una subopción solicitada.

El PS DEBE codificar cada una de las subopciones 2, 3, 4, 5, 6, 12, 13 y 14 de la opción 43 de DHCP como una cadena de caracteres que consta de caracteres del conjunto de caracteres NVT ASCII, sin emplear la terminación NULO.

Un PS autónomo DEBE enviar la subopción 2 de la opción 43 de DHCP que incluye la cadena de caracteres "SPS" (sin las comillas).

Un PS integrado DEBE enviar la subopción 2 de la opción 43 de DHCP que incluye la cadena de caracteres "EPS" (sin las comillas).

Un PS autónomo DEBE enviar la subopción 3 de la opción 43 de DHCP que incluye la cadena de caracteres "SPS" (sin las comillas).

Un PS integrado DEBE enviar la subopción 3 de la opción 43 de DHCP que incluye una relación de todos los tipos de dispositivos en el dispositivo completo separados por dos puntos, incluyendo como mínimo la cadena de caracteres separada por dos puntos: "ECM:EPS" (sin las comillas).

Si el PS solicita una licencia dirección IP de WAN-Man del PS, DEBE enviar la subopción 11 de la opción 43 de DHCP que contiene el valor 0x01, codificado como un número binario, en sus mensajes DHCP DISCOVER y DHCP REQUEST.

Si el PS solicita una licencia de dirección IP de WAN-Data del PS, DEBE enviar la subopción 11 de la opción 43 de DHCP que contiene el valor 0x02, codificado como un número binario, en sus mensajes DHCP DISCOVER y DHCP REQUEST.

En el cuadro 7-4 se presenta un resumen de cómo debe fijar el PS los valores de la subopción 11 de la opción 43 de DHCP para las interfaces WAN del PS.

El límite de longitud de las subopciones 4, 5, 6, 12, 13 y 14 es de 255 octetos para cada una. Por consiguiente, la longitud total de la opción 43 podría rebasar 255 octetos. Si el número total de octetos en todas las subopciones de la opción 43 de DHCP rebasa 255 octetos, el PS DEBE apegarse a RFC 3396 para dividir la opción en múltiples opciones más pequeñas.

El CDC DEBE implementar la opción de identificador de clase de fabricante (opción 60 de DHCP) como se indica en los cuadros 7-5 y 7-6.

Cuadro 7-4/J.191 – Valores de la subopción 11 de la opción 43 del DHCP

Id del elemento	Descripción y comentarios
PS WAN-Man = 0x01	Identifica la petición de una dirección del sector WAN-Man
PS WAN-Data = 0x02	Identifica la petición de una dirección del sector WAN-Data

En el caso de un PS integrado en el módem de cable, tanto este último como el elemento PS envían peticiones de DHCP independientes. En el cuadro 7-5 se describe cómo DEBE fijar el CDC el contenido de las opciones 60 y 43 del PS cuando el elemento PS está integrado en el módem de cable, y se solicitan direcciones independientes para la gestión de la WAN del PS y para los datos de la WAN del PS.

Cuadro 7-5/J.191 – Opciones del DHCP para las peticiones de direcciones de los sectores WAN-Man y WAN-Data del PS integrado

Opciones de petición del DHCP	Valor	Descripción
Petición de una dirección de gestión de la WAN del DHCP de los servicios de portal integrados		
Opción 60 del CPE	"IPCable2Home"	
Subopción 1 de la opción 43 del CPE	vector de subopción de la petición	Lista de subopciones (de la opción 43) que devolverá el servidor. No hay ninguna definida
Subopción 2 de la opción 43 del CPE	"EPS"	PS integrado
Subopción 3 de la opción 43 del CPE	"ECM:EPS"	Lista de dispositivos integrados (CM/PS integrados)
Subopción 4 de la opción 43 del CPE	por ejemplo,"123456"	Número de serie del dispositivo CM/PS
Subopción 5 de la opción 43 del CPE	por ejemplo "v3.2.1"	Número de versión del soporte físico del CM/PS
Subopción 6 de la opción 43 del CPE	por ejemplo "v1.0.2"	Número de versión del soporte lógico del CM/PS
Subopción 11 de la opción 43 del CPE	WAN-Man del PS (0x01)	Determina que se está solicitando una dirección en el sector de gestión de la WAN del PS
Subopción 12 de la opción 43 del CPE	por ejemplo, "ABC Inc. CM-PS123…"	Descripción del sistema CM/PS desde sysDescr
Subopción 13 de la opción 43 del CPE	"CM-PS123-1.0.2…"	Revisión de los microprogramas del CM/PS desde docsDevSwCurrentVers
Subopción 14 de la opción 43 del CPE	por ejemplo, "1.2.3…"	Versión del fichero de política de la barrera contra fuegos desde cabhSecFwPolicyFileCurrentVersion
Petición de una dirección de WAN-Data del DHCP de los servicios de portal integrados		
Opción 60 del CPE	"IPCable2Home"	
Subopción 1 de la opción 43 del CPE	vector de subopción de la petición	Lista de subopciones (de la opción 43) que devolverá el servidor. No hay ninguna definida
Subopción 2 de la opción 43 del CPE	"EPS"	PS integrado
Subopción 3 de la opción 43 del CPE	"ECM:EPS"	Lista de los dispositivos integrados (CM y PS integrados)
Subopción 4 de la opción 43 del CPE	Por ejemplo "123456"	Número de serie del dispositivo CM/PS
Subopción 11 de la opción 43 del CPE	WAN-Data del PS (0x02)	Determina que se está solicitando una dirección en el sector de WAN-Data del PS

En el cuadro 7-6 se describe qué valores DEBE utilizar el CDC para fijar el contenido de las opciones 60 y 43, cuando el PS es un dispositivo autónomo.

Cuadro 7-6/J.191 – Opciones del DHCP para las peticiones de direcciones de los sectores WAN-Man y WAN-Data del PS autónomo

Opciones de petición del DHCP	Valor	Descripción
Petición de una dirección de gestión de la WAN del DHCP de servicios de portal autónomos		
Opción 60 del CPE	"IPCable2Home"	
Subopción 1 de la opción 43 del CPE	vector de subopción de la petición	Lista de subopciones (de la opción 43) que devolverá el servidor. No hay ninguna definida
Subopción 2 de la opción 43 del CPE	"SPS"	PS autónomo
Subopción 3 de la opción 43 del CPE	"SPS"	Lista de dispositivos integrados (sólo el PS autónomo)
Subopción 4 de la opción 43 del CPE	por ejemplo, "123456"	Número de serie del dispositivo PS
Subopción 5 de la opción 43 del CPE	por ejemplo, "v3.2.1"	Número de versión de soporte físico del PS
Subopción 6 de la opción 43 del CPE	por ejemplo, "v1.0.2"	Número de versión del soporte lógico del PS
Subopción 11 de la opción 43 del CPE	WAN-Man del PPS (0x01)	Determina que se está solicitando una dirección en el sector de gestión de la WAN del PS
Subopción 12 de la opción 43 del CPE	por ejemplo, "ABC Inc. PS123 …"	Descripción del sistema del PS a partir de sysDescr
Subopción 13 de la opción 43 del CPE	por ejemplo, "PS123-1.0.2 …"	Revisión de los microprogramas del PS desde docsDevSwCurrentVers
Subopción 14 de la opción 43 del CPE	por ejemplo, "1.2.3 …"	Versión del fichero de política de la barrera contra fuegos desde cabhSecFwPolicyFileCurrentVersion
Petición DHCP de dirección de WAN-Data procedente del DHCP de servicios de portal autónomos		
Opción 60 del CPE	"IPCable2Home"	
Subopción 1 de la opción 43 del CPE	vector de subopción de la petición	Lista de subopciones (de la opción 43) que devolverá el servidor. No hay ninguna definida.
Subopción 2 de la opción 43 del CPE	"SPS"	PS autónomo
Subopción 3 de la opción 43 del CPE	"SPS"	Lista de dispositivos integrados (sólo para el PS autónomo)
Subopción 4 de la opción 43 del CPE	por ejemplo, "123456"	Número de serie del dispositivo del PS
Subopción 11 de la opción 43 del CPE	WAN-Data del PS (0x02)	Determina que se está solicitando una dirección en el sector WAN-Data del PS

Véase la cláusula 6.3.4 para obtener una descripción detallada del contenido del objeto sysDescr del PS.

El PS DEBE soportar las opciones DHCP indicadas como obligatorias en la columna de soporte del protocolo CDC del cuadro 7-7. En el cuadro 7-7 se relacionan las opciones obligatorias y facultativas del DHCP que debe soportar el CDC.

Cuadro 7-7/J.191 – Opciones DHCP del CDC

Número de la opción	Función de la opción	Obligatoriedad (M) de soporte del protocolo del CDC
0	Relleno	M
255	Final	M
1	Máscara de la subred	M
2	Opción de desplazamiento de tiempo	M
3	Opción del encaminador	M
4	Opción del servidor de tiempos	M
6	Servidor de nombres de dominio	M
7	Servidor de anotaciones históricas (syslog)	M
12	Nombre del anfitrión	M
15	Nombre del dominio	M
23	Tiempo de vida por defecto	M
26	MTU de la interfaz	M
43	Información específica del fabricante	M
50	Dirección IP solicitada	M
51	Tiempo de licencia de la dirección IP	M
54	Identificador del servidor	M
55	Lista de petición de parámetros	M
60	Identificador de la clase de fabricante	M
61	Identificador del cliente	M
177	Dirección de la entidad SNMP del proveedor de servicios – subopción 3	M
177	Nombre del sector Kerberos del sector de configuración – subopción 6	M
177	Dirección IP del servidor Kerberos – subopción 51	M

El PS DEBE soportar una dirección de entidad SNMP del proveedor de servicio (subopción 3 de la opción 177 del DHCP) configurada como una dirección IPv4. Más adelante se describe el formato de la subopción 3 de la opción 177 del DHCP:

La longitud de la subopción 3 de la opción 177 del DHCP DEBE ser 5 octetos. A continuación del octeto de longitud de la subopción 3 de la opción 177 del DHCP DEBE venir un solo octeto que indica el tipo de dirección específica que sigue. El valor del octeto 'address type' de la subopción 3 de la opción 177 del DHCP DEBE fijarse a 1 que indica una dirección IPv4 y a continuación de ese octeto DEBEN venir 4 octetos de la dirección IPv4.

El PS IGNORARÁ la subopción 3 de la opción 177 del DHCP si su formato o contenido no es conforme con los requisitos de esta subopción.

Código	Longitud	Tipo	Dirección			
3	5	1	a1	a2	a3	a4

El PS DEBE soportar un nombre de sector Kerberos (subopción 6 de la opción 177 del DHCP). El PS necesita un nombre de sector Kerberos para facilitar que el DNS examine la dirección de la

entidad del centro de distribución de claves (KDC) del proveedor de servicios. A continuación se describe el formato de la subopción 6 de la opción 177 del DHCP:

El nombre del sector Kerberos suministrado al PS en la subopción 6 de la opción 177 del DHCP DEBE codificarse conforme al nombre de sector de estilo de dominio que se describe en [RFC 1510]. El nombre del sector Kerberos proporcionado al PS en la subopción 6 de la opción 177 del DHCP DEBE tener únicamente mayúsculas y ser conforme a la sintaxis que se describe en la sección 3.1 de [RFC 1035]. La subopción se codifica de la siguiente manera:

Código	**Longitud**	**Nombre del sector Kerberos**			
6	n	k1	k2	…	kn

El PS DEBE ignorar la subopción 6 de la opción 177 del DHCP si su formato o contenido no cumple con los requisitos de esta subopción.

El PS DEBE soportar una dirección IP del servidor Kerberos (subopción 51 de la opción 177 del DHCP). La subopción de dirección IP del servidor Kerberos indica al PS la dirección de red de uno o varios servidores del centro de distribución de claves.

La codificación de la subopción de dirección del servidor KDC debe apegarse al formato de una dirección IPv4 utilizando el puerto por defecto. La longitud mínima de la subopción 51 de la opción 177 del DHCP es de 4 octetos, y la longitud DEBE ser siempre un múltiplo de 4. Si en esta última subopción 51 se relacionan múltiples servidores KDC esto DEBERÁ efectuarse en orden de prioridad decreciente. La subopción de dirección de servidor KDC se codifica de la siguiente manera:

Código	**Longitud**	**Dirección 1**				**Dirección 2**		
51	N	a1	a2	a3	a4	a1	a2	…

El PS DEBE tratar de intercambiar claves con los KDC en el orden relacionado en la subopción 51 de la opción 177 del DHCP, hasta que el intercambio de claves con uno de los KDC sea satisfactorio o se agote la lista en cuyo caso fracasa el intercambio. Véase 11.3.1 por lo que se refiere a los requisitos de intercambio de claves del PS. El PS DEBE ignorar la subopción 51 de la opción 177 del DHCP si su formato o contenido no cumple con los requisitos de esta subopción.

El PS DEBE incluir las opciones de DHCP relacionadas como obligatorias en el cuadro 7-8 en los mensajes DHCP DISCOVER y DHCP REQUEST que envía al servidor DHCP de la red de cable.

Cuadro 7-8/J.191 – Opciones DHCP del CDC en los mensajes DISCOVER y REQUEST

Número de opción	**Función de la opción**	**Obligatoriedad (M) de la inclusión del protocolo CDC**
255	Final	M
43	Información específica de fabricante	M
50	Dirección IP solicitada	M
55	Lista de petición de parámetros	M
60	Identificador de clase de fabricante	M
61	Indentificador de cliente	M

El PS DEBE solicitar las opciones DHCP relacionadas como obligatorias en el cuadro 7-9, dentro de la opción 55 del DHCP (Lista de petición de parámetros) [RFC 2132] enviada en los mensajes DHCP DISCOVER y DHCP REQUEST.

Cuadro 7-9/J.191 – Opciones DHCP del CDC solicitadas con la opción 55

Número de opción	Función de la opción	Obligatoriedad (M) de la inclusión del protocolo CDC
1	Máscara de subred	M
2	Opción de diferencia horaria	M
3	Opción de encaminador	M
4	Opción de servidor de tiempo	M
6	Servidor de nombres de dominio	M
7	Servidor de anotaciones históricas (syslog)	M
15	Nombre de dominio	M
23	Tiempo de vida por defecto	M
26	MTU de la interfaz	M
51	Tiempo de licencia de la dirección IP	M
54	Identificador de servidor	M
177	Opción de configuración de cliente compatible con PacketCable	M

Cuando la primera interfaz WAN-Data del PS no tenga una licencia DHCP actual, esa interfaz DEBE utilizar por defecto los siguientes parámetros IP:

Dirección IP de WAN-Data en modo de "repliegue": 192.168.100.5

Máscara de red: 255.255.255.0

Pasarela por defecto: 192.168.100.1

La finalidad de la dirección IP de WAN-Data en "repliegue" es facilitar el acceso a la dirección IP de diagnóstico del módem de cable (192.168.100.1) desde un dispositivo IP LAN. Esa dirección en modo de "repliegue" se DEBE utilizar únicamente como la parte de la dirección IP de la WAN que corresponde a la tupla NAT o NAPT dinámica de una correspondencia de dirección C-NAT y C-NAPT, respectivamente. SI el PS funciona en el modo 2 de dirección de la WAN y es necesario que trate de conseguir múltiples licencias de dirección IP de WAN-Data Y el PS no puede obtenerlas después de la emisión de tres mensajes DHCP DISCOVER (conforme con los procedimientos de reintento de DHCP de 7.2.3.3, el PS DEBE utilizar la dirección IP de WAN-Data en modo de "repliegue" como la parte WAN de cada tupla NAT dinámica, hasta que el PS consiga la licencia o licencias de dirección IP de WAN-Data necesarias que provienen de un servidor DHCP a través de una interfaz WAN del PS.

La dirección IP de WAN-Data en modo "repliegue" NO DEBE utilizarse cuando el PS esté configurado para funcionar en el modo de manejo de paquetes primario de transferencia.

El PS NO DEBE utilizar la dirección IP de WAN-Data en modo "repliegue" para ninguna correspondencia C-NAT o C-NAPT cuando el PS tenga una licencia de dirección IP de WAN-Man y de WAN-Data del PS. Si un servidor DHCP en la interfaz WAN del PS ofrece al PS (CDC) una licencia para la dirección IP 192.168.100.5, es decir, la misma dirección de la dirección IP de WAN-Data en modo "repliegue", el PS (CDC) PODRÁ aceptarla y utilizarla como la dirección IP de WAN-Data para una correspondencia C-NAT o C-NAPT.

Aun cuando esté utilizando la dirección IP de WAN-Data por defecto 192.168.100.5, el CDC DEBE continuar ejecutando un DHCP DISCOVER cada 10 segundos hasta que se otorgue una licencia DHCP válida a esa interfaz WAN-Data del PS (o a la interfaz WAN- Man, si las WAN-Man y WAN-data comparten una dirección IP).

Cuando un PS está tratando de conseguir una dirección IP de WAN-gestión para su interfaz WAN-Man, el CDC DEBE introducir siempre su dirección de soporte físico WAN en el campo del ID de cliente (opción 61 del DHCP) en el mensaje de terminación DHCP.

Si mientras trata de conseguir una licencia para la dirección IP de WAN-Man del PS el CDC no recibe DHCP OFFER, el PS DEBE registrar el ID de evento 68000100 en el registro histórico local y redifundirá un mensaje DHCP DISCOVER (es decir, rearranca la secuencia de configuración en el caso de esta condición de fallo) repitiendo el intento de obtención de la licencia DHCP hasta cinco veces. Si después del quinto intento para obtener dicha licencia el CDC no recibe DHCP OFFER, el PS DEBE utilizar la dirección IP WAN en modo de "repliegue", la máscara de red y la pasarela por defecto como se describió anteriormente Y continuará intentando conseguir la licencia al difundir DHCP DISCOVER por su interfaz WAN cada 10 segundos hasta que se otorgue la licencia DHCP válida para la dirección IP de WAN-Man.

Si durante este proceso el CDC recibe una dirección IP válida en el campo 'siaddr', Y un nombre de fichero válido en el campo 'file', Y no recibe la subopción 3, la subopción 6, O la subopción 51 (combinación 1 válida) de la opción 177 del DHCP, en el mensaje DHCP ACK [RFC 2131] provenientes del servidor DHCP en la red de cable, el PS DEBE fijar cabhPsDevProvMode a '1' (modo DHCP) y tratará de sincronizar la hora del día con el servidor ToD conforme a 7.4.3.

Si durante el proceso de obtención de una licencia de dirección IP de WAN-Man del PS el CDC recibe un mensaje DHCP ACK del servidor DHCP en la red de cable que incluye la opción 177 del DHCP con una dirección IP válida (dirección de la entidad SNMP) en la subopción 3, un nombre válido de sector Kerberos en la subopción 6, Y una dirección IP válida (dirección IP del servidor Kerberos) en la subopción 51, Y no recibe una dirección IP válida en el campo 'siaddr', Y no recibe un nombre de fichero válido en el campo 'file' (combinación 2 válida), el PS DEBE fijar cabhPsDevProvMode a '2' (modo SNMP) e iniciar el funcionamiento del CDS e intentar sincronizar la hora del día con el servidor ToD y ejecutar la autenticación con el servidor KDC conforme a la cláusula 11.

Si durante el proceso de conseguir una licencia de dirección IP de WAN-Man del PS el CDC recibe cualquier combinación de las subopciones 3, 6 y 51 de la opción 177 del DHCP, el campo 'siaddr' y el campo 'file' distinto de las dos combinaciones válidas que se describieron anteriormente, en el mensaje DHCP ACK proveniente del servidor DHCP en la red de cable, el PS habrá recibido una configuración DHCP no válida y DEBERÁ registrar el evento apropiado y redifundir un mensaje DHCP DISCOVER (es decir, rearrancar la secuencia de configuración en el caso de esta condición no válida) repitiendo todo el proceso de adquisición de la licencia DHCP hasta 5 veces.

Si tras el quinto intento para conseguir una licencia de una dirección IP de WAN-Man del PS el CDC recibe cualquier combinación de las subopciones 3, 6 y 51 de la opción 177 del DHCP, el campo 'siaddr' y el campo 'file' distinto de las dos combinaciones válidas anteriormente descritas, en el mensaje DHCP ACK proveniente del servidor DHCP en la red de cable, el PS DEBERÁ efectuar lo siguiente suponiendo que está conectado a través de un módem de cable a una red de datos por cable que no soporta la configuración de CableHome (modo CableHome aletargado):

- Desactivar el agente SNMP (CMP) para el acceso a la interfaz WAN. Permitir que el agente SNMP continúe habilitado para los mensajes que se reciben a través de la interfaz LAN (es decir, mensajes SNMP direccionados a la dirección del encaminador del servidor del PS).
- Inhabilitar el cliente TFTP.
- Inhabilitar el informe de eventos SYSLOG.

- Aceptar la licencia de dirección IP ofrecida (CPE) y utilizarla como la dirección WAN-Data del PS en el cuadro de correspondencia CAP, incluida la asignación de la dirección a cabhCdpWanDataAddrIp e introduciendo las otras anotaciones del cuadro de dirección WAN-Data del CDP (cabhCdpWanDataAddrTable). El PS funcionará sin una dirección IP de WAN-Man, que es una situación distinta de cualquiera de los modos de dirección WAN descritos en 7.2.2.2.2.
- Interrumpir el temporizador de configuración.
- Fijar el valor de cabhPsDevProvMode a dormantCHmode(3).
- Fijar el valor de cabhPsDevProvState a fail(3).
- Habilitar el CDS.
- Habilitar la funcionalidad de CAP y de USFS.
- Habilitar el CNP.
- Habilitar la barrera contra fuegos.
- Funcionar con parámetros que hayan sido suministrados anteriormente, incluidos los de valores de objetos MIB persistentes. El PS que funciona en el modo CableHome aletargado NO DEBE reactivar sus objetos MIB a los valores por defecto de fábrica.

Cuando un PS que funciona en el modo 2 de dirección WAN (descrito en 7.2.2.2) está tratando de conseguir una dirección IP de WAN-Data para una interfaz WAN-Data que utilizará una dirección IP distinta de la interfaz WAN-Man, el CDC DEBE incluir la opción de identificador de cliente (cabhCdpWanDataAddrClientId) en el mensaje de determinación del DHCP. Para habilitar estos ID de cliente de la WAN-Data únicos, el CDC DEBE habilitar el sistema NMS para producir anotaciones cabhCdpWanDataAddrClientId en el cuadro cabhCdpWanDataAddrTable.

Si un PS funciona en el modo 2 de dirección WAN (descrito en 7.2.2.2) el CDC DEBE tratar de obtener una dirección IP, a través del DHCP, para cada ID de cliente único (cabhCdpWanDataAddrClientId) del cuadro cabhCdpWanDataAddrTable, hasta el límite definido por cabhCdpWanDataIpAddrCount.

El CDC DEBE continuar retransmitiendo la difusión del mensaje DHCP DISCOVER y aplicando un algoritmo de reducción exponencial aleatorizada congruente con el descrito en RFC 2131. El CDC DEBE transmitir hasta cinco mensajes DHCP DISCOVER (uno inicial y cuatro intentos de retransmisión) antes de reconfigurar el valor del temporizador de reducción a CERO y de repetir el proceso.

Si el CDC tiene éxito para adquirir la dirección IP de WAN-Man (es decir, recibe un mensaje DHCP ACK de un servidor DHCP a través de la interfaz WAN-Man del PS) en el primer intento, Y si el PS está funcionando en el modo de configuración DHCP, DEBE intentar la sincronización de la hora del día con el servidor ToD al emitir una petición ToD conforme con 7.4.3, antes de intentar la descarga del fichero de configuración del PS.

Si el CDC no tiene éxito para conseguir la dirección IP de WAN-Man (es decir, el DHCP solicita fin de temporización conforme a RFC 2131) en el primer intento, el PS DEBE activar el CDS (es decir, iniciará el funcionamiento del CDS), de modo que este último pueda atender las peticiones DHCP de los dispositivos IP de LAN en el sector LAN-Trans.

El CDC DEBE responder únicamente a mensajes DHCP que se reciban a través de una interfaz WAN, o se envíen a través de la misma interfaz.

Cuando deje de ser válida la licencia de DHCP de WAN-MAN, el CDC DEBE despejar todas las anotaciones de la fila del cuadro cabhCdpWanDNSServerTable.

Hasta que la MIB cabhPsDevProvState tenga un valor de 'pass' (1) indicando que se completó el proceso de configuración, el PS DEBE bloquear el tráfico entrante en la interfaz WAN que no sea en respuesta a una petición LAN-WAN del mismo elemento PS o de un dispositivo IP de LAN.

Esto permitirá proteger contra posibles ataques de piratas informáticos durante el proceso de configuración cuando se inhabilita la barrera contra fuegos del PS.

7.3 Arquitectura de configuración de los servicios de portal en bloque

7.3.1 Directrices de diseño del sistema de configuración de los servicios de portal en bloque

Las siguientes directrices de diseño del sistema permiten obtener las capacidades definidas para la herramienta de configuración del PS en bloque:

Cuadro 7-10/J.191 – Directrices de diseño del sistema de los servicios de portal en bloque

Número	Directrices de diseño del sistema de configuración del PS en bloque (BPSC)
BPSC 1	Es necesario proporcionar un mecanismo que permita al PS descargar y procesar los ficheros de configuración

7.3.2 Descripción del sistema de configuración de los servicios de portal en bloque

La configuración de los servicios de portal en bloque se suele llevar a cabo durante la configuración del elemento PS, mediante el proceso de los valores de configuración contenidos en un fichero de configuración. No obstante, este proceso puede iniciarse en cualquier momento. La herramienta de configuración del PS en bloque consta de los siguientes elementos:

1) Formato del fichero de configuración.
2) Modos de desencadenar el proceso de la descarga.
3) Medios de autenticación del fichero.
4) Medios de comunicar la situación de la descarga del fichero de configuración del PS y otras consideraciones.

La configuración del PS en bloque (BPSC) es una herramienta que pueden utilizar los operadores para modificar los valores de configuración del PS en bloque, mediante un fichero de configuración. Lo normal es que el fichero de configuración contenga muchos valores, ya que la principal utilidad de los ficheros de configuración es la de modificar los valores de configuración con el mínimo de intervención por parte del operador de cable.

El proceso de configuración del PS en bloque puede comportarse igual que una serie de SNMP sucesivos ejecutados por un operador manualmente. El fichero de configuración es una herramienta destinada a mejorar la productividad de los operadores y a que las modificaciones de importancia sean menos proclives a errores.

Es importante observar que un PS que funciona en modo de configuración SNMP no necesita la carga de un fichero de configuración de PS antes de su funcionamiento. Se prevé que un PS que funciona en modo de configuración SNMP se inicializará por sí mismo para alcanzar un estado conocido pudiendo funcionar indefinidamente sin necesidad de cargar un fichero de configuración de PS. No obstante, un PS aceptará un fichero de configuración del PS cuando se le suministre.

La descarga del fichero de configuración de la barrera contra fuegos utiliza un procedimiento análogo a la descarga de parámetros de configuración del PS en bloque. Consúltese la cláusula 11.3.5.2 que contiene una descripción del procedimiento de descarga del fichero de configuración de la barrera contra fuegos.

7.3.3 Requisitos de configuración de los servicios de portal en bloque

Un PS que funciona en el modo de configuración DHCP DEBE descargar y procesar un fichero de configuración de PS.

Un PS que funciona en el modo de configuración SNMP DEBE tener la capacidad de funcionar sin un fichero de configuración de PS, pero debe poder descargar y procesar dicho fichero si se activa conforme a 7.3.3.2

Las fijaciones de los objetos MIB transferidas en el fichero de configuración del PS tendrán prioridad sobre las fijaciones de objetos MIB existentes, y las DEBEN reemplazar.

7.3.3.1 Requisitos de formato del fichero de configuración

Los datos de configuración del PS DEBEN estar contenidos en un fichero, que se descarga mediante TFTP. El fichero de configuración del PS DEBE constar de un número de valores de configuración (1 por parámetro), con el formato "tipo-longitud-valor (TLV)". El cuadro 7-11 proporciona las definiciones de estos términos.

Cuadro 7-11/J.191 – Definiciones TLV

Tipo	Identificador de un único octeto que define el parámetro
Longitud	Un octeto o varios que especifican la longitud del campo valor (sin incluir los campos tipo y longitud)
Valor	Una serie de octetos de la mencionada longitud que contienen el valor específico del parámetro

Los valores de configuración DEBEN disponerse correlativamente en el fichero, que consiste en una serie de octetos (sin marcas de registro). El PS DEBE tener la capacidad para recibir y procesar adecuadamente un fichero de configuración que se haya completado a un número entero de palabras de 32 bits, Y poder recibir y procesar otro fichero que no se haya completado. Véase 7.3.3.1.1 que contiene una definición del relleno. Los valores de configuración se dividen en tres tipos:

- Valores de configuración normales cuya presencia es necesaria.
- Valores de configuración adicionales u opcionales especificados para IPCable2Home que pueden estar presentes.
- Valores de configuración específicos del fabricante.

El fichero de configuración del PS PUEDE contener muchos parámetros diferentes, pero el único parámetro que DEBE incluirse en todos los ficheros de configuración de los servicios de portal es la marca de fin de datos (Tipo 255) y verificación de integridad de mensaje (MIC, *message integrity check*) de PS (tipo 53).

Para mayor uniformidad de la gestión de los dispositivos conformes con esta Recomendación, los dispositivos homologados DEBEN soportar un fichero de configuración de 64K bytes de longitud como máximo.

Un elemento de servicios de portal DEBE soportar, y el fichero de configuración del PS PUEDE incluir, los tipos de parámetro de configuración 0, 9, 10, 21, 28, 32, 33, 34, 38, 43, 53 y 255, descritos en esta cláusula.

El tamaño del valor del campo longitud para cualquier parámetro de configuración incluido en un fichero de configuración de los servicios de portal DEBE ser de 2 octetos.

El valor de la longitud para cada tipo descrito en 7.3.3.1.1, 7.3.3.1.2, 7.3.3.1.3, 7.3.3.1.4, 7.3.3.1.5, 7.3.3.1.6, 7.3.3.1.7 y 7.3.3.1.8 es la longitud real en octetos del campo valor.

7.3.3.1.1 Valor de configuración del relleno

Este valor no tiene campos de longitud ni valor y se utiliza exclusivamente tras la marca de fin de datos para rellenar el fichero a un número entero de palabras de 32 bits.

Tipo	Longitud	Valor
0	–	–

7.3.3.1.2 Nombre del fichero de actualización del soporte lógico

Se trata del nombre del fichero de actualización del soporte lógico del dispositivo IPCable2Home. Este nombre se especifica con la calificación completa del directorio. Se prevé que el fichero resida en un servidor TFTP identificado en una de las opciones de los valores de configuración.

Tipo	Longitud	Valor
9	Variable	nombre del fichero

7.3.3.1.3 Control de escritura y acceso SNMP

Este objeto permite desactivar el acceso del SNMP "Set" a objetos individuales de la MIB. Cada ejemplar de este objeto controla el acceso a todos los objetos de la MIB grabables cuyos prefijos Object Identifier (OID) concuerdan. Este objeto puede repetirse para desactivar el acceso al número de objetos MIB que se desee.

Tipo	Longitud	Valor
10	n	Prefijo OID más bandera de control

Siendo n el tamaño de la codificación del prefijo OID, de acuerdo con las reglas de codificación básicas ASN.1 [Rec. UIT-T X.690 | ISO/CEI 8825-1], más un byte para la bandera de control.

La bandera de control puede tener los valores:

– 0 – permitir el acceso de escritura;

– 1 – impedir el acceso de escritura.

Puede utilizarse cualquier prefijo OID. El OID nulo 0.0 puede utilizarse para controlar el acceso a todos los objetos MIB. (El OID 1.3.6.1 tendrá el mismo efecto.)

Cuando se presenten varios ejemplares de este objeto y se solapen, el prefijo de mayor longitud (el más específico) tiene prioridad.

Por consiguiente, un ejemplo podría ser

– someTable impide el acceso de escritura;

– someTable.1.3 permite el acceso de escritura.

En este ejemplo se impide el acceso a todos los objetos de someTable excepto para someTable.1.3.

7.3.3.1.4 Servidor TFTP de actualización del soporte lógico

Dirección IP del servidor TFTP en el que reside el fichero de actualización del soporte lógico para el dispositivo IPCable2Home.

Tipo	Longitud	Valor
21	4	ip1, ip2, ip3, ip4

7.3.3.1.5 Objeto SNMP MIB con longitud ampliada

Este objeto permite el establecimiento de objetos SNMP MIB arbitrarios a través del proceso de registro TFTP, siendo el valor una vinculación variable SNMP (VarBind) definida en RFC 1157. La VarBind se codifica con las reglas de codificación básicas ASN.1, como si formase parte de la petición SNMP Set.

Tipo	Longitud	Valor
28	Variable	vinculación variable

El PS DEBE tratar la vinculación variable, en un TLV de tipo 28, como si formase parte de la petición SNMP SET con las siguientes advertencias:

- DEBE tratar las peticiones como plenamente autorizadas (no puede rechazar la petición por falta de privilegios).
- No son aplicables las disposiciones de control de escritura SNMP (véase la cláusula anterior).
- El PS no genera ninguna respuesta SNMP.
- Este objeto PUEDE repetirse con distintas VarBind para establecer ("Set") objetos de la MIB. Todos los SNMP Set del fichero de configuración DEBEN tratarse como si fueran simultáneos. Las VarBind DEBEN limitarse a 65535 bytes.

7.3.3.1.6 Certificado de verificación de código del fabricante

Se trata del certificado de verificación del código del fabricante (M-CVC, *manufacturer's code verification certificate*) correspondiente a la descarga segura de programas. Véase 11.3.7.5.2.

Tipo	Longitud	Valor
32	Variable	CVC del fabricante (codificado en DER ASN.1)

7.3.3.1.7 Certificado de verificación de código del cofirmante

Se trata del certificado de verificación del código del cofirmante (C-CVC, c*o-signer's code verification certificate*) correspondiente a la descarga segura de soporte lógico. Véase 11.3.7.5.2.

Tipo	Longitud	Valor
33	Variable	CVC cofirmante (codificado en DER ASN.1)

7.3.3.1.8 Valor de arranque del SNMPv3

(Véase B.C.1.2.8 del anexo B/J.112.)

Los elementos de los servicios de portal conformes DEBEN entender el siguiente TLV y sus subelementos y ser capaces de arrancar el acceso SNMPv3 para el PS con independencia del funcionamiento del PS en el modo NmAccess o en el de coexistencia (véanse 6.3.3 y 6.3.6).

Tipo	Longitud	Valor
34	n	Compuesto

En el fichero de configuración se puede incluir un máximo de cinco de tales objetos. Cada uno de ellos genera una fila adicional en usmDHKickstartTable y en usmUserTable y provoca la generación de un número público agente para dichas filas.

7.3.3.1.8.1 Nombre de seguridad de arranque del SNMPv3

Tipo	Longitud	Valor
34.1	2-16	nombre de seguridad codificado en UTF8

Para el conjunto de caracteres ASCII, la codificación UTF8 y la ASCII son idénticas. Normalmente se especificará como uno de los usuarios USM incorporados en DOCSIS, por ejemplo, "docsisManager", "docsisOperator", "docsisMonitor", "docsisUser".

El nombre de seguridad NO termina en cero. Esto se indica en usmDHKickStartTable como usmDHKickStartSecurityName y en usmUserTable como usmUserName y usmUserSecurityName.

7.3.3.1.8.2 Número público de gestión de arranque del SNMPv3

Tipo	Longitud	Valor
34.2	n	Número público Diffie-Hellman del gestor expresado como cadena de octetos

Éste es el número público Diffie-Hellman derivado de un número aleatorio generado privadamente (por el gestor o por el operador) y transformado conforme a RFC 2786. En usmDHKickStartTable figura como usmKickstartMgrPublic. Cuando se combina con el objeto consignado en la misma fila que usmKickstartMyPublic puede utilizarse para obtener las claves en la fila relacionada de usmUserTable.

7.3.3.1.9 Elemento docsisV3NotificationReceiver del fichero de configuración

Tipo	Longitud	Valor
38	n	Compuesto

Este elemento del fichero de configuración del PS especifica la estación de gestión de la red que recibirá las notificaciones del PS cuando éste se encuentre en el modo de gestión de red de coexistencia. Este TLV (38) consta de varios subTLV en el elemento del fichero de configuración del TLV. El fichero de configuración del PS puede incluir un máximo de 10 de dichos elementos. En la cláusula 6.3.6.4 se presentan los detalles sobre cómo se efectúa la correspondencia de este elemento de fichero de configuración con los cuadros funcionales del SNMPv3.

NOTA – Todos los campos multi-byte de un Sub-TLV deben colocarse en el orden de los bytes de la red.

7.3.3.1.9.1 Sub-TLV 38.1 – Dirección IP del receptor de trampas

Dirección IP del receptor de trampas, en binario.

Tipo	Longitud	Valor
38.1	4	Dirección IP

7.3.3.1.9.2 Sub-TLV 38.2 – Número de puerto UDP del receptor de trampas

Número de puerto UDP del receptor de trampas, en binario.

Tipo	Longitud	Valor
38.2	2	Puerto UDP

(Si no existe se utiliza el valor 162 por defecto.)

7.3.3.1.9.3 Sub-TLV 38.3 – Tipo de trampa que envía el PS

Tipo de trampa

Tipo	Longitud	Valor
38.3	2	Tipo de trampa

Se DEBEN reconocer los siguientes valores de tipo de trampa:

– 1 = Trampa SNMP v1 en un paquete SNMP v1;
– 2 = Trampa SNMP v2c en un paquete SNMP v2c;
– 3 = Informativo SNMP en un paquete SNMP v2c;
– 4 = Trampa SNMP v2c en un paquete SNMP v3;
– 5 = Informativo SNMP en un paquete SNMP v3.

7.3.3.1.9.4 Sub-TLV 38.4 – Límite temporal

Límite temporal, en milisegundos, para el envío de mensajes informativos SNMO.

Tipo	Longitud	Valor
38.4	2	0-65535

7.3.3.1.9.5 Sub-TLV 38.5 – Número de reintentos para el envío de un informativo, después de la transmisión del informativo por primera vez

Tipo	Longitud	Valor
38.5	2	0-65535

7.3.3.1.9.6 Sub-TLV 38.6 – Parámetros de filtrado de la notificación

Tipo	Longitud	Valor
38.6	n	OID de filtro

Siendo n el tamaño del identificador de objeto filtro codificado en ASN.1.

Si no está presente este Sub-TLV, el receptor de notificación aceptará todas las notificaciones generadas por el agente SNMP.

OID de filtro: Identificador de objeto con formato ASN.1 del valor snmpTrapOID que identifica las notificaciones que han de enviarse al receptor de notificaciones. Se enviará esta notificación y todas las que estén por debajo de ella.

7.3.3.1.9.7 Sub-TLV 38.7 – Nombre de seguridad que ha de utilizarse para el envío de la notificación SNMP V3

Tipo	Longitud	Valor
38.7	2-16	Nombre de seguridad codificado en UTF8

El tipo de trampa = 1, 2 ó 3 antes mencionado no tiene necesidad de este Sub-TLV (si se presenta, deberá ignorarse). Si no se proporciona para un tipo de trampa 4 ó 5, se enviará la notificación v3 en el nivel de seguridad noAuthNoPriv empleando el nombre de seguridad "@PSconfig" (nota 2).

Nombre de seguridad:

– Nombre de seguridad v3 a utilizar cuando se envía una notificación v3. Sólo deberá utilizarse si el tipo de trampa tiene el valor 4 ó 5. Este nombre DEBE ser uno de los especificados en un TLV tipo 34 del fichero Config como parte del procedimiento de arranque (Kickstart) DH. Las notificaciones DEBEN enviarse utilizando las claves de autenticación y privacidad calculadas por el PS durante el procedimiento de arranque DH.

NOTA 1 – Al recibir uno de estos elementos TLV, el PS DEBE efectuar anotaciones en los siguientes cuadros a fin de provocar la transmisión de trampas deseada: snmpNotifyTable, snmpTargetAddrTable, snmpTargetParamsTable, snmpNotifyFilterProfileTable, snmpNotifyFilterTable, snmpCommunityTable, usmUserTable, vacmSecurityToGroupTable, vacmAccessTable y vacmViewTreeFamilyTable.

NOTA 2 – Tipo de trampa: La cadena de comunidad para las trampas de los paquetes SNMP v1 y v2 DEBE ser "public". El nombre de seguridad en las trampas y los informativos de los paquetes SNMP v3 en los que no se haya especificado nombre de seguridad DEBE ser "@PSconfig" y en este caso el nivel de seguridad DEBE ser NoAuthNoPriv.

NOTA 3 – OID de filtro: El SNMP v3 permite especificar qué OID de trampas han de enviarse a un receptor de trampas. El OID de filtro del elemento de configuración especifica el OID de la raíz de un subárbol de filtro de trampa. Todas las trampas con un OID de trampa contenidas en ese subárbol de filtro de trampas DEBEN enviarse al receptor de trampas.

NOTA 4 – El fichero de configuración del PS PUEDE incluir también elementos TLV MIB que efectúan anotaciones en cualquiera de los 10 cuadros enumerados en la nota 1. Estos elementos TLV MIB NO DEBEN utilizar columnas de índice que comiencen con los caracteres "@PSconfig".

NOTA 5 – Este elemento TLV DEBE procesarse sólo si el PS ha adoptado el modo de coexistencia SNMP v3 durante el proceso del fichero de configuración del PS.

7.3.3.1.10 Información específica del fabricante

Si se presenta información específica del fabricante para el PS, DEBE codificarse en el campo de información específica del fabricante (VSIF, *vendor specific information field*) (código 43) utilizando el campo ID de fabricante para especificar qué TLV tuplas son las que se aplican a determinados productos del fabricante. El ID del fabricante DEBE ser el primer Sub-TLV que se integra en el VSIF. Si el primer TLV en el VSIF no es un ID de fabricante, en ese caso se DEBE ignorar el fichero de configuración del PS.

Este valor de configuración puede aparecer en múltiples ocasiones. El mismo ID de fabricante puede aparecer múltiples veces. NO HABRÁ más de un Sub-TLV de ID de fabricante en un solo VSIF.

Tipo	Longitud	Valor
43	n	Valores específicos del fabricante

7.3.3.1.10.1 Sub-TLV 43.1 – Tipo de ID de fabricante

Identificación de fabricante especificada mediante el identificador único de organización de tres bytes del fabricante del PS.

Tipo	Longitud	Valor
43.1	3	v1, v2, v3

7.3.3.1.11 Marcador de fin de datos

Se trata de un marcador especial de fin de datos. No tiene campos de longitud ni de valor.

Tipo	Longitud	Valor
255	–	–

7.3.3.1.12 Verificación de integridad del mensaje (PS MIC, *PS message integrity check*)

Tipo	Longitud	Valor
53	20	Troceo SHA de 160 bits (20 octetos)

Este parámetro incluye un troceo (PS MIC) que se calcula con un algoritmo de troceo seguros (SHA-1, *secure hash algorithm*) que se define en FIPS 180-2. Este TLV se utiliza únicamente en el fichero de configuración inmediatamente antes del marcador de fin de datos.

7.3.3.2 Modo de activación

La transferencia del fichero de configuración desde el servidor TFTP en la red de cabecera hasta el elemento PS, se inicia por un evento denominado activador. Los requisitos para activar la transferencia de un fichero de configuración del PS desde el servidor TFTP al PS se indican a continuación.

El modo de activar la descarga del fichero de configuración del PS depende del modo de configuración en que esté funcionando el PS. El CMP DEBE leer el valor de cabhPsDevProvMode (véase 7.2.3.3) antes de iniciar la descarga del fichero de configuración del PS.

Activador de la descarga del fichero de configuración del PS para el modo de configuración DHCP:

Si el PS recibe la dirección de servidor TFTP en el campo 'siaddr' y el nombre del fichero de configuración en el campo 'file' del DHCP ACK, el PS DEBE combinar la dirección del servidor TFTP y el nombre del fichero de configuración del PS para formar un valor codificado como URL y escribir dicho valor en cabhPsDevProvConfigFile. El PS DEBE utilizar el siguiente formato en el valor codificado como URL para la dirección del servidor TFTP y el nombre del fichero de configuración del PS.

tftp://dirección IPv4 del servidor TFTP/trayecto completo al fichero de configuración del PS/nombre del fichero de configuración del PS.

La descarga del fichero de configuración del PS, efectuada por un PS funcionando en el modo de configuración DHCP, se activa por la presencia de la situación de fichero de configuración del PS (dirección IP del servidor TFTP) y de su nombre en el mensaje DHCP enviado al PS (CDC) por el servidor DHCP de la red de cable. Consúltese 7.2.3.3.

Si el PS está funcionando el modo de configuración DHCP (indicado por el valor de cabhPsDevProvMode), tras la recepción en el PS (CDC) de un DHCPACK procedente del servidor DHCP de la red de cable, el PS DEBE emitir una petición TFTP Get al servidor identificado en el campo 'siaddr' del mensaje DHCP a fin de descargar el fichero identificado en el campo 'file' del mensaje DHCP.

El PS DEBE emitir mensajes de petición TFTP Get sólo a través de la interfaz WAN-Man del PS.

La modificación de cabhPsDevProvConfigFile NO DEBE activar un PS que funcione en el modo de configuración DHCP para la descarga de un fichero de configuración. Este PS DEBE tratar el fichero cabhPsDevProvConfigFile como un objeto de sólo lectura.

El PS DEBE negarse a aceptar cualquier fichero de configuración de PS que se reciba a través de cualquier interfaz, excepto cuando se trata de la interfaz WAN-Man de PS.

Activación de la descarga del fichero de configuración del PS en el modo de configuración SNMP:

Si el PS está funcionando en el modo de configuración SNMP (indicado por el valor de cabhPsDevProvMode), la descarga del fichero de configuración del PS NO DEBE tener lugar antes de la terminación del proceso de autenticación SNMP v3 (consúltese en la cláusula 11 los detalles del proceso de autenticación SNMP).

Si el PS está funcionando en el modo de prestación SNMP (indicado por el valor de cabhPsdevProvMode), el elemento PS NO DEBE iniciar la descarga del fichero de configuración del PS si el NMS no ha suministrado un valor válido para cabhPsDevProvConfigHash (MIB de PSDev).

Cuando el PS que funciona en el modo de configuración SNMP (indicado por el valor de cabhPsDevProvMode) emite una petición TFTP para la descarga de un fichero de

configuración de PS (sujeto a las condiciones que se describen más adelante para otros requisitos), DEBE concluir la fase de descarga. Cuando el PS (CMP) termina satisfactoriamente dicha descarga, DEBE procesarlo antes de emitir una petición TFTP de otro fichero de configuración de PS.

Se necesita un mecanismo de señalización para informar a la entidad de gestión que el PS se encuentra procesando un fichero de configuración. El objeto MIB Dev de PS cabhPsDevProvConfigFileStatus se destina a desempeñar la función de mecanismos de señalización.

Si un PS (CMP) no se encuentra solicitando, descargando o procesando un fichero de configuración, DEBE fijar cabhPsDevProvConfigFileStatus = idle(1). Cuando el mismo PS ha emitido una petición TFTP de un fichero de configuración especificado en cabhPsDevProvConfigFile, DEBE fijar cabhPsDevProvConfigFileStatus = busy(2), y cuando completa el procesamiento del fichero de configuración del PS, DEBE fijar cabhPsDevProvConfigFileStatus = idle(1).

El PS (CMP) DEBE tratar de descargar y procesar el fichero de configuración con el nombre y dirección especificados en cabhPsDevProvConfigFile cuando recibe un mensaje de petición de establecimiento de SNMP para el objeto cabhPsDevProvConfigFile, si son verdaderas las condiciones:

- el PS se encuentra funcionando en el modo de configuración SNMP;
- el objeto cabhPsDevProvConfigHash tiene un valor válido; Y
- cabhPsDevProvConfigFileStatus = idle(1).

El formato de cabhPsDevProvConfigFile DEBE ser una dirección IP de servidor TFTP codificada como URL y un nombre de fichero de configuración.

Si el PS (CMP) que está funcionando en el modo de configuración SNMP recibe una petición de establecimiento de SNMP del NMS con objeto de actualizar el valor de cabhPsDevProvConfigFile Y cabhPsDevProvConfigFileStatus = busy(2) O si el objeto cabhPsDevProvConfigHash no tiene un valor válido, en ese caso el PS DEBE rechazar la petición de establecimiento.

Funcionamiento tras la activación:

Una vez activado, el PS DEBE utilizar un cliente TFTP conforme a RFC 1350 para descargar los ficheros de configuración del PS.

A continuación, el elemento PS DEBE seguir tratando de descargar el fichero de configuración del PS especificado de la ubicación determinada hasta que lo logre satisfactoriamente y se calcule con éxito el troceo como se describe en 7.3.3.3. Si el primer intento no tuvo éxito, el PS DEBE utilizar un límite temporal adaptativo para el TFTP basado en la reducción exponencial binaria que se describe más adelante, hasta que el PS (CMP) reciba satisfactoriamente el fichero solicitado del servidor TFTP en la cabecera:

- cada reintento se realiza 2^n segundos a partir del intento anterior, siendo n = [0, 1, 2, 3, 4 ó 5] el contador de reintentos del fichero de configuración del PS;
- n = 0 para el primer reintento, y a continuación aumenta en 1 para cada intento subsiguiente, hasta n = 5;
- si el PS no consigue satisfactoriamente el fichero solicitado después del intento con n = 5, n se reactiva a 0 y el PS debe rearrancar el proceso de adquisición de IP de la WAN-Man a través de DHCP.

El PS DEBE intercambiar mensajes TFTP sólo a través de la interfaz WAN-Man del PS y rechazar cualquier fichero de configuración que no se reciba a través de dicha interfaz.

Cuando se completa la descarga TFTP del fichero de configuración del PS, Y ese fichero se autentica adecuadamente conforme a 7.3.3.3, el PS debe procesar los TLV incluidos en el

fichero como se describe más adelante. Consúltese 7.3.3.4 para obtener detalles sobre el tratamiento de errores y la generación de eventos durante el procesamiento del fichero de configuración del PS.

El PS DEBE utilizar parámetros obtenidos del fichero de configuración de PS para fijar los objetos gestionados en la base de datos del PS. Desde el punto de vista funcional, ese proceso es equivalente al funcionamiento en modo SNMP SET, pero no depende del usuario o de permisos de acceso basados en vistas. El PS DEBE actualizar los objetos gestionados sin condiciones en la base de datos del PS que correspondan a OID reconocidos.

El PS DEBE traducir los elementos TLV-28 del fichero de configuración del PS en una sola PDU de SNMP que incluya (n) MIB OID/ejemplar y componentes de valor (vinculaciones variables (varbinds) de SNMP). Conforme a la [RFC 1905], la única PDU de SNMP generada por el fichero de configuración del PS será considerada "como simultánea" y el PS debe comportarse congruentemente, sin tener en cuenta el orden en que aparecen los elementos TLV-28 en el fichero de configuración del PS o en la PDU de SNMP. El requisito de una única PDU de SNMP generada por el fichero de configuración del PS es congruente con el comportamiento de los paquetes PDU de SNMP que se reciben del gestor del SNMP; el orden de las varbind de la PDU del SNMP no es relevante, y no hay un límite determinado para la PDU de SNMP MAX. Una vez creada la PDU de SNMP única, el PS la procesa y determina la aceptación/rechazo de la configuración del PS basándose en las reglas de procesamiento del fichero de configuración del PS que se describen en 7.3.3.4.

El tamaño del fichero de configuración del PS DEBE actualizarse en el objeto MIB cabhPsDevProvConfigFileSize.

El número de TLV procesados (es decir, los TLV que tienen por objeto modificar la configuración del PS de acuerdo con su propio campo valor) y el número de TLV ignorados (es decir, los TLV que tienen por objeto modificar la configuración del PS conforme a sus propios campos valor y que fracasan) DEBEN actualizarse en los objetos MIB cabhPsDevProvConfigTLVProcessed y cabhPsDevProvConfigTLVRejected, respectivamente. Los tipos de parámetros de configuración 255 (marcador de fin de datos), 53 (PS MIC), 0 (valor de configuración de relleno) y los pares de campo de tipo y de longitud que engloban sub TLV no especifican valores en los campos valor cuyo objetivo sea modificar la configuración del PS y por consiguiente NO DEBEN tenerse en cuenta en los valores de cabhPsDevProvConfigTLVProcessed y cabhPsDevProvConfigTLVRejected.

Conforme a estas definiciones un TLV que no configura satisfactoriamente el PS se cuenta dos veces, una vez por cabhPsDevProvConfigTLVProcessed y otra por cabhPsDevProvConfigTLVRejected. Un TLV que configura satisfactoriamente el PS se cuenta solamente por cabhPsDevProvConfigTLVProcessed.

7.3.3.3 Medios de autenticación del fichero de configuración del PS

Esta cláusula define el procedimiento de autenticación del fichero de configuración del PS.

El algoritmo que se emplea para verificar el troceo del fichero de configuración del PS depende del modo de configuración del elemento PS (véase 5.5). Hay dos tipos de modo de configuración, el modo de configuración DHCP y el modo de configuración SNMP. En las siguientes cláusulas se describen los algoritmos y los requisitos de seguridad necesarios para verificar el troceo del fichero de configuración del PS basándose en el modo de configuración del elemento PS. Este elemento DEBE soportar los dos algoritmos de seguridad que se determinan en 7.3.3.3.1 y 7.3.3.3.2.

7.3.3.3.1 Algoritmo de autenticación del fichero de configuración del PS para el modo de configuración DHCP

El procedimiento para verificar el troceo del fichero de configuración de PS mediante el elemento PS funcionando en el modo de configuración DHCP es el siguiente:

1) Cuando el generador del fichero de configuración del sistema de configuración crea un nuevo fichero de configuración de PS o modifica un fichero existente, dicho generador creará un troceo SHA-1 del contenido del fichero de configuración del PS, que se considera como una cadena de bytes. El marcador de fin de datos y cualquier relleno que venga a continuación no se incluyen en el cálculo del troceo.
2) El generador del fichero de configuración añade el valor de troceo, que se calculó en el paso 1, al fichero de configuración del PS como el último valor TLV (inmediatamente antes del marcador de fin de datos) utilizando un TLV tipo 53. A continuación, el fichero de configuración del PS se pone a disposición del servidor TFTP pertinente.
3) El elemento PS descarga el fichero de configuración del PS.
4) El PS DEBE actualizar el objeto MIB cabhPsDevProvConfigHash con el valor de troceo del TLV de troceo que se creó en los pasos 1 y 2.
5) El elemento PS DEBE calcular un troceo SHA-1 del contenido del fichero de configuración del PS excluyendo el TLV de troceo (que se emplea para configurar el objeto MIB cabhPsDevProvConfigHash), el marcador de fin de datos y cualquier relleno que venga a continuación. Si el troceo calculado y el valor del objeto MIB anterior son idénticos, se verifica la integridad del fichero de configuración del PS y a continuación se DEBE procesar; de lo contrario, el fichero DEBE rechazarse.

7.3.3.3.2 Algoritmo de autenticación del fichero de configuración para el modo de configuración SNMP

El procedimiento para verificar el troceo del fichero de configuración del PS mediante el elemento PS en modo de configuración SNMP es el siguiente:

1) Cuando el generador del fichero de configuración del sistema de configuración crea un nuevo fichero de configuración de PS o modifica un fichero existente, dicho generador creará un troceo SHA-1 del contenido del fichero de configuración del PS, que se considera como una cadena de bytes. El marcador de fin de datos y cualquier relleno que venga a continuación no se incluyen en el cálculo del troceo.
2) El NMS envía el valor de troceo que se calculó en el paso 1 al elemento PS a través de SNMP SET. El PS actualiza su objeto MIB cabhPsDevProvConfigHash con el nuevo valor.
3) El NMS envía el nombre y la ubicación del fichero de configuración del PS a través de SNMP SET. El PS actualiza su objeto MIB cabhPsDevProvConfigFile con el nuevo valor.
4) El elemento PS descarga el fichero nombrado desde el servidor TFTP configurado. Si el fichero de configuración del PS incluye el TLV tipo 53, el PS debe ignorarlo.
5) El elemento PS DEBE calcular un troceo SHA-1 del contenido del fichero de configuración del PS excluyendo el TLV 53 si está presente, el marcador de fin de datos y cualquier relleno que venga a continuación. Si el troceo que se calculó y el valor del objeto MIB cabhPsDevProvConfigHash son idénticos, se verifica la integridad del fichero de configuración del PS y a continuación DEBE procesarse; de lo contrario, el fichero DEBE rechazarse.

Se considera que la descarga del fichero de configuración del PS ha tenido éxito cuando el elemento PS ha recibido completa y correctamente el contenido del fichero de configuración del PS dentro del periodo de tiempo del TFTP Y se ha efectuado por parte del PS el cálculo de los valores de troceo del fichero de configuración del PS sin errores.

7.3.3.4 Medios de comunicación del estado

El PS DEBE comunicar el estado y las condiciones de error de descarga del fichero de configuración por medio del proceso de comunicación de eventos descrito en 6.5.

En el cuadro 7-12 se indican los modos de éxito y de fracaso con los que podría encontrarse la descarga y el procesamiento del fichero de configuración del PS, y las medidas que DEBE tomar el PS cuando los detecta.

Cuadro 7-12/J.191 – Modos de procesamiento del fichero de configuración del PS

Modo de fallo	Medida
El campo tipo no es válido para IPCable2Home	Desechar el TLV en cuestión y comunicar el evento. Continuar procesando el fichero.
Fallo de TFTP – se envió la petición Get y no se recibió respuesta.	Comunicar un evento (68000500) y reintentar TFTP.
Fallo de TFTP – no se encontró el fichero de configuración	Comunicar un evento (68000600) y reintentar TFTP.
Fallo de TFTP – paquetes en desorden	Comunicar un evento (68000700) y reintentar TFTP.
Fallo durante la descarga de TFTP – se rebasó el número máximo de reintentos	Comunicar un evento (68000900) y reactivar.
Descarga satisfactoria de TFTP	Comunicar un evento (68001000) e iniciar la verificación de la autenticación.
Fallo del proceso de verificación de autenticación del fichero	Comunicar un evento (68000800) y reactivar. No se debe tratar de procesar el fichero.
El fichero es demasiado largo	Comunicar un evento (73040102) y reactivar. No se debe tratar de procesar el fichero
No existe marcador de fin de fichero	Comunicar un evento (73040102) y reactivar. No se debe tratar de procesar el fichero.
Duplicación del OID de TLV-28	Comunicar un evento (73040102), rechazar el fichero de configuración, y reactivar. Conservar todos los valores de objeto existentes antes de tratar de procesar el fichero de configuración con problemas.
Tipo reconocido pero valor erróneo u OID de TLV-28 válido pero el valor de la MIB es erróneo	Comunicar un evento (73040102), rechazar el fichero de configuración y reactivar. Conservar todos los valores de objeto existentes antes de tratar de procesar este fichero de configuración erróneo.
Imposibilidad de fijar el valor	Comunicar el evento, rechazar el fichero de configuración y reactivar. Regresar a su valor original (es decir, al valor antes de SNMP Set) cualquier valor almacenado en memoria no volátil.
El CMP descubre un OID de SNMP OID que no puede reconocer	Desechar el TLV en cuestión y comunicar el evento (73040100). Continuar el procesamiento del fichero.

Véase el anexo B para obtener una lista de los eventos incluidos los enumerados en el cuadro 7-12 así como información relativa a la forma en que comunican los eventos.

Intento infructuoso de descarga del fichero de configuración del PS – Con posibilidad de reintentos de TFTP

Si el contador de reintentos del fichero de configuración del PS indica menos de 5, Y concluye el periodo de temporización de la petición TFTP Get, el fichero de configuración del PS no se encuentra en el servidor TFTP, O la petición TFTP Get sufre un fallo debido al desorden de los paquetes, el PS DEBE iniciar el funcionamiento de CDS y CNP, comunicar el evento pertinente y reintentar la descarga del fichero de configuración del PS, de acuerdo con el algoritmo de reintentos que se describe en 7.3.3.2.

El PS DEBE comunicar el evento pertinente indicado en el anexo B, señalando la descarga sin éxito del fichero de configuración del PS, cada vez que el PS fracasa durante el proceso de descarga de ese fichero.

Intento infructuoso de descarga del fichero de configuración del PS – Se agotan los reintentos de TFTP

Si el contador de reintentos del fichero de configuración del PS es igual a 5, Y el PS no ha podido descargar con éxito el fichero de configuración del PS, el PS DEBE comunicar el evento indicado en el anexo B a fin de señalar el fallo del proceso de descarga, Y liberar su dirección IP de WAN-Man del PS conforme a la norma [RFC 2131], Y reactivar el proceso de adquisición de IP de WAN-Man a través de DHCP.

Descarga satisfactoria del fichero de configuración del PS

Si el PS descarga con éxito el fichero de configuración del PS, DEBERÁ reactivar a cero el contador de reintentos del fichero de configuración del PS y comunicar el evento pertinente indicado en el anexo B para señalar la descarga con éxito del fichero.

Si falla la verificación de la autenticación del fichero de configuración del PS de acuerdo a 7.3.3.3, el PS DEBE detener el proceso de configuración, rechazar el fichero de configuración del PS, comunicar el evento pertinente y reactivar el proceso de adquisición de IP de WAN-Man a través de DHCP.

Si el fichero de configuración del PS no incluye EOF TLV o resulta demasiado largo para su proceso, el PS DEBE detener el proceso de configuración, rechazar el fichero de configuración del PS, comunicar el evento pertinente y reactivar el proceso de adquisición de IP de WAN-Man a través de DHCP.

Si el fichero de configuración del PS incluye elementos TLV-28 duplicados (lo que significa que el objeto MIB de SNMP tiene un OID idéntico), el PS DEBE detener el proceso de configuración, rechazar el fichero de configuración del PS, comunicar el evento pertinente y reactivar el proceso de adquisición de IP de WAN-Man a través de DHCP.

Si el fichero de configuración del PS incluye un campo de tipo reconocido pero un campo de valor erróneo o un OID de TLV 28 válido pero con un valor de MIB erróneo, el PS DEBE detener el proceso de configuración, rechazar el fichero de configuración del PS, comunicar el evento pertinente y reactivar el proceso de obtención de IP de WAN-Man a través de DHCP.

Si el fichero de configuración del PS incluye un campo de tipo que no puede reconocer o un elemento TLV-28 con un OID que no puede reconocer, el PS DEBE ignorar ese TLV, comunicar el evento pertinente, Y continuar con el procesamiento del fichero de configuración del PS.

7.4 Arquitectura del cliente de hora del día

7.4.1 Directrices de diseño del sistema cliente de hora del día

Las siguientes directrices de diseño del sistema permiten obtener las capacidades definidas para el cliente de hora del día del PS:

Cuadro 7-13/J.191 – Directrices de diseño del sistema cliente de hora del día

Número	Directrices de diseño del sistema cliente de hora del día
TOD 1	Es necesario proporcionar un mecanismo que permita al PS obtener la sincronización temporal con la red de cabecera

7.4.2 Descripción del sistema cliente de hora del día

El elemento de servicios de portal utiliza un cliente de hora del día conforme a RFC 868, a fin de obtener la sincronización temporal con un servidor de tiempo de la red de cabecera. La sincronización temporal es indispensable para las funciones de seguridad del PS así como para la mensajería de eventos.

Cuando el cliente CDC DHCP solicita una dirección IP – del servidor DHCP de cabecera – para la interfaz WAN-Man, el cliente DHCP recibirá una dirección IP del servidor de hora del día (ToD) de la cabecera dentro de la opción 4 del DHCP. El cliente DHCP recibirá asimismo la diferencia horaria (respecto a la UTC), dentro de la opción 2 del DHCP.

Una vez que la pila IP WAN-Man comienza a utilizar la dirección IP recibida del DHCP, debe enviar una consulta temporal RFC 868 al servidor ToD. Si el servidor ToD proporciona una respuesta válida, el PS comenzará a utilizar esta hora del día para las identificaciones de tiempo de los mensajes y las funciones de seguridad.

7.4.3 Requisitos del cliente de hora del día

El elemento de servicios de portal DEBE implementar un cliente de hora del día.

El cliente de hora del día de servicios de portal DEBE cumplir el protocolo de hora del día [RFC 868] y utilizar únicamente el protocolo UDP.

Una vez rearrancado, el elemento de servicios de portal DEBE inicializar su hora a 00:00.0 (medianoche) del 1 de enero de 1970.

El elemento de servicios de portal DEBE intentar sincronizar la hora del día con los servidores de tiempo proporcionados en la opción 4 del DHCP ACK, que se reciben por la interfaz WAN-Man durante la obtención de la licencia de la WAN-Man.

Si el PS recibe la opción 4 del DHCP (opción de servidor de tiempo) en el DHCP ACK, DEBE almacenar la dirección IP del servidor de tiempo del cual aceptó la respuesta el PS como el valor de cabhPsDevTimeServerAddr.

El PS DEBE combinar el tiempo recuperado del servidor ToD con la diferencia horaria proporcionada por la opción 2 del DHCP para crear la hora local actual.

El elemento de servicios de portal DEBE utilizar la hora local actual calculada a partir de la hora recuperada del servidor ToD y la diferencia horaria recibida por la opción 2 del DHCP para las funciones que necesitan la hora del día y que demandan una precisión al segundo más próximo.

La prioridad del reloj de hora del sistema para un PS integrado es la siguiente:

- Primera prioridad: hora del día obtenida del servidor ToD.
- Segunda prioridad: hora del día obtenida del módem de cable.
- Tercera prioridad: hora reactivada al 1 de enero de 1970.

Un PS integrado DEBE utilizar la hora del día válida más reciente obtenida del servidor ToD para el reloj de hora del día del sistema, aun en el caso de que esto signifique la sustitución de la hora del sistema obtenida por el CM.

Si un PS integrado no puede obtener la hora del día del servidor ToD, DEBE utilizar la hora del día obtenida por el módem de cable para el reloj de hora del día del sistema.

Si un PS integrado no puede obtener la hora del día del servidor ToD, Y tampoco puede obtener la hora del día válida del módem de cable, DEBE utilizar la hora del día inicializada en el proceso de arranque al 1 de enero de 1970 para el reloj de hora del día del sistema.

La prioridad del reloj de hora de día del sistema para un PS autónomo es la siguiente:

- Primera prioridad: hora del día obtenida del servidor ToD.
- Segunda prioridad: hora inicializada al 1 de enero de 1970.

Un PS autónomo DEBE utilizar la hora del día válida más reciente obtenida del servidor ToD para el reloj de hora del día del sistema.

Si un PS autónomo no puede obtener la hora del día del servidor ToD, DEBE utilizar la hora del día inicializada en el proceso de arranque al 1 de enero de 1970 para el reloj de hora del día del sistema.

El elemento PS DEBE seguir tratando de comunicarse con el servidor de hora del día, hasta establecer la hora local. El servidor DHCP podría ofrecer al PS múltiples direcciones IP de servidor de hora del día en su mensaje DHCP ACK. El PS DEBE tratar de obtener la hora del día de todos los servidores de hora del día incluidos en el DHCP ACK que recibe del servidor DHCP, hasta establecer la hora local. El límite temporal específico para las peticiones de hora del día depende de la implementación. No obstante, el cliente hora del día del PS NO DEBE rebasar más de tres peticiones de ToD en cualquier periodo de 5 minutos, por cada servidor identificado en el DHCP ACK. Como mínimo, el cliente hora del día del PS DEBE emitir una petición ToD por cada periodo de 5 minutos y por cada servidor especificado, hasta establecer la hora local.

Si el servidor ToD no proporciona una respuesta válida el PS DEBE efectuar lo siguiente, aunque no necesariamente en este orden:

- fijar el valor de cabhPsDevTodSyncStatus a '2' (acceso al ToD fracasado);
- si hay licencias activas en el sector LAN-Trans indicadas por un valor distinto de cero para cabhCdpLanTransCurCount, fijar cabhCdpLanAddrCreateTime a la hora actual y fijar cabhCdpLanAddrExpireTime al valor de cabhCdpLanAddrCreateTime más el valor de cabhCdpServerLeaseTime para cada licencia activa (Hora de expiración = CreateTime + LeaseTime);
- efectuar el registro histórico del fallo y generar un evento normal definido en el anexo B,
- seguir intentando la comunicación con el servidor ToD hasta que se establezca la hora local, y
- tratar de descargar el fichero de configuración del PS conforme a 7.3.3.2.

Si el servidor ToD no proporciona una respuesta válida el PS DEBE efectuar lo siguiente y no necesariamente en el orden de la lista:

- fijar el valor de cabhPsDevTodSyncStatus a '1' (acceso al ToD con éxito);
- si hay licencias activas en el sector LAN-Trans indicadas por un valor distinto de cero para cabhCdpLanTransCurCount, fijar cabhCdpLanAddrCreateTime a la hora actual y cabhCdpLanAddrExpireTime al valor de cabhCdpLanAddrCreateTime más el valor de cabhCdpServerLeaseTime para cada licencia activa (Hora de expiración = CreateTime + LeaseTime);
- tratar de descargar el fichero de configuración del PS conforme a 7.3.3.2.

Si el valor de cabhPsDevTodSyncStatus es '1', es decir, si ya se estableció el tiempo local, no es necesario que el cliente hora del día emita una petición ToD.

El PS DEBE enviar y recibir mensajes ToD sólo a través de la interfaz WAN-Man.

8 Tratamiento de los paquetes y traducción de direcciones

8.1 Introducción y presentación

8.1.1 Objetivos

Entre los objetivos clave que inspiran las capacidades de tratamiento de los paquetes de IPCable2Home se incluyen:

- Proporcionar la funcionalidad de traducción de direcciones de fácil manejo que dote al operador de cable de visibilidad y capacidad de gestión de los dispositivos en el hogar sin menoscabo de las arquitecturas de encaminamiento orientadas a fuentes basadas en cable.
- Evitar el tráfico superfluo en el cable y en la red doméstica.
- Mantenimiento de direcciones públicas mundialmente direccionables, así como dirección de gestión privada de redes de cable.
- Facilitar el direccionamiento de tráfico IP en el hogar mediante la asignación de direcciones de red a los dispositivos IP de LAN de modo que residan en la misma subred lógica.

8.1.2 Hipótesis

- Se supone que cuando el operador de cable que gestiona los servidores proporciona direcciones IP mundialmente encaminables a los dispositivos clientes en el hogar, dichas direcciones no residirán forzosamente en la misma subred.
- Se supone que el cambio de proveedor de servicios de Internet se produce pocas veces, con una frecuencia semejante a la del cambio del principal operador de larga distancia del hogar.

8.2 Arquitectura

En esta cláusula se describen los conceptos clave de la funcionalidad de tratamiento de paquetes de IPCable2Home y de traducción de direcciones.

8.2.1 Directrices de diseño del sistema

Cuadro 8-1/J.191 – Directrices de diseño del sistema de tratamiento de paquetes y de traducción de direcciones

Número	Directrices del diseño del sistema
Tratamiento de paquete 1	Los mecanismos de direccionamiento los controlará el operador y le proporcionarán conocimientos sobre los dispositivos IPCable2Home y la accesibilidad a los mismos.
Tratamiento de paquete 2	El direccionamiento no comprometerá en ningún caso las arquitecturas de encaminamiento de la red de cable vigentes (por ejemplo MPLS, encaminamiento orientado al origen).
Tratamiento de paquete 3	Los mecanismos de gestión de tráfico aislarán la red de cable del tráfico generado por las comunicaciones entre entidades pares dentro del hogar.
Tratamiento de paquete 4	Las direcciones IP se conservarán en la medida de lo posible (ya sean direcciones encaminables mundialmente o direcciones de gestión de la red de cable privada).

8.2.2 Descripción del sistema de tratamiento de paquetes

Esta cláusula proporciona una visión general de los conceptos clave del tratamiento de paquetes y traducción de direcciones.

8.2.2.1 Resumen funcional del tratamiento de paquetes

La funcionalidad de traducción de direcciones y de tratamiento de paquetes la proporciona una entidad funcional denominada portal de dirección del cable (CAP). El CAP comprende los siguientes elementos de traducción de direcciones y de entrega de paquetes:

- Traducción de dirección de cable (CAT).
- Función transferencia.
- Conmutación de entrega selectiva hacia el origen (USFS, *upstream selective forwarding switch*).

Como muestra la figura 8-1, la función CAT proporciona un mecanismo de interconexión entre los sectores de dirección WAN-Data y LAN-Trans (mediante la traducción de direcciones), mientras que la función transferencia proporciona un mecanismo de interconexión entre los sectores de direcciones WAN-Data y LAN-Pass (mediante puenteo). La función CAT es conforme con la traducción de dirección de red (NAT) tradicional, sección 2 de RFC 3022. Como ocurre con la NAT tradicional, hay dos versiones de la CAT que se denominan encaminamiento transparente con traducción de dirección de la red de cable (C-NAT, *cable network address translation*) y encaminamiento transparente con traducción de dirección y de puertos de la red de cable (C-NAPT, *cable network address and port translation*). El encaminamiento transparente C-NAT es la versión homologada de cable del NAT básico, sección 2.1 de RFC 3022, mientras que el encaminamiento transparente C-NAPT es la versión homologada para el cable de NAPT, sección 2.2 de RFC 3022.

De acuerdo con RFC 3022, el encaminamiento transparente C-NAT es "un método por el que las direcciones IP se convierten de un grupo a otro, de modo transparente a los usuarios finales" mientras que el encaminamiento transparente C-NAPT "es un método por el que varias direcciones de red y sus puertos TCP/UDP (Protocolo de control de la transmisión/Protocolo de datagramas del usuario) se traducen a una única dirección de red y a sus puertos TCP/UDP". Además, de acuerdo con RFC 3022, el objeto de la funcionalidad C-NAT y C-NAPT es "proporcionar un mecanismo que permita conectar un sector de direcciones privadas a un sector externo de direcciones únicas registradas mundialmente".

La función transferencia (Pass-through) es un proceso de puenteo específico que interconecta los sectores de direcciones WAN-Data y LAN-Pass sin traducción de direcciones.

La conmutación de entrega selectiva hacia el origen (USFS) define una función del CAP con capacidad de confinar el tráfico de la red doméstica dentro de ésta, aunque los dispositivos en la red doméstica que generan este tráfico residan en subredes IP lógicas distintas. Más concretamente, esta función permite la entrega de tráfico con origen en una dirección IP de uno de los sectores de direcciones LAN, con destino direcciones IP de uno de los sectores de direcciones de la LAN, directamente a su destino. Esta funcionalidad de entrega directa evita que el tráfico atraviese la red HFC e interconecta los sectores de direcciones LAN-Trans y LAN-Pass.

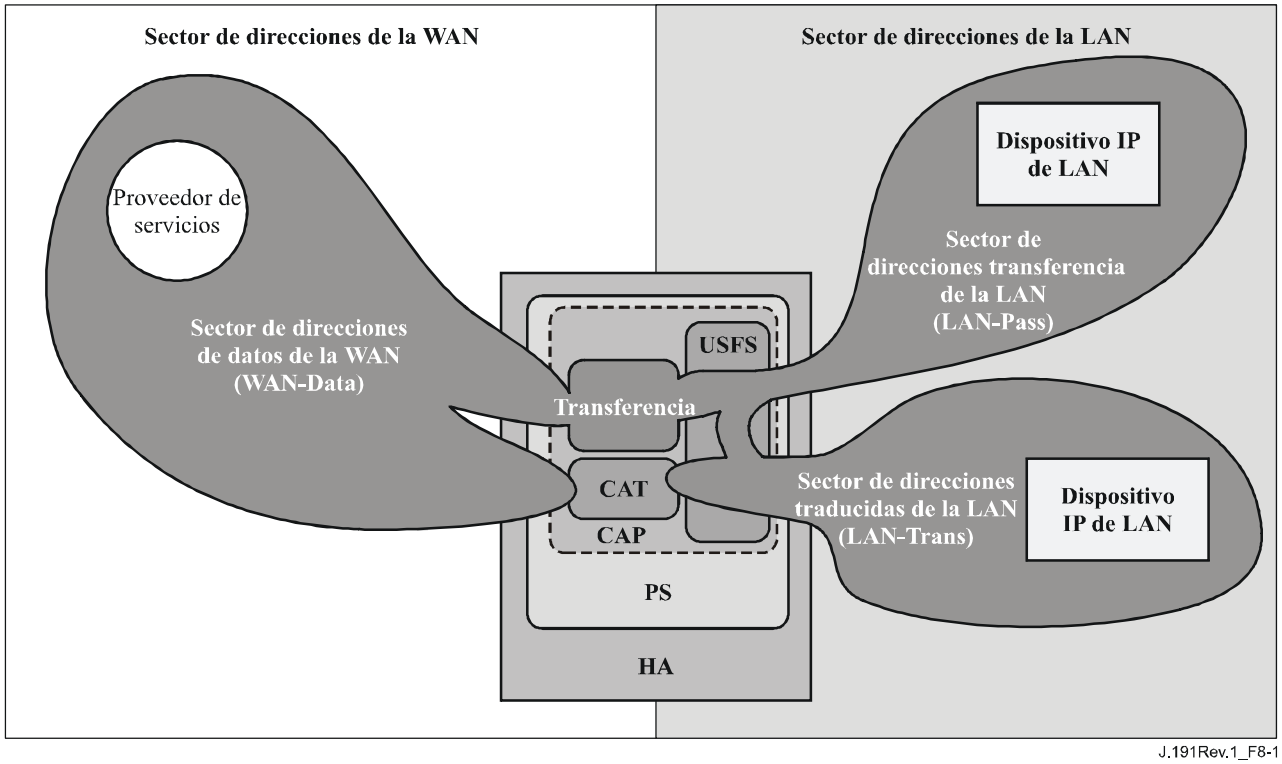


Figura 8-1/J.191 – Funciones del portal de dirección de cable (CAP)

En esta Recomendación, las expresiones vinculación de direcciones, desvinculación de direcciones, traducción de direcciones y sesión se utilizan respetando las definiciones de RFC 2663. Por otra parte, el término "correspondencia" se define como la información necesaria para ejecutar un encaminamiento transparente C-NAT y un encaminamiento transparente C-NAPT.

Concretamente, una correspondencia C-NAT se define como una tupla de la forma (dirección IP WAN-Data, dirección IP LAN-Trans) que proporciona una correspondencia biunívoca entre las direcciones WAN-Data y las direcciones LAN-Trans. Análogamente, una correspondencia C-NAPT se define como una tupla de la forma (dirección IP WAN-Data y puerto TCP/UDP, dirección IP LAN-Trans y puerto TCP/UDP) que proporciona una correspondencia de uno a varios entre una única dirección WAN-Data y varias direcciones LAN-Trans. Para el tráfico ICMP (como por ejemplo el ping), se utiliza un número correlativo en vez del número de puerto TCP/UDP.

El tráfico LAN-a-WAN se define como el conjunto de paquetes que tienen origen en dispositivos IP de LAN con destino a dispositivos en el lado WAN del PS. El tráfico WAN-a-LAN se define como los paquetes que tienen origen en servidores de la WAN con destino a dispositivos IP de LAN. El tráfico LAN-a-LAN se define como el conjunto de paquetes que tienen origen en dispositivos IP de LAN con destino a dispositivos IP de LAN en la misma subred o en otra distinta.

8.2.2.2 Modos de tratamiento de paquetes

El elemento de servicios de portal es configurable, a través del objeto de la MIB cabhCapPrimaryMode para poder funcionar en uno de los tres modos de tratamiento de paquetes primarios cuando maneja tráfico LAN-a-WAN y tráfico WAN-a-LAN: modo transferencia, modo de encaminamiento transparente C-NAT, y modo de encaminamiento transparente C-NAPT. Además, los modos primarios C-NAT y C-NAPT pueden funcionar también en modo híbrido como se expone más adelante.

En modo transferencia, el CAP se comporta como un puente transparente [ISO/CEI 15802-3] entre el sector WAN-Data y el LAN-Pass. En el modo transferencia, las decisiones de encaminamiento se

toman principalmente en la capa 2 de OSI (capa del enlace de datos). En este modo, el CAP no ejecuta función alguna de encaminamiento transparente C-NAT ni C-NAPT.

El CAP soporta el encaminamiento de la capa 3 de OSI (capa de red) tanto en el modo de encaminamiento transparente C-NAT como en el modo de encaminamiento transparente C-NAPT, como se describe más adelante.

En el modo C-NAT, el elemento PS (CDC) adquiere una dirección IP o varias destinadas al tráfico WAN-Data durante el proceso de arranque del PS. Una vez adquiridas, a través de DHCP, estas direcciones IP se utilizan como la porción de direcciones IP WAN-Data de las tuplas de correspondencia C-NAT creadas dinámicamente. Estas direcciones IP de la WAN integran un grupo de direcciones disponibles para las correspondencias C-NAT creadas dinámicamente. Si existe una dirección IP disponible en el grupo de direcciones IP WAN-Data, el CAP crea una correspondencia C-NAT dinámica cuando observa por primera vez tráfico IP LAN-a-WAN que no dispone de una correspondencia. Si no hay direcciones IP disponibles en el grupo de direcciones IP WAN-Data la correspondencia C-NAT dinámica no puede crearse, ignorándose este tráfico y generándose un evento (véase el anexo B).

La porción de la dirección IP LAN-Trans de las tuplas de correspondencia C-NAT creadas dinámicamente la proporciona el grupo de direcciones IP determinadas por el operador de cable en la MIB de CDP. El CAP introduce la tupla de la dirección única IP WAN-Data y una dirección única IP LAN-Trans en el cuadro de correspondencia de CAP, junto con otros parámetros que incluyen los números de puerto de WAN y de LAN, el método de correspondencia y el protocolo de transporte que se emplea para la correspondencia. El CAP no traducirá el número de puerto de las correspondencias C-NAT: los números de los puertos de origen y destino en la cabecera UDP o TCP no se modifican. El CAP introducirá el valor 0 en las anotaciones del número de puerto de WAN y de LAN del cuadro de correspondencia de CAP. La anotación del número de puerto con valor 0 tiene dos finalidades:

1) indica al CAP que no deben traducirse los números de puerto; y
2) indica a cualquier persona que examine el cuadro de correspondencia de CAP que se trata de una correspondencia C-NAT, por lo cual debe hacerse una distinción entre las correspondencias C-NAT (número de puerto 0) y las relativas a C-NAPT (número de puerto distinto de 0).

Las correspondencias C-NAT dinámicas para tráfico UDP se destruyen cuando expira el límite temporal de inactividad cabhCapUdpTimeWait. Las correspondencias C-NAT dinámicas para el tráfico TCP se destruyen cuando expira un periodo temporal de inactividad, cabhCapTcpTimeWait, o bien cuando termina la sesión TCP. Las correspondencias C-NAT dinámicas para el tráfico ICMP se destruyen cuando expira un límite temporal de inactividad, cabhCapIcmpTimeWait. Además, se pueden crear y destruir correspondencias C-NAT estáticas, cuando el sistema del NMS escribe o suprime entradas del cuadro de la MIB cabhCapMappingTable.

En el modo C-NAPT (modo por defecto del sistema cuando sale de fábrica) el elemento PS (CDC) adquiere una dirección IP, destinada al tráfico WAN-Data. Una vez adquirida, a través de DHCP, esta dirección IP se utiliza como porción de dirección IP WAN-Data de las tuplas de correspondencia C-NAPT creadas dinámicamente. Si la dirección IP WAN-Data ya se hubiera adquirido, las correspondencias C-NAPT dinámicas se crearían cuando el CAP observara por primera vez tráfico IP LAN-a-WAN sin correspondencia definida. Si la dirección IP WAN-Data no hubiera sido adquirida (es decir no hubiera una licencia DHCP activa), no podría crearse la correspondencia C-NAPT dinámica y se rechazaría el tráfico, generándose un evento normal (véase el anexo B).

Las correspondencias C-NAPT dinámicas para el tráfico UDP se destruyen cuando expira el límite temporal de inactividad cabhCapUdpTimeWait. Las correspondencias C-NAPT dinámicas para el tráfico TCP se destruyen cuando expira un límite temporal de inactividad, cabhCapTcpTimeWait, o

termina una sesión TCP. Las correspondencias C-NAPT dinámicas para el tráfico ICMP se destruyen cuando expira un límite temporal de inactividad, cabhCapIcmpTimeWait. Además, pueden crearse y destruirse correspondencias C-NAPT estáticas cuando el sistema NMS describe o suprime entradas del cuadro de la MIB cabhCapMappingTable.

La figura 8-2 muestra un proceso característico de correspondencia C-NAPT dinámica con un paquete TCP. En este ejemplo, el PS se configura para funcionar en el modo NAPT y ya ha obtenido una dirección IP de la WAN, habiendo obtenido asimismo el dispositivo IP de LAN una dirección IP del sector LAN-Trans.

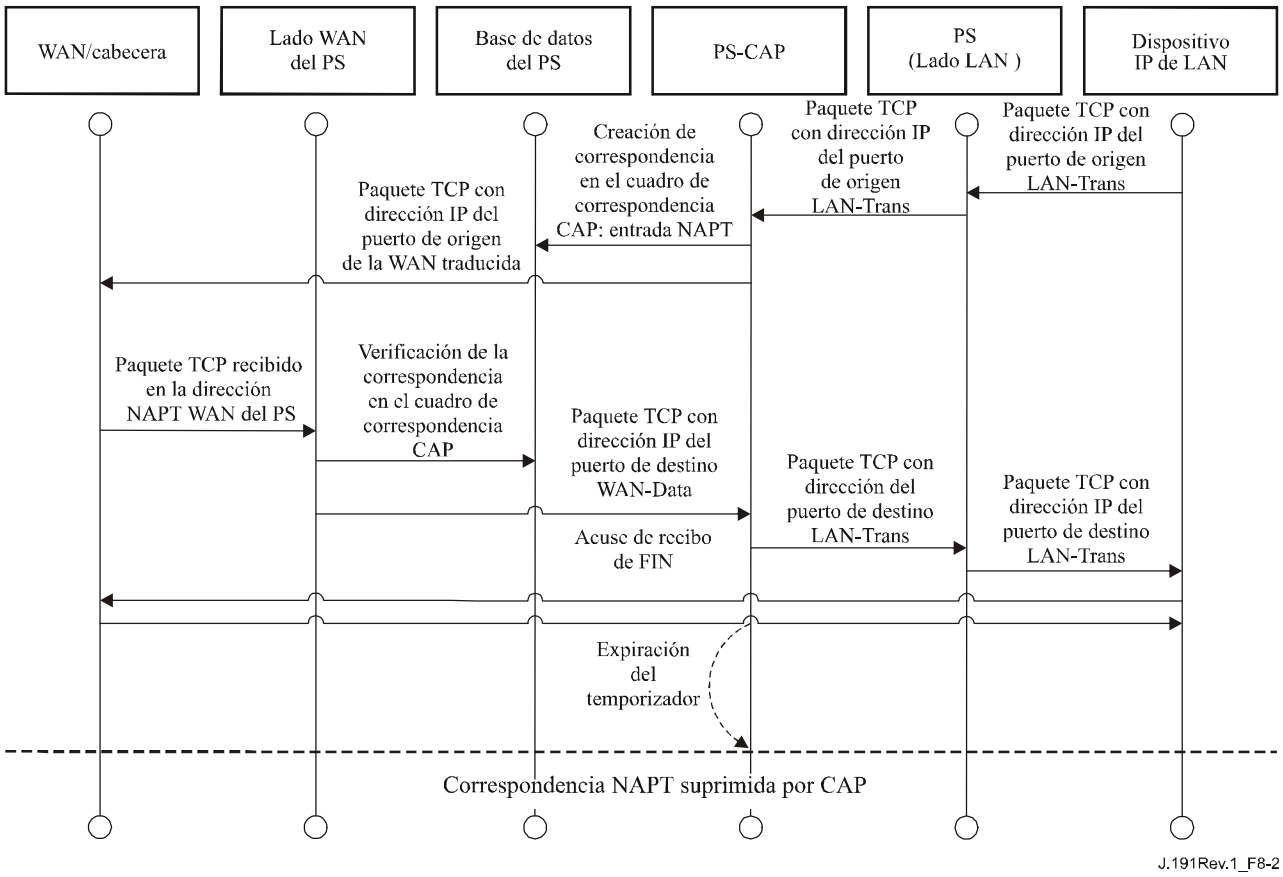


Figura 8-2/J.191 – Diagrama secuencial de la configuración del PS (cuadro de correspondencia CAP-NAPT)

El PS puede funcionar también en un modo híbrido de puenteo y encaminamiento. En tal caso, el NMS establece el modo primario en encaminamiento transparente C-NAT o C-NAPT, y el NMS escribe en el cuadro transferencia (cabhCapPassthroughTable) una dirección MAC o varias pertenecientes a dispositivos IP de LAN cuyo tráfico vaya a ser puenteo. En dicho modo híbrido, el PS examina las direcciones MAC de las tramas recibidas para determinar si debe puentear las tramas en modo transparente o debe ejecutar funciones de encaminamiento transparente C-NAT o C-NAPT en la capa IP. Cuando se trate de tráfico LAN-a-WAN, el PS examinará la dirección MAC de origen, y si ésta existiese en el cabhCapPassthroughTable, la trama se puentearía transparentemente a la interfaz WAN-Data. Cuando se trata de tráfico WAN-a-LAN el PS examina la dirección MAC de destino y si ésta existiera en cabhCapPassthroughTable, la trama se puentearía transparentemente a la interfaz LAN adecuada. Si la dirección MAC no existe en cabhCapPassthroughTable, el paquete lo procesan las funciones de capa superior, y entre ellas la función de encaminamiento transparente C-NAT/C-NAPT.

Se supone que cuando el PS se encuentre en el modo de encaminamiento (C-NAT/C-NAPT), podrá procesar tráfico de difusión conforme a las normas RFC 919, 922, 1812 y 2644. Además, se prevé que cuando el PS se encuentre en el modo de transferencia, el tráfico de difusión se puenteará a todas las interfaces.

Cuando el PS se encuentre en el modo de puenteo/encaminamiento mixto, y recibe tráfico de difusión originado por un dispositivo del cuadro de transferencia, se prevé que puenteará ese tráfico a todas las interfaces. Cuando el PS se encuentre en el modo de puenteo/encaminamiento mixto, y recibe tráfico de difusión en cualquier interfaz WAN, se prevé que lo puenteará a todas las interfaces LAN.

Debe observarse que la funcionalidad USFS (véase 8.2.2.3) se aplica en cada uno de los tres modos de tratamiento de paquetes primario, independientemente de la utilización o no del modo híbrido. Las decisiones de entrega USFS tendrán prioridad sobre otras decisiones de entrega que puedan provocar la entrega de tráfico de la LAN a la WAN.

8.2.2.3 Resumen de la conmutación de entrega selectiva hacia el origen

En ciertos casos, un dispositivo IP de LAN del sector de direcciones LAN-Pass residirá en una subred IP lógica distinta que los demás dispositivos IP de LAN conectados al mismo elemento PS. Es importante evitar que el tráfico entre dichos dispositivos IP de LAN atraviese la red HFC. La conmutación de entrega selectiva hacia el origen (USFS) proporciona la función que evita el antedicho tráfico HFC no deseado.

Más concretamente, el USFS encamina el tráfico con origen y destino dentro del hogar, directamente a su destino. El tráfico con origen en dispositivos IP de LAN con destino a direcciones IP exteriores al sector de direcciones de la LAN atraviesa la funcionalidad de puenteo y encaminamiento CAP sin perturbaciones.

La funcionalidad USFS utiliza el cuadro de traducción de direcciones IP del elemento PS (definido en RFC 2011). Este cuadro, el ipNetToMediaTable RFC 2011, contiene una lista de direcciones MAC, subdirecciones IP correspondientes, y números de índice de interfaz PS de las interfaces físicas a las que están asociadas estas direcciones. El USFS consultará este cuadro antes de adoptar decisiones sobre el encaminamiento del flujo de tráfico LAN-a-WAN. Para rellenar el ipNetToMediaTable el PS obtiene las direcciones MAC e IP y sus asociaciones. Para cada interfaz física asociada, el PS obtiene todas las direcciones IP LAN-Trans y LAN-Pass junto con las vinculaciones MAC asociadas pudiendo obtenerse éstas de diferentes maneras. Entre los métodos de obtención de direcciones IP/MAC específicos del fabricante se encuentran los siguientes: espionaje ARP, supervisión de tráfico y consulta de las entradas del CDP. Las entradas se suprimen del ipNetToMediaTable una vez transcurrido un periodo razonable de inactividad.

El USFS inspecciona todo el tráfico IP recibido de las interfaces PS LAN. Si se comprueba (en el ipNetToMediaTable) que la dirección IP de destino reside en la interfaz PS LAN, la dirección de destino de enlace de datos de la trama original, que es la dirección de la pasarela por defecto, se modifica a la del dispositivo IP de LAN de destino, y el tráfico se entrega desde la interfaz PS LAN adecuada. Si no se encuentra una dirección IP de destino concordante en el ipNetToMediaTable, el paquete se entrega en su forma original a la función de encaminamiento transparente C-NAT/C-NAPT o la función de puenteo transferencia (dependiendo del modo de tratamiento de paquetes activo).

8.2.2.4 Multidifusión

El CAP soporta tráfico multidifusión WAN-a-LAN mediante el puenteo transparente de la mensajería IGMP en sentido descendente [RFC 2236] y de los paquetes multidifusión IP en sentido descendente. Además, cuando el CAP se encuentra funcionando en el modo de encaminamiento transparente C-NAT/C-NAPT, realiza la traducción de la dirección de los mensajes IGMP en sentido ascendente originados por los dispositivos IP LAN que residen en el dominio LAN-Trans.

El CAP entrega a la LAN tráfico IGMP con origen en la WAN para que los anuncios lleguen a los dispositivos IP de LAN. Un dispositivo IP de LAN determinará la multidifusión a la que desea incorporarse y enviará un mensaje "join" de multidifusión. A continuación la fuente de multidifusión podrá pasar datos al dispositivo IP de LAN. Cuando ya no interese el servicio multidifusión, el dispositivo IP de LAN podrá ignorar el servicio suspendiendo la secuencia, o enviar un mensaje "leave" IGMP a la cadena para interrumpir el tráfico transmitido. La figura 8-3 proporciona un ejemplo detallado de los procesos IGMP y multidifusión atravesando un PS.

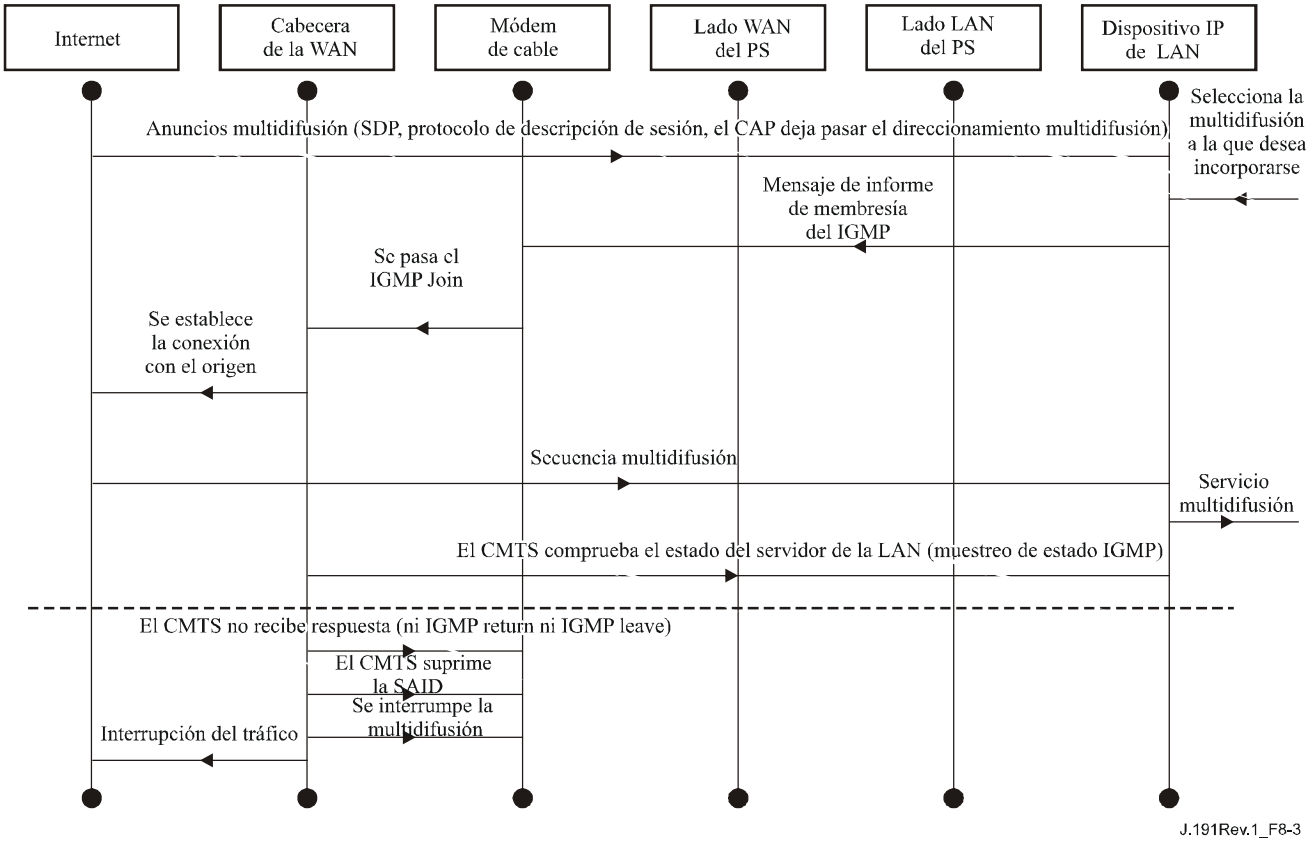


Figura 8-3/J.191 – Secuencia multidifusión mediante IGMP

8.2.2.5 Ejemplos de tratamiento de paquetes

Esta cláusula pretende informar sobre el proceso del tratamiento de paquetes. La figura 8-4 muestra un ejemplo de las posibles etapas de procesamiento de paquetes para el tráfico unidifusión LAN-a-WAN, mientras que la figura 8-5 muestra un ejemplo de las posibles etapas de procesamiento de paquetes para el tráfico unidifusión WAN-a-LAN. Estos ejemplos tienen exclusivamente carácter informativo y no suponen requisitos ni implementación específica alguna.

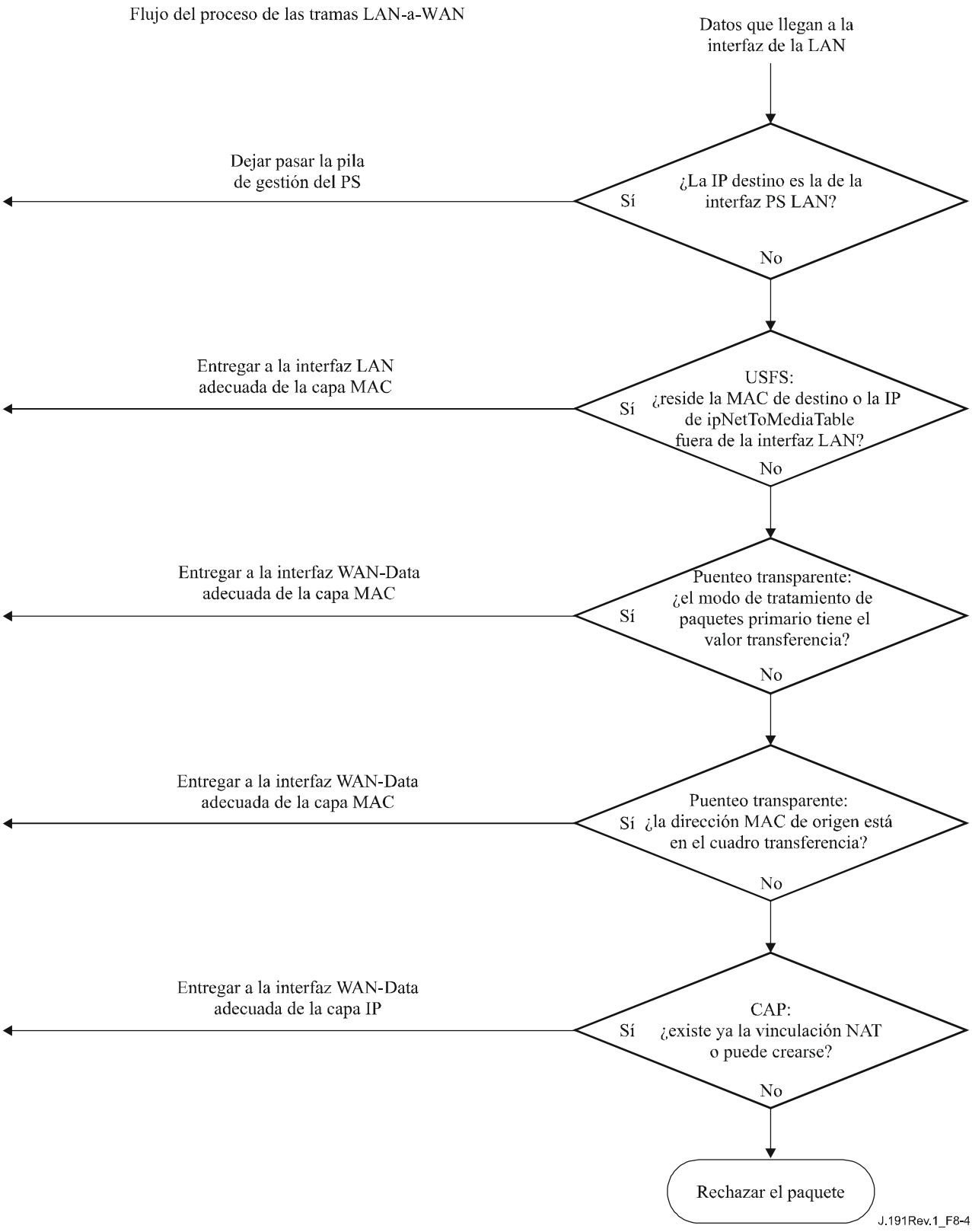


Figura 8-4/J.191 – Ejemplo de procesamiento de paquetes LAN-a-WAN

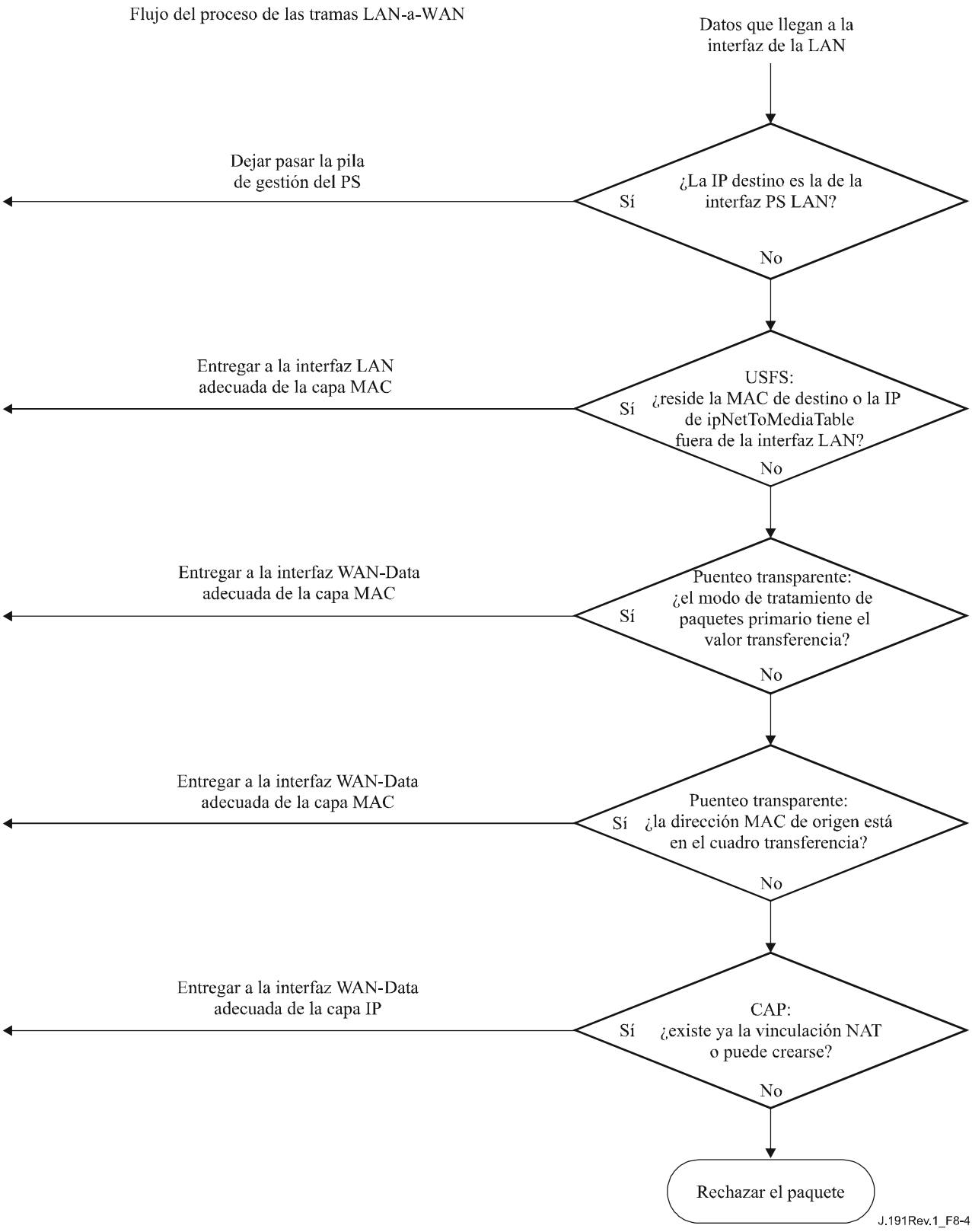


Figura 8-5/J.191 – Ejemplo de proceso de paquetes WAN-a-LAN

8.3 Requisitos CAP

8.3.1 Requisitos generales

Para poder comunicarse normalmente con los anfitriones de Internet, las interfaces IP lógicas del elemento de servicios de portal DEBEN ser conformes con las secciones 3 y 4 de RFC 1122.

El CAP DEBE soportar tráfico de multidifusión de WAN-a-LAN puenteando de manera transparente los mensajes IGMP de WAN-a-LAN y los paquetes multidifusión IP de WAN a LAN como se describe en RFC 2236.

Si el modo de tratamiento de paquetes primario, cabhCapPrimaryMode, se fija a transferencia, todos los mensajes IGMP de LAN-a-WAN DEBEN puentearse de manera transparente.

Si el modo de tratamiento de paquetes primario, cabhCapPrimaryMode, se fija a C-NAPT, la dirección IP de origen de todos los mensajes IGMP de LAN-a-WAN, originados por dispositivos IP de LAN que residen en el dominio LAN-Trans, DEBEN traducirse a la dirección IP de WAN-Data que se utiliza para las correspondencias C-NAPT, y a continuación enviarse a la red WAN.

Si el modo de tratamiento de paquetes primario, cabhCapPrimaryMode, se fija a C-NAT, la dirección IP de origen de todos los mensajes IGMP de LAN a WAN (originados por dispositivos IP de LAN que residen en el dominio LAN-Trans y que tienen una dirección IP que forma parte de una correspondencia C-NAT existente) DEBE traducirse a la dirección IP de WAN-Data que está siendo utilizada en esa correspondencia C-NAT, y a continuación enviarse a la red WAN.

8.3.2 Requisitos del tratamiento de paquetes

El CAP DEBE soportar el modo transferencia, el modo de encaminamiento transparente C-NAT y el modo de encaminamiento transparente C-NAPT, además el CAP DEBE soportar la selección de este modo primario de tratamiento de paquetes mediante el objeto de la MIB cabhCapPrimaryMode.

Si el modo primario de tratamiento de paquetes, cabhCapPrimaryMode, tiene el valor C-NAT, el CAP DEBE asegurarse de que exista una dirección IP disponible en el grupo de direcciones IP WAN-Data suministrada por la cabecera (con una licencia activa DHCP) antes de intentar utilizar esta dirección IP como parte de la correspondencia C-NAT. Si el CAP no pudiera crear una correspondencia C-NAT, por haberse agotado el grupo de direcciones IP WAN-Data, debería generar un evento normal (definido en el anexo B).

El CAP DEBE fijar a cero los números de puerto de la WAN y la LAN (cabhCapMappingWanPort y cabhCapMappingLanPort, respectivamente) del cuadro de correspondencia de CAP para cada correspondencia C-NAT dinámica que cree.

Si el operador de cable crea o modifica una fila del cuadro de correspondencia CAP, es decir, si se crea una fila mediante el método de correspondencia estática (cabhCapMappingMethod = static(1)), Y los objetos de número de puerto de la fila (cabhCapMappingLanPort y cabhCapMappingWanPort) no se han especificado, el CAP DEBE efectuar la anotación cero para cabhCapMappingLanPort y cabhCapMappingWanPort en esa fila.

El CAP NO DEBE traducir el número de puerto de ningún paquete cuya dirección IP aparezca en el cuadro de correspondencia CAP con número de puerto igual a cero.

Si el modo primario de tratamiento de paquetes cabhCapPrimaryMode, tiene el valor C-NAPT, el CAP DEBE asegurarse de que exista una dirección IP de la WAN vigente (con una licencia DHCP activa suministrada por la cabecera) antes de intentar utilizar dicha dirección IP como parte de la correspondencia C-NAPT. Si el CAP no pudiese crear una correspondencia C-NAPT, por no tener una dirección IP de la WAN activa o por no quedar números de puerto, debería generar un evento normal (definido en el anexo B).

El tráfico unidifusión LAN-a-LAN nunca DEBE encaminarse ni puentearse hacia el exterior de una interfaz WAN.

Cuando expire la licencia DHCP de una dirección IP de WAN-Data (que forma parte de la correspondencia C-NAT o C-NAPT), DEBERÁN suprimirse todas las correspondencias asociadas con esa dirección IP del cuadro cabhCapMappingTable.

8.3.2.1 Requisitos del modo transferencia

Cuando el modo primario de tratamiento de paquetes del CAP, cabhCapPrimaryMode, tiene el valor modo transferencia, el CAP DEBE actuar como un puente transparente, definido en ISO/CEI 15802-3, entre los sectores WAN-Data y LAN-Pass, y NO DEBE ejecutar función alguna de encaminamiento transparente C-NAT ni C-NAPT. Aunque el modo primario de tratamiento de paquetes sea transferencia, el procesamiento USFS DEBE tener prioridad frente a las decisiones de puenteo LAN-a-WAN.

8.3.2.2 Requisitos del encaminamiento transparente C-NAT y C-NAPT

Cuando el modo primario de tratamiento de paquetes (cabhCapPrimaryMode) tiene el valor C-NAT, el CAP DEBE soportar los procesos de traducción de direcciones C-NAT de conformidad con los requisitos NAT básicos definidos en RFC 3022.

Cuando el modo primario de tratamiento de paquetes (cabhCapPrimaryMode) tiene el valor C-NAPT, el CAP DEBE soportar los procesos de traducción de direcciones C-NAPT de conformidad con los requisitos NAPT básicos definidos en RFC 3022.

Independientemente del modo primario de tratamiento de paquetes el CAP DEBE soportar la creación y supresión de correspondencias estáticas C-NAT y C-NAPT, mediante la autorización al sistema NMS para leer, crear y suprimir (a través del CMP) entradas de correspondencia CAP estáticas (cabhCapMappingTable).

Las correspondencias estáticas C-NAT y C-NAPT creadas por el NMS DEBEN conservarse en los rearranques del PS.

El CAP DEBE soportar la creación de correspondencias dinámicas C-NAT y C-NAPT, iniciadas por tráfico TCP, UDP o ICMP LAN-a-WAN. El CAP DEBE autorizar al sistema NMS la lectura (a través del CMP) de entradas de correspondencia CAP dinámicas (cabhCapMappingTable).

El CAP DEBE soportar la supresión de correspondencias dinámicas C-NAT y C-NAPT si una correspondencia determinada está asociada a una sesión TCP Y dicha sesión TCP termina O se supera el límite de inactividad del TCP, cabhCapTcpTimeWait, para dicha correspondencia.

El CAP DEBE soportar la supresión de correspondencias dinámicas C-NAT y C-NAPT si una determinada correspondencia está asociada a una sesión UDP Y se supera el límite de inactividad del UDP, cabhCapUdpTimeWait, para dicha correspondencia.

El CAP DEBE soportar la supresión de correspondencias dinámicas C-NAT y C-NAPT si una determinada correspondencia está asociada a una sesión ICMP Y se supera el límite de inactividad del ICMP, cabhCapIcmpTimeWait, para dicha correspondencia.

Las correspondencias dinámicas C-NAT y C-NAPT NO DEBEN conservarse tras los rearranques del PS.

8.3.2.3 Requisitos del modo híbrido puenteo/encaminamiento

El CAP DEBE soportar el modo híbrido puenteo/encaminamiento descrito en 8.2.2, en el que el modo primario de tratamiento de paquetes del CAP, cabhCapPrimaryMode, tiene el valor de encaminamiento transparente C-NAT o C-NAPT y donde el CAP puentea asimismo el tráfico de modo transparente para direcciones MAC específicas. Si el modo primario de tratamiento de paquetes del CAP, cabhCapPrimaryMode, tiene el valor de encaminamiento transparente C-NAT o C-NAPT Y el NMS ha escrito una dirección MAC, perteneciente a un dispositivo IP de LAN, en el cabhCapPassthroughTable, el CAP DEBE puentear transparentemente el tráfico LAN-a-WAN que tiene origen en dicha dirección MAC y el tráfico WAN-a-LAN destinado a dicha dirección MAC.

Cuando se encuentra en el modo híbrido puenteo/encaminamiento descrito en 8.2.2, la función USFS DEBE aplicarse a todo el tráfico recibido que tenga su origen en la LAN.

8.3.3 Requisitos del USFS

La funcionalidad de conmutación de entrega selectiva hacia el origen (USFS) DEBE aplicarse al procesamiento de paquetes, con independencia del modo de tratamiento de paquetes del CAP (transferencia, C-NAT, C-NAPT o híbrido puenteo/encaminamiento).

El elemento PS DEBE obtener todas las direcciones IP LAN-Trans, IP LAN-Pass y MAC de los dispositivos IP de LAN asociados a cada una de sus interfaces de red físicas activas. Las direcciones IP y las direcciones MAC obtenidas por el elemento PS y los números de índice de la interfaz física del PS DEBEN ser accesibles al sistema NMS (a través del CMP) mediante ipNetToMediaTable RFC 2011. El elemento PS DEBE suprimir entradas de ipNetToMediaTable, cuando se alcance el límite temporal de inactividad.

La función USFS DEBE inspeccionar todo el tráfico IP que tenga origen en las interfaces PS LAN, para determinar si la dirección IP de destino de un paquete es la del dispositivo que reside en la interfaz PS LAN. Si la dirección IP de destino de un paquete inspeccionado por el USFS es la de un dispositivo IP de LAN que reside fuera de la interfaz PS LAN, la función USFS DEBE sustituir la dirección de destino de la capa MAC, dentro de la cabecera de la capa 2 del paquete, por la dirección MAC de dicho dispositivo IP de LAN de destino y entregar la trama por la interfaz LAN física adecuada.

9 Resolución de nombres

9.1 Introducción y presentación

9.1.1 Objetivos

Entre los objetivos de la resolución de nombres se encuentran:

- Proporcionar el servicio de nombres de dominio (DNS) desde un servidor del PS a los clientes DNS de los dispositivos IP de LAN, incluso estando el cable desconectado.
- Permitir que los abonados se refieran a los dispositivos locales mediante nombres de dispositivos intuitivos en vez de por direcciones IP.
- Proporcionar respuestas a los clientes DNS de LAN, mediante consultas repetitivas a los servidores DNS distantes, cuando recibe una solicitud de resolución de nombres de anfitrión que no sean locales.
- Proporcionar una recuperación fácil del servicio DNS una vez reestablecida la conectividad del cable tras la desconexión.

9.1.2 Hipótesis

Entre las hipótesis de funcionamiento de los servicios de gestión de nombres se encuentran las siguientes:

- El servidor DNS del elemento PS es el único servidor DNS con autoridad frente a los dispositivos IP de LAN del sector LAN-Trans.
- El elemento PS no prestará el servicio DNS a los dispositivos IP de LAN del sector LAN-Pass.
- Si el elemento PS utiliza varias direcciones WAN-Data, se utilizará la información del servidor DNS de la WAN obtenida durante el último proceso de adquisición de direcciones WAN-Data (DHCP).

9.2 Arquitectura

9.2.1 Directrices de diseño del sistema

Cuadro 9-1/J.191 – Directrices de diseño del sistema de resolución de nombres

Referencia	Directriz de diseño del sistema
Resolución de nombres 1	Proporcionar el servicio de nombres de dominio (DNS) desde un servidor del PS a los clientes DNS de dispositivos IP de LAN, para la resolución de nombres de los dispositivos IP de LAN (independientemente del estado de la conexión de la WAN).
Resolución de nombres 2	Proporcionar respuestas de DNS, mediante consultas repetitivas iniciando con un DNS de cabecera, para los clientes DNS de dispositivos IP de LAN, para la resolución de nombres de anfitrión que no sean locales.

9.2.2 Descripción del sistema

Esta cláusula proporciona un resumen de los servicios de resolución de nombres del elemento PS.

9.2.2.1 Resumen funcional de la resolución de nombres

El portal de denominación del cable (CNP) es un servicio que funciona en el PS y constituye un servidor DNS sencillo para los dispositivos IP de LAN del sector de direcciones LAN-Trans. Los dispositivos IP de LAN del sector LAN-Pass no utilizan el CNP, porque son atendidos por servidores DNS exteriores al hogar.

El CDP configura todos los dispositivos IP de LAN del sector LAN-Trans para que utilicen el CNP como su servidor de nombres de dominio. El servicio CNP del sector LAN-Trans no depende del estado de conexión de la WAN. El CNP efectúa las tareas siguientes:

- Resuelve los nombres de servidor para los dispositivos IP de LAN, devolviendo sus correspondientes direcciones IP.
- Proporciona respuestas de DNS, mediante consultas repetitivas comenzando con un servidor DNS de cabecera, cuando haya consultas que no puedan resolverse por la información local del PS. Esto ocurre cuando la información del servidor DNS de la WAN está disponible en el PS. De lo contrario, el CNP devuelve un error que indica que el nombre no puede resolverse en dicho momento.

La utilización del CNP como servidor DNS primario en la red LAN evita la necesidad de reconfigurar los dispositivos IP de LAN cuando se modifica el estado de conexión de la WAN y permite asimismo modificar la asignación de servidor DNS externo sin tener que reconfigurar los dispositivos IP de LAN.

9.2.2.2 Funcionamiento de la resolución de nombres

Cuando se solicita al CNP que determine un nombre de servidor, ejecuta el proceso de consulta mostrado en la figura 9-1. El CNP responde a las consultas iniciales de DNS normales [RFC 1035], dirigidas a cabhCdpServerDnsAddress, de todas las búsquedas de nombres. El CNP se encarga de efectuar consultas repetitivas a servidores DNS externos (comenzando con la primera anotación de cabhCdpWanDnsServerIp en el cuadro cabhCdpWanDnsServerTable del CDP) cuando un dispositivo IP de LAN le hace una consulta y también para responder a dicho dispositivo ya sea con una respuesta o con un mensaje de error.

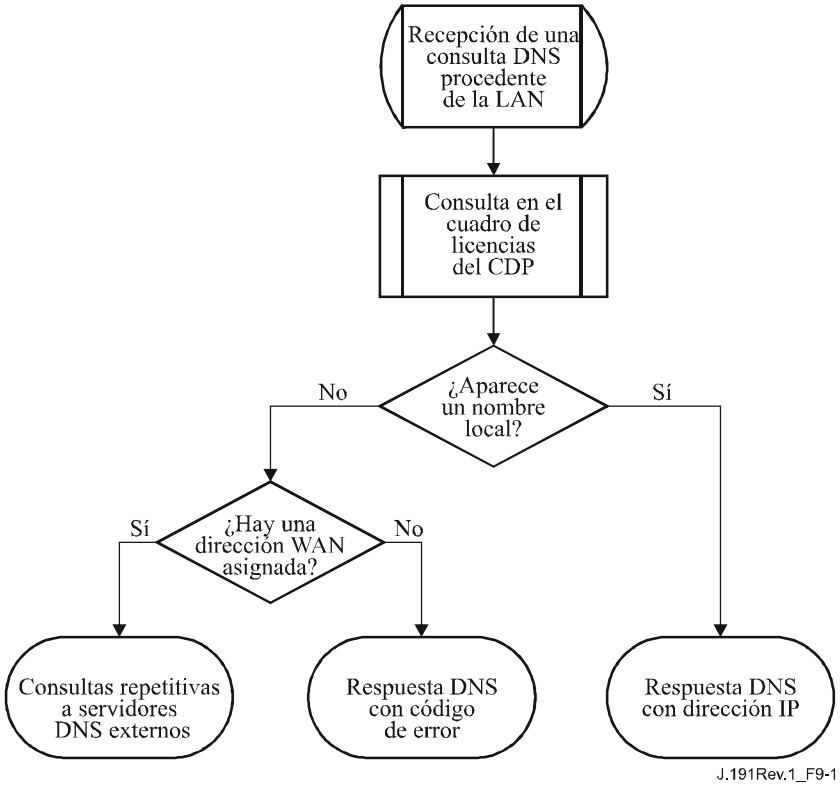


Figura 9-1/J.191 – Procesamiento de los paquetes del CNP

El CNP se basa en el cuadro cabhCdpLanAddrTable del CDP, para enterarse de los nombres de anfitrión asociados con las direcciones IP actuales de los dispositivos IP de LAN activos. Mientras un dispositivo IP de LAN mantiene una licencia DHCP activa con el CDP y ha proporcionado un nombre de anfitrión al CDP (como parte de su proceso de adquisición de dirección IP) el CNP podrá determinar su nombre. Si no puede encontrarse en cabhCdpLanAddrTable, el nombre de anfitrión del que se solicita la determinación, el CNP ejecuta consultas repetitivas a los servidores DNS externos (el primero de los cuales lo obtiene el CDC a través de las opciones DHCP).

Una consulta normal de DNS especifica un nombre de dominio objetivo (QNAME), un tipo de consulta (QTYPE, *query type*) y una clase de consulta (QCLASS, *query class*), y solicita los registros de recursos concordantes. El CNP responde las consultas DNS con QCLASS = IN, y QTYPE = A, NS, SOA o PTR definidos en RFC 1035. No es necesario el soporte de transferencia de zona ni el DNS por TCP.

Como el CNP es un servidor DNS autorizado dentro del sector LAN-Trans, proporcionará registros de comienzo de autoridad (SOA, *start of authority*) y servidor de nombres (NS) autorizado a petición. A continuación se presenta un ejemplo de los campos del registro SOA (véase la sección 3.3.13 de RFC 1035) (véase el cuadro 9-2).

Cuadro 9-2/J.191 – Campos del registro SOA

Campo RDATA de RFC 1035	Objeto de la MIB del CDP
MNAME	cabhCdpServerDomainName
RNAME	Sin especificar
SERIAL	Sin especificar
REFRESH	Sin especificar
RETRY	Sin especificar
EXPIRE	Sin especificar
MINIMUM	Sin especificar

El campo MNAME es el nombre de dominio del sector de direcciones LAN-Trans. El CNP utiliza el valor almacenado en cabhCdpServerDomainName como nombre del dominio del sector de direcciones LAN-Trans.

El campo RNAME es el buzón de la persona responsable del dominio. Si el PS mantuviera una dirección de correo electrónico para el administrador, esta información podría especificarse en dicho campo.

El campo SERIAL es un número de 32 bits sin signo que identifica la versión de la información de zona. Como no se especifican transferencias de zona, el valor de este campo no se especifica.

9.3 Requisitos de la resolución de nombres

El CNP DEBE ajustarse al formato normal de los mensajes DNS y soportar las consultas normales DNS, de acuerdo con lo descrito en RFC 1034 y RFC 1035.

El CNP es un servidor sin memoria de estado que DEBE poder aceptar consultas y enviar respuestas en paquetes UDP [RFC 768].

El CNP DEBE soportar el modo recursivo con arreglo a lo definido en [RFC 1034].

El CNP responde a las consultas sobre nombres, comenzando con información local del PS, y sus mensajes de respuesta DEBEN contener una respuesta o un error.

El CNP DEBE responder sólo a las consultas DNS dirigidas a cabhCdpServerDnsAddress.

El CNP NO DEBE responder a las consultas DNS dirigidas a las direcciones IP WAN-Man y WAN-Data del PS.

Cuando recibe una consulta inicial de resolución de nombre de anfitrión procedente de un dispositivo IP de LAN, el CNP DEBE acceder al cabhCdpLanAddrTable del CDP para consultar los nombres de anfitrión asociados a las direcciones IP de las que se ha otorgado licencia a los dispositivos IP de LAN.

Independientemente de la presencia de cualquier anotación cabhCdpWanDnsServerIP en cabhCdpWanDnsServerTable del CDP, si el CNP puede resolver el nombre del anfitrión a partir de datos locales, el CNP DEBE responder a la consulta de resolución de nombre del anfitrión con la dirección IP del dispositivo IP de LAN nombrado.

Si el CNP no puede determinar el nombre de anfitrión consultado a partir de los datos locales, Y está ocupado el cuadro cabhCdpWanDnsServerTable del CDP con por lo menos una anotación cabhCdpWanDnsServerIp, el CNP DEBE tratar de resolver la consulta mediante consultas recursivas a los servidores DNS externos, comenzando con los servidores DNS representados por la anotación cabhCdpWanDnsServerIp en el cuadro cabhCdpWanDnsServerTable.

Si el CNP no puede determinar el nombre de anfitrión a partir de los datos locales, Y no hay anotaciones cabhCdpWanDnsServerIp en el cuadro cabhCdpWanDnsServerTable, el CNP DEBE

responder a la consulta de determinación del nombre de anfitrión con el error adecuado que se especifica en RFC 1035.

El CNP DEBE responder a las consultas DNS del tipo QCLASS = IN y QTYPE = A, NS, SOA o PTR.

Las respuestas del CNP a las consultas DNS DEBEN respetar la sección 3.3 de RFC 1035, con el bit de respuesta autorizada de la sección de cabecera igual a '1' (véase la sección 4.1.1 de RFC 1035).

Como el CNP es un servidor DNS autorizado del sector LAN-Trans, DEBE proporcionar registros de comienzo de autoridad (SOA) y servidor de nombres autorizado (NS) a petición. Los campos del registro SOA (véase la sección 3.3.13 de RFC 1035) DEBEN contener una entrada para el campo MNAME que sea igual al valor del objeto de la MIB cabhCdpServerDomainName del CDP.

Aunque no se haya fijado cabhCdpServerDomainName, el CNP DEBE proporcionar servicio de referencia DNS a los dispositivos IP de LAN.

10 Calidad de servicio

10.1 Introducción

Esta cláusula describe la función del entorno de IPCable2Home para permitir que las aplicaciones de red doméstica utilicen los recursos QoS IPCablecom y DOCSIS. Estos recursos constituyen un mecanismo de gestión que otorga prioridades a los flujos de la sesión de datos para soportar tráfico de aplicaciones en tiempo real, tales como VoIP, secuencias A/V y videojuegos, mediante la reducción de la latencia de los paquetes y de los retardos de la fluctuación de fase. Los mecanismos QoS IPCablecom y DOCSIS proporcionan asimismo mayor eficacia a la gestión del tráfico en toda la red HFC.

La QoS define los requisitos necesarios del elemento PS que permiten a las aplicaciones IPCablecom establecer diversos niveles de QoS en la red HFC.

10.1.1 Objetivos

Entre los objetivos de la QoS se encuentran:

- Conseguir que las aplicaciones de red doméstica establezcan sesiones de datos de distinta prioridad entre el CMTS y el dispositivo PS que utiliza la mensajería homologada con IPCablecom.
- Facilitar el diseño y las pruebas en condiciones de explotación que conduzcan a la fabricación e interfuncionamiento de soportes físicos y lógicos homologados por diversos fabricantes.

10.1.2 Hipótesis

Se han establecido las siguientes hipótesis para la QoS de IPCable2Home:

- La QoS supone la existencia de sistemas J.112 e IPCablecom en la red de cable.
- Para evitar problemas con las funciones NAT del elemento CAP, las aplicaciones homologadas con IPCablecom utilizan el direccionamiento LAN-Pass definido en las cláusulas 7 y 8.

10.2 Arquitectura de la QoS

La arquitectura de la calidad de servicio del cable (CQoS, *cable quality of service*) está integrada por elementos funcionales de IPCable2Home y por la clase de dispositivo HA. Los diseñadores de equipos de red de IPCable2Home (tanto de soporte físico como de soporte lógico) implementan uno o más de estos elementos en función del conjunto de características que se desea exhiban dichos productos. Se requiere la especificación de conjuntos de capacidades mínimos para participar en el dominio CQoS. Los elementos CQoS básicos se presentan en 10.2.2.

10.2.1 Directrices de diseño del sistema

Las directrices de diseño del sistema QoS de IPCable2Home se relacionan en el cuadro 10-1.

Cuadro 10-1/J.191 – Directrices de diseño del sistema QoS de IPCable2Home

Número	Directrices de diseño del sistema QoS
QoS 1	Existirá un mecanismo de señalización normal QoS que permita a los dispositivos domésticos de pasarela (HA) soportar el establecimiento de sesiones de servicio de diferentes prioridades en la red DOCSIS para aplicaciones multimedia.
QoS 2	Las aplicaciones multimedia pueden estar integradas en el dispositivo HA o en un dispositivo externo conectado mediante una tecnología de red doméstica.
QoS 4	La CQoS 1.0 debe soportar las configuraciones de HA de PS integrado y autónomo.
QoS 5	Las aplicaciones multimedia pueden incorporar servicios IPCablecom (E-MTA/S-MTA).

10.2.2 Descripción del sistema de la QoS

La arquitectura CQoS se compone de las siguientes entidades:

- Dominio CQoS.
- Función de servicios de portal (PS).
- Función de portal de calidad de servicio de IPCable2Home (CQP).
- Dispositivo HA.
- CMTS.

El dominio CQoS define la esfera de influencia directa de la funcionalidad CQoS, que alcanza al dispositivo HA desde la cabecera de la red de cable. Los elementos PS y CQP pertenecen totalmente al dominio CQoS y son objeto de especificación. El dominio CQoS existe para prestar servicios a las aplicaciones homologadas con IPCablecom.

La arquitectura de referencia describe asimismo el dispositivo HA. Véase la cláusula 5.

El sistema de terminación del módem de cable (CMTS, *cable modem termination system*) está situado en la cabecera de la red de cable y gestiona las funciones QoS DOCSIS.

10.2.2.1 El elemento de servicios de portal

El elemento de servicios de portal (PS) es un elemento lógico que dispone de direccionamiento, gestión y seguridad de red, y componentes QoS del portal que proporcionan funciones de traducción entre la red HFC y la red doméstica. El PS sólo reside en los dispositivos HA (véase la cláusula 5). El componente QoS recibe el nombre de portal de calidad de servicio del cable (CQP, *cable qualtiy-of-service portal*).

10.2.2.1.1 Componente CQP

El elemento PS incorpora un componente de portal de calidad de servicio del cable (CQP), que desempeña la función de un portal CQP para aplicaciones conformes a IPCablecom. Su función primordial es retransmitir los mensajes de QoS entre el CMTS y las aplicaciones de IPCablecom.

10.2.2.1.2 Configuración del PS autónomo

En esta Recomendación no se determinan los requisitos de QoS entre un PS y un CM, y por consiguiente no se describen las funciones necesarias para mantener las prioridades de la sesión de datos y para evitar la contienda debido al acceso asíncrono de múltiples dispositivos. Es recomendable que esta interfaz sea una conexión PS a CM dedicada (es decir, que no se comparte con otros dispositivos) con un gran ancho de banda, para reducir la fluctuación de fase de los paquetes de QoS producida por la contienda de múltiples dispositivos.

10.2.2.2 Dominio CQoS

El dominio CQoS existe independientemente para cada hogar. Los hogares individuales son autónomos y tienen dominios CQoS independientes. El elemento CQP restringe el dominio CQoS a un hogar determinado.

10.2.2.3 Clases de dispositivos físicos y elementos funcionales CQoS

Los dispositivos HA están integrados por el elemento lógico PS y el elemento funcional CQP. El CQP actúa transparentemente de puente para los mensajes QoS de las aplicaciones IPCablecom (APP). La figura 10-1 muestra un ejemplo de las relaciones entre los elementos funcionales CQoS y la clase de dispositivo HA.

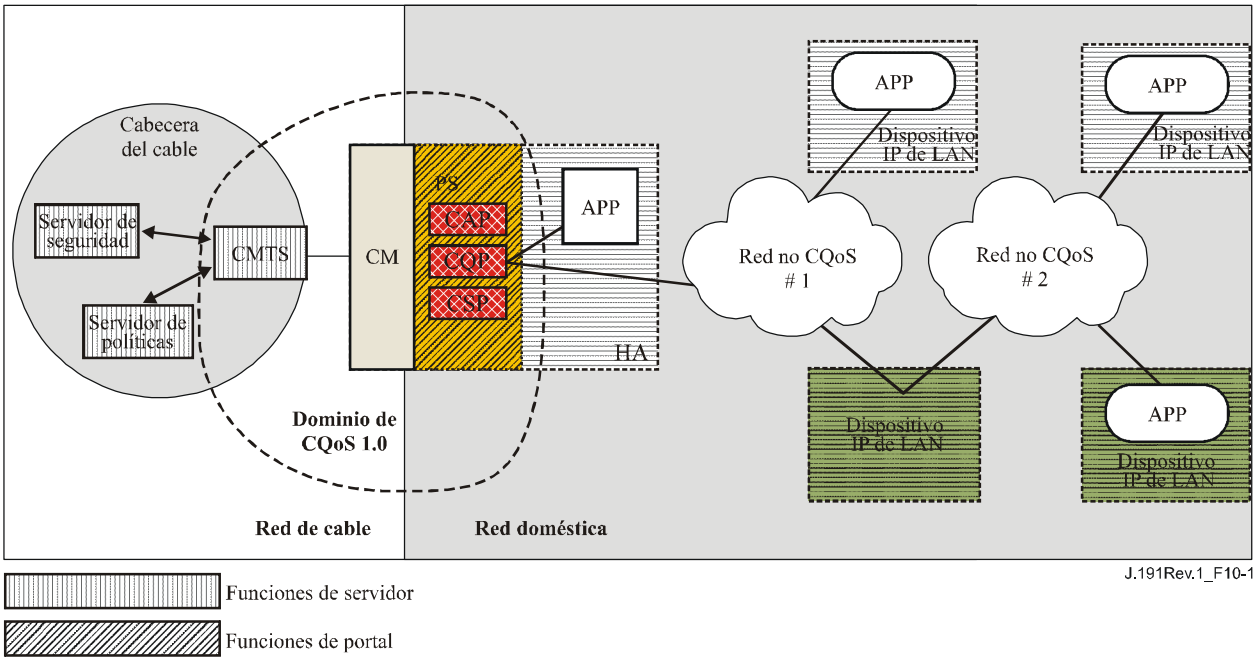


Figura 10-1/J.191 – Ejemplo de elementos funcionales de CQoS

10.3 Requisitos de la mensajería QoS de cable

La arquitectura QoS de IPCable2Home (CQoS) está integrada por el elemento funcional CQP del dominio CQoS. El CQP existe en el PS y soporta la entrega de mensajes QoS a través de la red HFC para aplicaciones IPCablecom. La mensajería homologada con IPCablecom incluye los mensajes QoS y otros mensajes relativos a aspectos específicos del servicio tales como las decisiones políticas y la aplicación de los modelos de reserva de dos fases.

En las siguientes subcláusulas se definen los requisitos funcionales del CQP y demás elementos CQoS.

10.3.1 Requisitos del CQP

El CQP DEBE actuar como puente transparente y entregar los mensajes QoS IPCablecom J.161 y J.163 entre el CMTS y las aplicaciones IPCablecom. Los datos de la aplicación se asocian a un flujo de servicio DOCSIS de acuerdo con un clasificador creado en la interfaz CM a partir de la información contenida en los mensajes IPCablecom (tales como RSVP PATH).

Como el requisito del CQP es solamente entregar los mensajes QoS IPCablecom, no hay dependencia del NMS para soportar esta función. Por consiguiente, esta función CQP se mantiene idéntica tanto en el modo de configuración DHCP como en el modo de configuración SNMP (véase 5.5).

10.3.2 Gestión de la política del QoS y control de admisión

La mensajería QoS de IPCable2Home se define en las especificaciones IPCablecom (Recs. UIT-T J.161 y J.163). Por este motivo, las funciones de gestión de políticas del QoS y de control de la admisión de IPCable2Home se definen asimismo en esas Recomendaciones IPCablecom.

11 Seguridad

11.1 Introducción y presentación

En esta cláusula se definen las interfaces de seguridad, protocolos y requisitos funcionales necesarios para la entrega fiable de servicios IP basados en cable al HA en un entorno seguro.

Para poder prestar servicios IP multimedia fiables a los dispositivos clientes en la red doméstica se necesita un mecanismo seguro que los proteja frente a los accesos, supervisión y perturbación ilegales. El objeto de las tecnologías de seguridad es la protección del valor de los activos de información susceptibles de compra o fuentes de ingresos de cualquier tipo. Las amenazas a estas fuentes de ingresos se presentan cuando un usuario de la red obtiene el valor, invierte trabajo y capital e inventa una técnica para evitar pagar lo necesario (véase el anexo C). Ciertos usuarios de la red hacen denodados esfuerzos para cometer robos cuando detectan elementos de gran valor. La incorporación de tecnologías de seguridad para proteger los elementos valiosos supone un cierto costo; cuanto más dinero se invierte mayor es la seguridad (la eficacia de la seguridad se basa de este modo en criterios económicos básicos).

11.1.1 Objetivos

Entre los objetivos del modelo de seguridad se encuentran:

- Utilizar una tecnología de seguridad rentable que obligue a los usuarios que intenten robar o perturbar los servicios de la red a invertir una cantidad exagerada de tiempo o dinero.
- Asegurar las conexiones en el hogar que permitan la configuración de servicios de valor elevado basados en cable, de modo que sean como mínimo tan seguros como las tecnologías de módem de cable e IPCablecom en la red híbrida fibra-coaxial (HFC, *hybrid fibre coax*).
- Proporcionar mecanismos de seguridad flexibles que sean compatibles con los mecanismos de seguridad de módem de cable e IPCablecom utilizados en la red HFC.

11.1.2 Hipótesis

Entre las hipótesis del entorno de seguridad de IPCable2Home se encuentran las siguientes:

- Se supone que en el HA integrado, es decir, un PS/CM contenido en un solo dispositivo físico, el CM es un módem de cable J.112 (o J.122).

- Pueden existir niveles de seguridad inferiores en la red doméstica cuando los servicios prestados se consideren de escaso valor.

11.2 Arquitectura de seguridad

La arquitectura de seguridad se basa en la arquitectura general definida en la cláusula 5. La arquitectura define un elemento de servicios de portal (PS), que incluye las funciones de gestión y configuración, seguridad y QoS.

La arquitectura incluye asimismo un conjunto de elementos de la cabecera. Entre éstos se encuentran el sistema de terminación de módem de cable (CMTS), el servidor de protocolo dinámico de configuración de anfitrión (DHCP, *dynamic host configuration protocol*), el sistema de gestión de la red, el servidor de seguridad, etc.

La especificación se centra en la definición, funcionalidad e interfaces de las funciones de seguridad y de los servidores de cabecera relacionados con la seguridad.

11.2.1 Directrices de diseño del sistema

Los requisitos de diseño de la seguridad se relacionan en el cuadro 11-1. Esta relación proporciona una orientación para el desarrollo de las especificaciones de seguridad.

Cuadro 11-1/J.191 – Directrices de diseño del sistema de seguridad de IPCable2Home

Referencia	Directrices de diseño del sistema de seguridad
SEC1	El operador podrá gestionar a distancia productos barrera contra fuegos homologados.
SEC2	En el diseño del sistema de seguridad se incluirá una interfaz de registro histórico de eventos y de mensajería de la barrera contra fuegos que permita al operador supervisar y analizar la actividad de la barrera contra fuegos.
SEC3	Los mensajes de gestión de la barrera contra fuegos intercambiados entre la cabecera de cable y el PS se autenticarán y opcionalmente se criptarán para protegerlos de la supervisión o control no autorizados.
SEC4	Se incluirá en el diseño del sistema la autenticación recíproca de elementos.
SEC5	El nivel de seguridad del hogar será tal que no sea fácil para un abonado ordinario tener acceso no autorizado a la red HCC y a los servicios basados en cable.
SEC6	Una vez establecida una cuenta de abonado, la autenticación del PS con el sistema de configuración del operador será automática.
SEC7	El operador tendrá la posibilidad de descargarse con seguridad imágenes de programas informáticos, ficheros de configuración y conjuntos de reglas de barrera contra fuegos para el elemento PS.
SEC8	La seguridad de IPCable2Home proporcionará el soporte necesario para la DQoS con seguridad IPCablecom a través de la barrera contra fuegos.
SEC9	Los mensajes de gestión de la red intercambiados entre la cabecera de cable y el PS se autenticarán y opcionalmente se criptarán para protegerlos de la supervisión y control no autorizados.

El contenido de esta cláusula se limita a estos requisitos primarios de la seguridad del sistema, reconociendo no obstante de que en ciertos casos puede ser conveniente utilizar medidas de seguridad adicionales. Cuestiones peculiares de los operadores y de los fabricantes pueden hacer que se creen más medidas de protección de seguridad. Esta Recomendación no restringe la utilización de protección adicional siempre que no entre en conflicto con el propósito y las directrices de la presente Recomendación.

11.2.2 Descripción del sistema

Esta cláusula proporciona un resumen de todos los elementos que integran la arquitectura de seguridad.

La arquitectura de seguridad está compuesta por los siguientes elementos de seguridad:

- Dominio de seguridad.
- Función de servicios de portal (PS).
- Función de portal de seguridad de cable (CSP).
- Barrera contra fuegos (FW).
- Servidor de seguridad (centro de distribución de claves (KDC, *key distribution centre*)).

El dominio de seguridad define la frontera de la esfera de influencia directa en la que la funcionalidad de seguridad se extiende desde la cabecera de la red de cable hasta el PS. Los elementos PS, CSP y FW están totalmente integrados en el dominio de seguridad. El elemento PS contiene funciones de direccionamiento de la red, gestión y funciones del portal de seguridad. El CSP se comporta como el elemento frontera entre el dominio de seguridad y el dominio no seguro. El dominio de seguridad existe para prestar servicios de seguridad a los dispositivos homologados.

Estos elementos contienen la funcionalidad específica de cliente, servidor o de portal y pueden existir en diversos tipos de dispositivos físicos. La arquitectura define una clase de dispositivo de acceso a la vivienda (HA). La figura 11-1 contiene un ejemplo de la relación entre los distintos elementos de seguridad y las clases de dispositivo HA. En la figura 11-1, las aplicaciones del hogar se representan como APP y el servidor OSS es el servidor NMS.

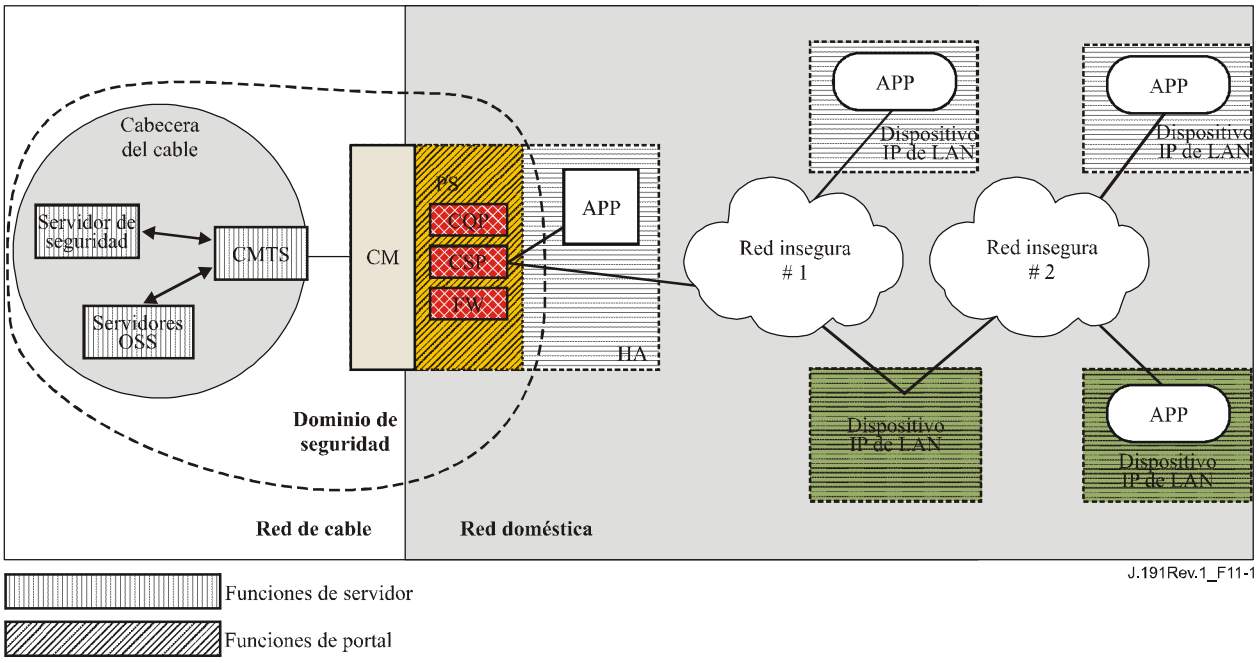


Figura 11-1/J.191 – Elementos de seguridad de IPCable2Home

11.2.2.1 El dominio de seguridad

El dominio de seguridad se define en la figura 11-1 y comprende el elemento PS del HA y los servidores de cabecera que se ilustran.

11.2.2.2 La función PS – Servicios de portal

El servicio de portal (PS) es un elemento lógico dotado de funciones de direccionamiento de la red, gestión y portal de seguridad, que sólo reside en los dispositivos HA. El PS está integrado por los siguientes elementos:

- Portal de seguridad de cable (CSP).
- Barrera contra fuegos (FW).

El CSP se comporta como un portal de seguridad para otros elementos PS. Una de sus funciones primordiales es efectuar la entrega de los mensajes de seguridad intercambiados entre los servidores OSS de cabecera (entre ellos el servidor de seguridad) y las aplicaciones IPCablecom. El CSP presta asimismo servicios de seguridad al elemento PS tales como la autenticación y la gestión de claves.

Además, el PS incluye la funcionalidad de barrera contra fuegos. La barrera contra fuegos protege al usuario y la red HFC del tráfico indeseado proveniente de los dominios WAN o LAN. Dicho tráfico puede contener ataques deliberados contra la red doméstica así como limitaciones de tráfico para aplicaciones de control paternal.

La especificación de seguridad no describirá detalladamente la implementación de una barrera contra fuegos, sino que se limitará a definir un conjunto de requisitos que permita la gestión del operador a distancia.

Las barreras contra fuegos se suelen construir utilizando una combinación de dos elementos distintos: filtrado de paquetes y servidor apoderado. El módulo de filtrado de paquetes es con toda seguridad el componente más común de la barrera contra fuegos porque determina las secuencias de paquetes que han de bloquearse y aquéllas a las que se permite atravesar la barrera contra fuegos. Las decisiones específicas de rechazo de paquetes se basan en información de configuración estática que obliga a inspeccionar los campos de cabecera del paquete, especialmente: las direcciones IP de origen y destino, los números de puerto de protocolo de origen y destino, el tipo de protocolo, etc. Dependiendo del nivel de seguridad deseado en una barrera contra fuegos, puede ser necesario configurar un número mayor de filtros, lo que puede revestir cierta complejidad y exigir un conocimiento profundo del tipo de servicios (protocolos) que han de filtrarse.

Un apoderado específico de la aplicación (ASP, *application-specific proxy*), otro componente típico de la barrera contra fuegos, crea un punto extremo del protocolo y su enlace mediante la implementación de las partes cliente y servidor necesarias de un protocolo cliente-servidor específico. La utilización de ASP comporta ciertos beneficios de seguridad. Por ejemplo, permite añadir una lista de control de acceso a los protocolos, requiriendo de los usuarios o de los sistemas cierto grado de autenticación antes de otorgar el acceso. Por otra parte, al ser específico del protocolo, el ASP entiende el protocolo y puede configurarse para bloquear exclusivamente ciertas subsecciones del protocolo. Por ejemplo, un FTP ASP puede configurarse para bloquear el tráfico procedente de usuarios no autenticados, concediendo a los usuarios autenticados acceso selectivo a los mandatos "put" y "get", es decir dependiendo de las direcciones desde las que se emiten dichos mandatos.

La combinación específica de filtros de paquete y de ASP en un producto barrera contra fuegos determinado constituye un compromiso entre la calidad de funcionamiento y el nivel de seguridad de la barrera contra fuegos. Al tratarse normalmente de un mecanismo de la capa de red, es probable que el filtrado de paquetes ofrezca un rendimiento mejor que los ASP por ser éstos mecanismos de la capa de aplicación. Una solución de compromiso cada vez más utilizada consiste en la utilización del filtrado dinámico de paquetes (SPF, *stateful packet filtering*) donde la información acumulada del estado de los paquetes que pertenecen a la misma conexión se mantiene y se utiliza en la toma de decisiones de rechazo de paquetes.

El filtrado estático, o SPF, y los ASP de una barrera contra fuegos son en última ejemplar los controles que utiliza la política de seguridad para implementar el nivel de seguridad deseado en un sitio. No obstante, aunque la política de seguridad determina los servicios permitidos y su modo de utilización a través de una barrera contra fuegos, no define en detalle la configuración específica de la barrera contra fuegos. El conjunto de reglas derivado de la política de seguridad es el que define el conjunto de reglas de control de acceso (reglas de acción de filtrado y del apoderado) que determina, acto seguido, cuáles son los paquetes que ha de entregar la barrera contra fuegos y cuáles los que ha de rechazar. Uno de los problemas más importantes para derivar el conjunto de reglas de las sentencias de la política de seguridad es que suelen expresarse en lenguaje humano de alto nivel.

Como la barrera contra fuegos sólo necesita el conjunto de reglas para configurar sus componentes SPF y ASP, la definición de la política de seguridad y la derivación del conjunto de reglas correspondientes se consideran ajenos al propósito de la presente Recomendación. Se configura en la barrera contra fuegos un conjunto de reglas adecuado mediante la descarga de un fichero de configuración de la barrera contra fuegos autenticado. El formato real del fichero que contiene el conjunto de reglas aplicable a un producto barrera contra fuegos determinado y el modo en que dicho fichero se utiliza en la barrera contra fuegos para configurar los componentes SPF y ASP es específico de la implementación. La presente Recomendación sólo contempla los mecanismos de autenticación utilizados en la descarga de un conjunto de reglas de barrera contra fuegos para el elemento PS.

La figura 11-2 ilustra la relación entre los componentes de la barrera contra fuegos. En especial, el dibujo indica que se utilizará un conjunto de reglas (RS, *rule set*) para la configuración interna de todos los componentes de la barrera contra fuegos. Estos componentes están integrados por el filtro de paquetes entrantes (IPF, *inbound packet filter*), el filtro de paquetes salientes (OPF, *outbound packet filter*), y el apoderado específico de las aplicaciones (ASP) o las funciones de filtrado dinámico de paquetes (SPF). La figura 11-2 proporciona asimismo una visión más detallada del PS y su relación con las funciones de barrera contra fuegos y otros componentes del dispositivo HA. Concretamente, la figura indica que la función apoderado específico de la aplicación/filtrado dinámico de paquetes (ASP/SPF, *application specific proxy/stateful packet filtering*) está estrechamente asociada a la función de traducción de direcciones de la red del CAP (NAT). Como la función NAT perturba otras aplicaciones, se necesita un proceso específico de la aplicación como parte de la implementación NAT y, por consiguiente, la implementación del PS PUEDE combinar las funciones ASP/SPF y NAT.

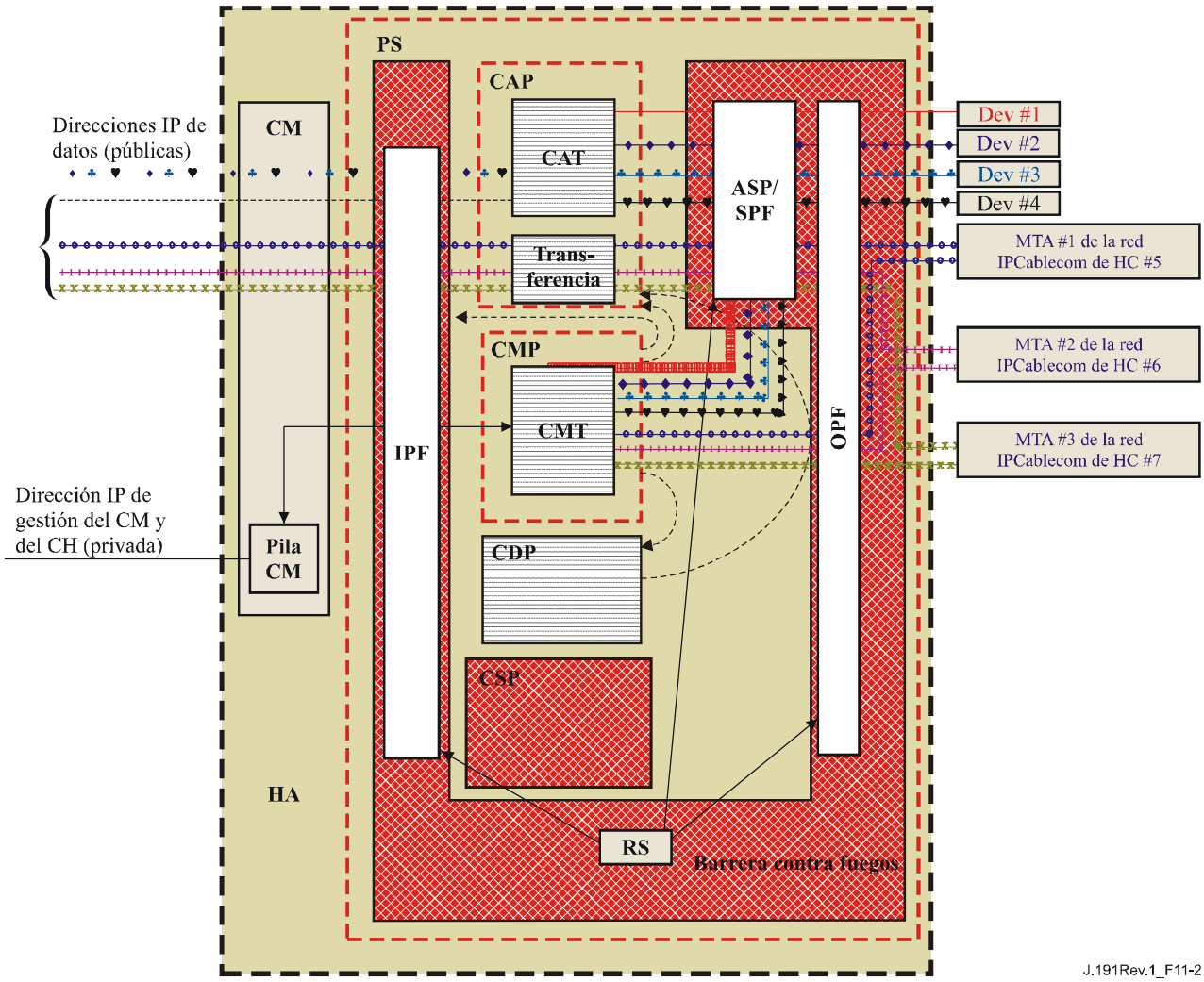


Figura 11-2/J.191 – Ejemplo de elemento PS de un dispositivo HA

11.2.3 Servidor del centro de distribución de claves (KDC)

El servidor de seguridad soportado en IPCable2Home es el servidor del centro de distribución de claves (KDC). Si hay disponible un servidor KDC que soporte IPCable2Home en la cabecera, se utilizará para prestar los servicios de autenticación y de distribución de claves utilizando el protocolo Kerberos. Si está disponible, el KDC se comunicará con la función CSP para establecer dichos servicios.

11.2.4 Otras funciones y elementos relacionados

Los siguientes no se consideran elementos de seguridad aunque utilizan o participan en la gestión de los servicios de seguridad citados.

- OSS
- CMP

El OSS representa un conjunto de servidores de cabecera que hacen posible la gestión de los elementos en el hogar. Los servidores OSS se comunican con el CMP para gestionar las funciones y servicios de seguridad. El enlace entre el OSS y el CMP se asegura con los servicios de autenticación y privacidad definidos en esta Recomendación.

El CMP es la función de gestión interior del PS. La arquitectura de seguridad presta servicios de autenticación y otros servicios de seguridad para su comunicación con los servidores OSS de la

cabecera. El CMP activa las funciones de gestión del PS y entre ellas la gestión de los servicios de seguridad.

En las cláusulas 12 y 13, y en la cláusula 10 relativa a QoS, se exponen en más detalles estos elementos y sus funciones.

11.3 Requisitos

Todas las referencias relativas a la seguridad IPCablecom pueden consultarse en la Rec. UIT-T J.170.

11.3.1 Autenticación de elementos

A efectos de seguridad, es importante conocer al interlocutor de una comunicación antes de intercambiar información de importancia. La autenticación constituye un medio de identificar con seguridad a los desconocidos que deseen establecer comunicación. La autenticación tiene tres partes, la credencial de identidad, la comprobación de la credencial de identidad a fin de validarse y los medios comunes de comunicar la información de identidad. La presente Recomendación especifica una credencial de identificación que es normal en la industria, y que consiste en la utilización de certificados X.509 junto con RFC 3280. El certificado del elemento PS proporciona la identidad del elemento PS asociado vinculando criptográficamente la dirección MAC WAN-Man del elemento PS a un certificado de clave pública. Además, los certificados de clave pública constituyen un modo seguro de comunicar la información de identidad.

Cuando un KDC que soporte esta Recomendación esté disponible en la cabecera, se soportará la autenticación. Si hay un KDC disponible, se recomienda que el operador de cable proporcione el elemento PS en el modo de configuración SNMP (descrito en 5.5) para aprovechar el protocolo de autenticación recíproco especificado utilizando Kerberos con la extensión PKINIT. Kerberos proporciona un protocolo de seguridad de la autenticación recíproca a fin de proporcionar material de clave y establecer la comunicación únicamente entre partes autenticadas de la red IPCable2Home. Como este modelo de autenticación ya ha sido especificado en otro proyecto de la UIT, es decir, IPCablecom, la presente Recomendación se referirá al modelo IPCablecom cuando proceda.

11.3.1.1 Kerberos/PKINIT

Cuando el elemento PS se proporciona en el modo de configuración SNMP, la presente Recomendación especifica la utilización de Kerberos con la extensión de clave pública PKINIT para autenticar elementos y para soportar los requisitos de la gestión de claves. Los elementos (clientes) se autentican a sí mismos ante el KDC con el protocolo PKINIT. Una vez autenticados ante el KDC, los clientes pueden recibir un tique Kerberos para autenticarse por sí mismos ante un servidor específico.

Durante el modo de configuración SNMP, el elemento PS, el NMS (es decir, el gestor SNMP) y el KDC DEBEN seguir la especificación de Kerberos/PKINIT que se describe en 6.4 y 6.5 de la Rec. UIT-T J.170, a menos que se señale lo contrario en la presente Recomendación. El KDC de IPCable2Home es equivalente al KDC de MSO de IPCablecom (IPCablecom especifica la utilización de varios KDC), o puede ser idéntico. La especificación de IPCable2Home utiliza el término sistemas de gestión de red (NMS *network management systems*) para proporcionar la funcionalidad SNMP. Al hacer referencia al conjunto de especificaciones de IPCablecom, debe observarse que IPCablecom utiliza el término servidor de configuración para indicar la funcionalidad SNMP. El lector debería tener en cuenta que en general esta funcionalidad tendrá que ser compatible con ambas especificaciones, no obstante, no son idénticas como se determina en la información específica de IPCablecom e IPCable2Home. El elemento PS DEBE desempeñar el papel de cliente ante el KDC. En la especificación de seguridad de IPCablecom el MTA es el cliente y se prevé que las aplicaciones de IPCable2Home utilizarán para el elemento PS la funcionalidad de cliente especificada para el MTA. El elemento PS emplea Kerberos para SNMP.

Los certificados utilizados en PKINIT para IPCable2Home se especifican en la sección PKI de esta Recomendación. En esta Recomendación se propone un certificado para el elemento PS (certificado del elemento PS) para aquellos casos en que IPCablecom especifica un certificado de dispositivo MTA, y las implementaciones de los elementos PS DEBEN incluir el certificado del elemento PS.

Las siguientes cláusulas de la funcionalidad de Kerberos según la Rec. UIT-T J.170 no son aplicables a esta Recomendación:

- Cláusula 6.4.8.4, Preautenticador para ubicación del servidor de aprovisionamiento.
- Cláusula 6.4.7, Nombres de principal de MTA.
- Cláusula 6.4.8, Correspondencia de dirección MAC de MTA con FQDN de MTA.
- Cláusula 6.4.10, Versión de claves de servicio.
- Cláusula 6.4.11, Operación a través de sectores Kerberos.
- Cláusula 6.5.4, Mensajes clave rehecha.
- Cláusula 6.5.6, IPSec basada en Kerberos.
- Cláusula 6.4.6, Ubicaciones de servidores Kerberos y convenios de denominación.

11.3.1.2 Variables de autenticación específicas de IPCable2Home

Las especificaciones del modelo IPCablecom establecen ciertos nombres de variables específicos para Kerberos en la arquitectura de red IPCablecom. A fin de que esta Recomendación pueda utilizar el modelo IPCablecom, DEBEN modificarse los siguientes nombres de variables:

- Sustituir pktcKdcToMtaMaxClockSkew definido en la Especificación de seguridad IPCablecom por KdcToClientMaxClockSkew.
- Sustituir pktcSrvrToMtaMaxClockSkew definido en la Especificación de seguridad IPCablecom por SrvrToClientMaxClockSkew.
- Sustituir mtaprovsrvr definido en la Especificación de seguridad IPCablecom por provsrvr.

Las implementaciones de Kerberos de IPCable2Home DEBEN ignorar la porción de campo del identificador de objeto (OID), que introduce el valor de clabProjIPCablecom (2) en AppSpecificTypedData en los mensajes KRB-ERROR.

11.3.1.3 Perfil de IPCable2Home para las ubicaciones de servidores Kerberos y convenios de denominación

Los nombres de sector Kerberos PUEDEN utilizar la misma sintaxis de un nombre de dominio, no obstante, los sectores Kerberos DEBEN indicarse únicamente en letras mayúsculas. DEBEN seguirse los detalles del sector Kerberos conformes al anexo B/J.170.

Los convenios de KDC enumerados en 6.4.5.2/J.170 se considerarán informativos en la presente Recomendación a fin de que el KDC pueda desempeñar las funciones administrativas necesarias para intercambiar la información pertinente con el NMS (servidor de configuración o gestor SNMP). El elemento PS suministra al KDC la dirección IP del servidor de configuración en la petición AS como información indispensable para establecer el contacto adecuado entre el KDC y el servidor de configuración.

Un nombre principal del elemento PS DEBE ser del tipo NT-SRV-INST exactamente con dos componentes: el primero DEBE ser la cadena "PSElement" (sin incluir las comillas) y el segundo DEBE ser la dirección WAN-Man-MAC:

PSElement/<WAN-Man-MAC>

siendo <WAN-Man-MAC> la dirección MAC de gestión de la WAN del elemento PS. El formato <WAN-Man-MAC> DEBE ser "XX:XX:XX:XX:XX:XX" (sin incluir las comillas) donde X es un

carácter hexadecimal de la dirección MAC. Los caracteres hexadecimales a-f DEBEN indicarse con minúsculas.

Un nombre principal de elemento de NMS DEBE ser del tipo NT-SRV-HST exactamente con dos componentes: el primero DEBE ser la cadena "provsrvr" (sin incluir las comillas) y el segundo DEBE ser la dirección de la entidad SNMP del proveedor de servicio:

provsrvr/<SNMP entity address>

Siendo <SNMP entity address> la dirección IP de la entidad SNMP del proveedor de servicio (subopción 3 de la opción 177 del DHCP de CDC) utilizando notación separada por puntos y entre corchetes (por ejemplo, [12.34.56.78]).

11.3.2 Infraestructura de claves públicas (PKI)

La presente Recomendación utiliza certificados de claves públicas que cumplen la Rec. UIT-T X.509 | ISO/CEI 9594-8 y RFC 3280.

11.3.2.1 Estructura genérica

11.3.2.1.1 Versión

La versión de los certificados DEBE ser Rec. UIT-T X.509 v3, al igual que se indica v2 en los certificados actuales (porque v1 no tuvo ninguna numeración de versión asociada). Todos los certificados DEBEN cumplir RFC 3280 excepto cuando se declare explícitamente la disconformidad con la RFC en esta cláusula. Las peticiones de disconformidad solicitadas para esta Recomendación en relación con el contenido no suponen la disconformidad con respecto al formato. Las solicitudes específicas de disconformidad con respecto al formato se describirán explícitamente.

11.3.2.1.2 Tipo de clave pública

Las claves públicas RSA se utilizan en las jerarquías de certificado descritas en 11.3.2.2. El OID de subjectPublicKeyInfo.algorithm utilizado DEBE ser 1.2.840.113549.1.1.1 (rsaEncryption).

El exponente público para todas las claves RSA DEBE ser $F_4 – 65537$.

11.3.2.1.3 Extensiones

Las extensiones (subjectKeyIdentifier, authorityKeyIdentifier, KeyUsage y BasicConstraints) DEBEN cumplir RFC 3280. Cualquier otra extensión de certificado PUEDE incluirse a sí mismo como no crítica. Las etiquetas de codificación son [c:crítica, n:no crítica; m:obligatoria, o:opcional] y se identifican en el cuadro para cada uno de los certificados.

11.3.2.1.3.1 subjectKeyIdentifier

La extensión subjectKeyIdentifier incluida en todos los certificados de acuerdo con lo requerido en RFC 3280 (es decir para todos los certificados con la excepción de los certificados de dispositivos y los auxiliares) DEBE incluir el valor keyIdentifier compuesto del valor de troceo SHA-1 de 160 bits de la subjectPublicKey de BIT STRING (excluyendo de la codificación ASN.1 la etiqueta, la longitud y el número de bits no utilizados) (véase RFC 3280).

11.3.2.1.3.2 authorityKeyIdentifier

La extensión authorityKeyIdentifier incluida en todos los certificados requeridos por RFC 3280 DEBE incluir el subjectKeyIdentifier del certificado del expedidor (véase RFC 3280) con excepción de los certificados raíz.

11.3.2.1.3.3 KeyUsage

La extensión keyUsage DEBE utilizarse para todos los certificados de la autoridad de certificación (CA, *certificate authority*) y certificados de verificación de código (CVC, *code verification*

certificates). Para los certificados CA la extensión keyUsage DEBE marcarse como crítica con un valor de keyCertSign y cRLSign. Para los certificados CVC la extensión keyUsage DEBE marcarse como crítica con un valor de digitalSignature y keyEncipherment. Los certificados de la entidad final pueden utilizar la extensión keyUsage como se especifica en RFC 3280.

11.3.2.1.3.4 basicConstraints

La extensión basicConstraints DEBE utilizarse para todos los certificados CA y CVC y DEBE marcarse como crítica. Los valores para cada certificado correspondientes a basicConstraints DEBEN marcarse de acuerdo con lo especificado en los cuadros de descripción de certificados 11-2 a 11-13.

11.3.2.1.4 Algoritmo de firma

El mecanismo de firma utilizado DEBE ser SHA-1 [FIPS 186-2] con criptación RSA. El OID específico es 1.2.840.113549.1.1.5.

11.3.2.1.5 SubjectName e IssuerName

Si una cadena no pudiera codificarse como PrintableString DEBE codificarse como UTF8String (etiqueta [UNIVERSAL 12]).

Al codificar un nombre X.500:

- Cada RelativeDistinguishedName (RDN) DEBE contener un único elemento del conjunto de atributos X.500.
- El orden de los RDN en un nombre X.500 DEBE ser idéntico al orden de presentación en esta Recomendación.

11.3.2.1.6 serialNumber

El número de serie DEBE ser un entero positivo y único que asigna la CA a cada certificado (es decir, el nombre del expedidor y el número de serie identifican un certificado único). Las CA DEBEN exigir que el serialNumber sea un entero no negativo. El fabricante NO DEBERÍA imponer o suponer una relación entre el número de serie del certificado y el número de serie del módem al que se expide el certificado.

Dada la singularidad de los requisitos antes señalados, se prevé que los números de serie incluirán números enteros grandes. Los usuarios de los certificados DEBEN tener la capacidad para manejar valores de serialNumber de hasta 20 octetos. Los CA conformes NO DEBEN utilizar valores de serialNumber más largos que 20 octetos.

11.3.2.2 Jerarquías de los certificados de IPCable2Home

Se utilizan tres jerarquías distintas de certificados. La cadena del fabricante se utiliza para identificar a los fabricantes autorizados; la cadena de verificación de códigos se utiliza para identificar imágenes de soporte lógico homologado y la cadena de proveedor de servicios se utiliza para identificar los dispositivos de la red del proveedor de servicios destinados a la autenticación recíproca en los dispositivos de los abonados.

Las jerarquías de certificados que se describen en esta Recomendación podrán aplicarse a todos los proyectos de la UIT que necesiten certificados. Cada proyecto puede adoptar esta jerarquía ya que es posible pasar a una estructura de certificados compartidos más genérica. Además, cada proyecto puede tener necesidad de realizar ajustes particulares de los requisitos de ese proyecto específico. El objetivo será crear una PKI que pueda reutilizarse en cada proyecto. Puede haber diferencia en los certificados de entidad final requeridos en cada proyecto, pero en los casos en los que los certificados de entidad final se solapan, un certificado de entidad final podría utilizarse para diversos servicios en la infraestructura de cable. Por ejemplo, IPCablecom requiere un KDC para el proveedor de servicios e IPCable2Home también lo necesita. Si el proveedor de servicios tiene

instaladas ambas arquitecturas de red en sus sistemas, éstas podrán utilizar el mismo KDC y el mismo certificado de KDC para la comunicación en ambos sistemas, es decir, IPCablecom e IPCable2Home. En este caso, el KDC de IPCable2Home es equivalente o idéntico al KDC de MSO de IPCablecom (IPCablecom recomienda el empleo de varios KDC).

En la figura 11-3 a continuación, el término autoridad del certificado se abrevia por CA y el certificado de verificación de códigos se abrevia por CVC.

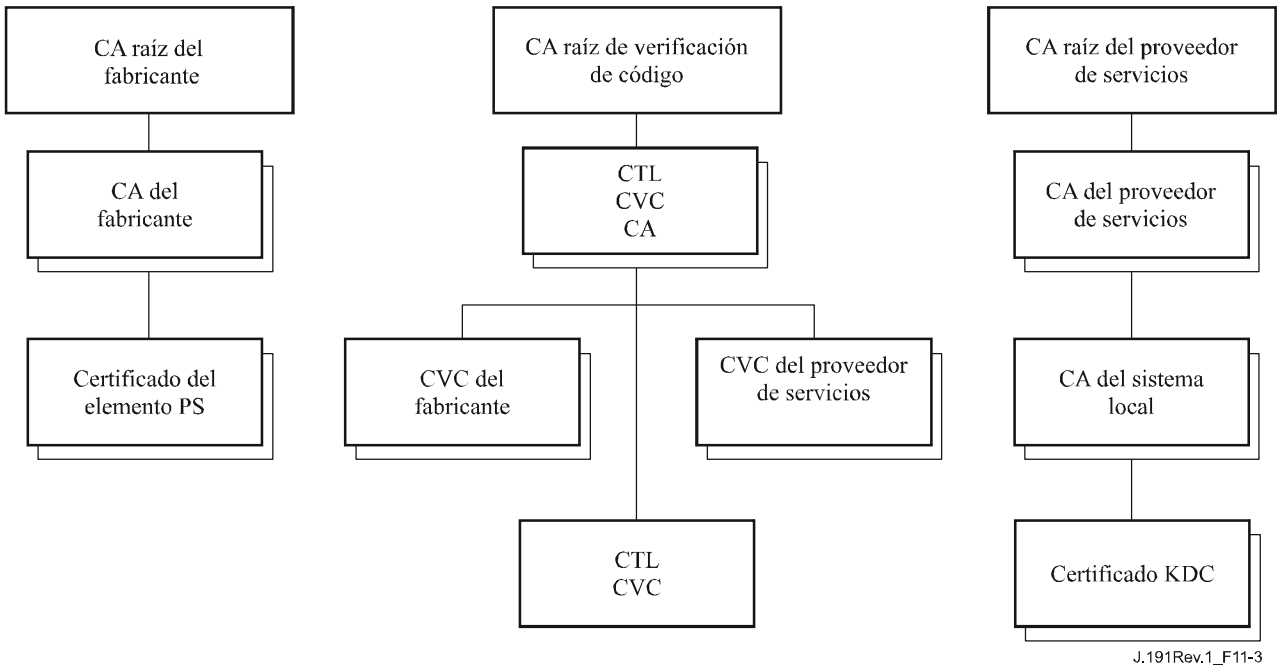


Figura 11-3/J.191 – Jerarquía del certificado de IPCable2Home

11.3.2.2.1 Jerarquía de los certificados del fabricante

La jerarquía de certificados del fabricante, o cadena del fabricante, arranca del CA raíz del fabricante, que se utiliza para emitir los certificados de autoridad de certificado (CA) del fabricante para un conjunto de fabricantes autorizados. Los fabricantes utilizan su propia CA para expedir certificados individuales de los elementos PS. Esta cadena se utiliza para la autenticación de los dispositivos en el hogar.

La información que contienen los cuadros siguientes corresponde a los valores específicos de los campos requeridos de acuerdo con RFC 3280. Estos valores específicos para la jerarquía de certificados del fabricante DEBEN respetarse de acuerdo con los cuadros 11-2 a 11-4. Si un campo requerido no está relacionado específicamente en los cuadros, DEBEN respetarse las directrices de RFC 3280. DEBEN incluirse asimismo las extensiones genéricas de acuerdo con lo especificado en la cláusula 11.3.2, PKI.

11.3.2.2.1.1 Certificado CA raíz del fabricante

El certificado CA raíz del fabricante (véase el cuadro 11-2) DEBE verificarse como parte de la cadena de certificados que contiene el certificado CA raíz del fabricante, el certificado CA del fabricante y el certificado del elemento PS.

Cuadro 11-2/J.191 – Certificado CA raíz del fabricante

Forma del nombre del sujeto	C=<país> O= CN=CA raíz del fabricante
Uso previsto	Este certificado se utiliza para expedir certificados CA de fabricante
Firmado por	Autofirmado
Periodo de validez	Superior a 20 años
Longitud del módulo	2048
Extensiones	keyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true)

11.3.2.2.1.2 Certificado CA del fabricante

El certificado CA del fabricante DEBE verificarse como parte de la cadena de certificados que contiene el certificado CA raíz del fabricante, el certificado CA del fabricante y el certificado del elemento PS.

La provincia o estado, ciudad y planta del fabricante son atributos opcionales. Un fabricante PUEDE tener más de un certificado CA de fabricante. Si un fabricante utiliza más de un certificado CA de fabricante, el elemento PS DEBE tener acceso al certificado adecuado verificado mediante confrontación del nombre del expedidor que figura en el certificado elemento PS con el nombre del sujeto en el certificado CA del fabricante. El authorityKeyIdentifier del certificado del elemento PS DEBE confrontarse con el subjectKeyIdentifier del certificado del fabricante descrito en RFC 3280.

Cuadro 11-3/J.191 – Certificado CA del fabricante

Forma del nombre del sujeto	C=<país> O=<nombre de la empresa> [S=<estado/provincia>] [L=<ciudad>] OU= [OU=<planta del fabricante>] CN=<nombre de la empresa> Mfg CA
Uso previsto	Este certificado se emite para cada fabricante por el CA raíz del fabricante y puede proporcionarse a cada elemento PS ya sea en fábrica, o durante una actualización del código en condiciones de explotación. Este certificado aparece como un parámetro de sólo lectura en la MIB del elemento PS. Este certificado expide certificados del elemento PS. Este certificado, junto con el certificado CA raíz de fabricante y el certificado del elemento PS, se utiliza para autenticar la identidad del elemento PS. La lista facultativa de la planta del fabricante puede ser el nombre y/o la ubicación de la planta.
Firmado por	CA raíz de fabricante
Periodo de validez	20 años
Longitud del módulo	2048

Cuadro 11-3/J.191 – Certificado CA del fabricante

Extensiones	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m] basicConstraints[c,m](cA=true, pathLenConstraint=0)

El nombre de la empresa en el campo Organización (O) PUEDE ser distinto del nombre de la empresa (CN, *company name*) en el campo Nombre Común.

11.3.2.2.1.3 Certificado del elemento PS

El certificado del elemento PS DEBE verificarse como parte de la cadena de certificados que contiene el certificado CA raíz del fabricante, el certificado CA del fabricante y el certificado de elemento PS.

La provincia o estado, ciudad, nombre del producto y planta del fabricante son atributos opcionales.

La dirección MAC de WAN-Man del elemento PS DEBE expresarse como seis pares de dígitos hexadecimales separados por ":", por ejemplo "00:60:21:A5:0A:23". Los caracteres HEX alpha (A-F) DEBEN expresarse en mayúsculas.

Un certificado de elemento PS se instala permanentemente y no puede renovarse ni sustituirse. Por consiguiente, el certificado de elemento PS DEBE tener un periodo de validez superior al de la vida útil prevista del dispositivo en cuestión.

Cuadro 11-4/J.191 – Certificado del elemento PS

Forma del nombre del sujeto	C=<país> O=<nombre de la empresa> [S=<Estado/provincia>] [L=<ciudad>] OU=IPCable2Home [OU=<nombre de producto>] [OU=<planta del fabricante>] CN=<dirección MAC de WAN-Man>
Uso previsto	Este certificado se emite por el CA fabricante y se instala en fábrica. El servidor NMS no puede actualizar este certificado. El certificado aparece como un parámetro de sólo lectura en la MIB del elemento PS. Este certificado se utiliza para autenticar la identidad del elemento PS.
Firmado por	CA del fabricante
Periodo de validez	Superior a 20 años
Longitud del módulo	1024, 1536, 2048
Extensiones	keyUsage[c,m](digitalSignature, keyEncipherment), authorityKeyIdentifier [n,m].

11.3.2.2.2 Jerarquía del certificado de verificación de código

La jerarquía del certificado de verificación de código (CVC), o cadena de verificación de código, arranca del CA raíz de verificación de código, que emite el certificado CA de verificación de código. El CA de verificación de código se utiliza para emitir CVC a un conjunto de fabricantes y proveedores de servicios autorizados. El CA de verificación de código emite asimismo el CVC. Esta cadena se utiliza específicamente para autenticar descargas de soporte lógico. El PKI admite para los CVC de fabricante, un CVC y un CVC de proveedor de servicios.

La información contenida en los siguientes cuadros corresponde a los valores específicos de los campos requeridos de acuerdo con RFC 3280. Estos valores específicos para la jerarquía de certificado de verificación de código DEBEN cumplirse de acuerdo con los cuadros 11-5, 11-6, 11-7, 11-8 y 11-9 a continuación. Si un campo requerido no está específicamente relacionado en los cuadros, DEBEN cumplirse las directrices de RFC 3280. Las extensiones genéricas DEBEN incluirse asimismo de acuerdo con lo especificado en la cláusula 11.3.2, PKI.

11.3.2.2.2.1 Certificado CA raíz de verificación de código

Este certificado DEBE verificarse como parte de la cadena de certificados que contiene el certificado CA raíz de verificación de código, el CA de verificación de código y los certificados de verificación de código.

Cuadro 11-5/J.191 – Certificado CA raíz de verificación de código

Forma del nombre del sujeto	C=<país> O= CN=CA raíz CVC
Uso previsto	Este certificado se utiliza para firmar certificados CA de verificación del código.
Firmado por	Autofirmado
Periodo de validez	Superior a 20 años
Longitud del módulo	2048
Extensiones	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true).

11.3.2.2.2.2 Certificado CA de verificación de código

El certificado CA de verificación de código DEBE verificarse como parte de la cadena de certificados que contiene el certificado CA raíz de verificación de código, el certificado CA de verificación de código y el certificado de verificación de código. El PS autónomo sólo DEBE soportar un CVC CA a la vez.

Cuadro 11-6/J.191 – Certificado CA de verificación de código

Forma del nombre del sujeto	C=<país> O= CN=CVC CA
Uso previsto	Este certificado se emite a un organismo de certificación por el CA raíz de verificación de código. Este certificado expide certificados de verificación de código.
Firmado por	CA raíz de verificación de código
Periodo de validez	20 años
Longitud del módulo	2048
Extensiones	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints [c,m](cA=true, pathLenConstraint=0).

11.3.2.2.2.3 Certificado de verificación de código del fabricante

Este certificado DEBE verificarse como parte de la cadena de certificados que contiene el certificado CA raíz de verificación de código, el certificado CA de verificación de código y los certificados de verificación de código.

Cuadro 11-7/J.191 – Certificado de verificación de código del fabricante

Forma del nombre del sujeto	C=<país> O=<nombre de la empresa> [S=<estado/provincia>] [L=<ciudad>] CN=<nombre de la empresa> Mfg CVC
Uso previsto	La CA de verificación de código emite este certificado a cada fabricante autorizado. Se utiliza en la política establecida por cada operador de cable para la descarga segura de soporte lógico. El nombre de la empresa en los campos O y CN puede diferir.
Firmado por	CA de verificación de código
Periodo de validez	Hasta 10 años
Longitud del módulo	1024, 1536, 2048
Extensiones	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m].

11.3.2.2.2.4 Certificado de verificación de código

El certificado de verificación de código DEBE verificarse como parte de la cadena de certificados que contiene el certificado CA raíz de verificación de código, el certificado CA de verificación de código y el certificado de verificación de código.

Cuadro 11-8/J.191 – Certificado de verificación de código

Forma del nombre del sujeto	C=<país> O= CN=CVC
Uso previsto	La CA de verificación de código emite este certificado. Se utiliza para autenticar código certificado. Se utiliza en la política establecida por el operador de cable para la descarga segura de soporte lógico.
Firmado por	CA de verificación de código
Periodo de validez	Hasta 10 años
Longitud del módulo	1024, 1536, 2048
Extensiones	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m].

11.3.2.2.2.5 Certificado de verificación de código del proveedor de servicios

El certificado de verificación de código del proveedor de servicios DEBE verificarse como parte de la cadena de certificados que contiene el certificado CA raíz de verificación de código, el certificado CA de verificación de código y el certificado de verificación de código del proveedor de servicios.

Cuadro 11-9/J.191 – Certificado de verificación de código del proveedor de servicios

Forma del nombre del sujeto	C=<país> O=<nombre de la empresa> [S=<estado/provincia>,] [L=<ciudad>,] CN=<nombre de la empresa> proveedor de servicios CVC
Uso previsto	La CA de verificación de código emite este certificado a cada uno de los proveedores de servicios autorizados. Se utiliza en la política establecida por el operador de cable para la descarga segura de soporte lógico. El nombre de la empresa en los campos O y CN puede diferir.
Firmado por	CA raíz de verificación de código
Periodo de validez	Hasta 10 años
Longitud del módulo	1024, 1536, 2048
Extensiones	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m]

11.3.2.2.3 Jerarquía de certificados del proveedor de servicios

La jerarquía de certificados del proveedor de servicios, o cadena del proveedor de servicios, arranca del CA raíz del proveedor de servicios, que se utiliza para expedir certificados para un conjunto de proveedores de servicios autorizados. La CA del proveedor de servicios puede utilizarse para expedir certificados CA del sistema local opcionales o certificados auxiliares. Si la CA del proveedor de servicios no expide certificados auxiliares entonces lo hará la CA del sistema local. Los certificados auxiliares son los certificados de la entidad final de la red del operador de cable.

La información contenida en los cuadros siguientes corresponde a los valores específicos de los campos requeridos de acuerdo con RFC 3280. Estos valores específicos para la jerarquía de certificados del proveedor de servicios DEBEN cumplirse de acuerdo con los cuadros 11-10 a 11-13, a continuación. Si un campo requerido no está específicamente relacionado en estos cuadros, DEBEN cumplirse las directrices de RFC 3280. Las extensiones genéricas DEBEN incluirse asimismo de acuerdo con lo especificado en la cláusula 11.3.2, PKI.

11.3.2.2.3.1 Certificado CA raíz del proveedor de servicios

Este certificado DEBE verificarse como parte de la cadena de certificados que contiene el certificado CA raíz del proveedor de servicios, el certificado CA del proveedor de servicios, el certificado CA del sistema local opcional y los certificados auxiliares.

Cuadro 11-10/J.191 – Certificado CA raíz del proveedor de servicios

Forma del nombre del sujeto	C=<país> O= CN=CA raíz del proveedor de servicios
Uso previsto	Este certificado se utiliza para expedir certificados CA del proveedor de servicios.
Firmado por	Autofirmado
Periodo de validez	Superior a 20 años
Longitud del módulo	2048
Extensiones	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true)

11.3.2.2.3.2 Certificado CA del proveedor de servicios

El certificado CA del proveedor de servicios DEBE verificarse como parte de la cadena de certificados que contiene el certificado CA raíz del proveedor de servicios, el certificado CA del proveedor de servicios, el certificado CA opcional del sistema local y los certificados auxiliares.

Cuadro 11-11/J.191 – Certificado CA del proveedor de servicios

Forma del nombre del sujeto	C=<país> O=<nombre de la empresa> CN=<nombre de la empresa>CA proveedor de servicios
Uso previsto	La CA raíz del proveedor de servicios emite este certificado a cada uno de los proveedores de servicios. Para facilitar la actualización de este certificado, cada uno de los elementos de red se configura con el atributo OrganizationName del SubjectName del certificado CA del proveedor de servicios. Éste es el único atributo del certificado que debe mantenerse inalterado. Este certificado aparece como un parámetro de sólo lectura en el objeto de la MIB que identifica el atributo OrganizationName para el sector Kerberos. Este elemento no acepta certificados de proveedor de servicios que no concuerden con este valor del atributo OrganizationName en el SubjectName. Si la cabecera contiene un KDC que soporta esta Recomendación, el elemento PS necesita ejecutar el primer intercambio PKINIT con el KDC justo tras un arranque, momento en el que los cuadros de la MIB aún no están configurados. En dicho momento, el cliente Kerberos DEBE aceptar cualquier atributo OrganizationalName del proveedor de servicios, pero DEBE comprobar más adelante que el valor añadido a la MIB para este sector es el mismo que el de la respuesta inicial PKINIT. Esta CA expide certificados CA del sistema local y certificados auxiliares.
Firmado por	CA raíz del proveedor de servicios
Periodo de validez	20 años
Longitud del módulo	2048
Extensiones	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=1)

El nombre de la empresa en el campo Organización (O) PUEDE ser distinto del nombre de la empresa (CN) en el campo nombre común.

11.3.2.2.3.3 Certificado CA del sistema local

Este certificado es opcional para el proveedor de servicios. Si existe este certificado DEBE verificarse como parte de la cadena de certificados que contiene el certificado CA raíz del proveedor de servicios, el certificado CA del proveedor de servicios, el certificado CA opcional del sistema local y los certificados auxiliares.

Cuadro 11-12/J.191 – Certificado CA del sistema local

Forma del nombre del sujeto	C=<país> O=<nombre de la empresa> OU=<nombre del sistema local> CN=<nombre de la empresa>CA del sistema local
Uso previsto	Este certificado es opcional y de existir lo emite la CA del proveedor de servicios. Este CA expide certificados auxiliares. Se permite a los servidores de red moverse libremente entre CA regionales del mismo proveedor de servicios.
Firmado por	CA de proveedores de servicios
Periodo de validez	20 años
Longitud del módulo	1024, 1536, 2048
Extensiones	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=0).

El nombre de la empresa en el campo Organización (O) PUEDE ser distinto del nombre de la empresa (CN) en el campo nombre común.

11.3.2.2.3.4 Certificado KDC

Este certificado DEBE verificarse como parte de la cadena de certificados que contiene el certificado CA raíz de proveedor de servicios, el certificado CA de proveedor de servicios, el certificado CA opcional del sistema local y los certificados auxiliares (por ejemplo, los certificados KDC).

El certificado KDC DEBE incluir el subjectAltName PKINIT de Kerberos como se indica en 8.2.4.1/J.170.

Cuadro 11-13/J.191 – Certificado KDC

Forma del nombre del sujeto	C=<país> O=<nombre de la empresa> [OU=<nombre del sistema local>] OU=centro de distribución de claves CN=<nombre de DNS>
Uso previsto	Este certificado se emite ya sea por la CA del proveedor de servicios o por la CA del sistema local, y se utiliza para autenticar la identidad del KDC ante los clientes Kerberos durante los intercambios PKINIT. Este certificado se entrega al elemento PS dentro de la respuesta PKINIT.
Firmado por	CA del proveedor de servicios o CA del sistema local
Periodo de validez	20 años
Longitud del módulo	1024, 1536, 2048
Extensiones	keyUsage[c,o](digitalSignature) authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>) subjectAltName[n,m] (see Annex C/J.170)

11.3.2.3 Validación de los certificados

La validación de los certificados supone la de la cadena de certificados vinculada desde los certificados de la entidad final hasta la raíz válida. Por ejemplo, la firma del certificado del elemento PS se verifica con el certificado CA del fabricante y a continuación la firma del certificado CA del fabricante se verifica con el certificado CA raíz del fabricante. El certificado CA raíz del fabricante es autofirmado y se recibe de una fuente de confianza mediante un procedimiento seguro. La clave pública presente en el certificado CA raíz del fabricante se utiliza para validar la signatura en este mismo certificado.

Las reglas exactas para la validación de la cadena de certificados DEBEN ajustarse totalmente a RFC 3280, que la denomina "validación del trayecto de los certificados". En general, los certificados X.509 soportan un generoso conjunto de reglas para determinar si el nombre del expedidor de un certificado corresponde al nombre del sujeto de otro. Las reglas son tales que puede declararse la concordancia de dos campos de nombres aunque la comparación binaria de éstos no produzca una concordancia. RFC 3280 recomienda que las autoridades de los certificados limiten la codificación de los campos de nombre de modo que una implementación pueda declarar su concordancia o discordancia mediante una comparación binaria sencilla. La seguridad de IPCable2Home se ajusta a la presente Recomendación. Por consiguiente, el campo tbsCertificate.issuer codificado en DER de un certificado DEBE coincidir exactamente con el campo tbsCertificate.subject codificado en DER del certificado expedidor. Una implementación PUEDE comparar un nombre de expedidor con un nombre de sujeto efectuando una comparación binaria de los campos tbsCertificate.issuer y tbsCertificate.subject codificados en DER.

La validación de los periodos de validez de jerarquización no se comprueba ni se prescribe, a propósito, lo que es conforme con las normas actuales. En el momento de su expedición, la fecha de comienzo de la validez de cualquier certificado de entidad final DEBE coincidir o ser posterior con la fecha de comienzo del periodo de validez del certificado CA expedidor. Una vez renovado un certificado CA, las fechas de comienzo de los certificados de la entidad final PUEDEN ser anteriores a la fecha de comienzo del certificado CA expedidor. La fecha final de validez para las entidades puede ser anterior, idéntica o posterior a la fecha final de validez para la CA expedidora de acuerdo con lo especificado en los cuadros del certificado.

11.3.2.3.1 Validación de la cadena del fabricante y de la verificación raíz

El KDC DEBE validar la cadena vinculada de certificados del fabricante. El primer certificado de la cadena no suele incluirse explícitamente en la cadena de certificados que se envía por el cable. En los casos en que el certificado CA raíz del fabricante se incluye explícitamente en el cable ya DEBE ser conocido por la parte verificante antes del momento de verificación de este certificado. El certificado CA raíz del fabricante enviado por el cable NO DEBE contener modificaciones al certificado con la posible excepción del número de serie del certificado, el periodo de validez y el valor de la firma. Si hay modificaciones, distintas del número de serie del certificado, su periodo de validez o el valor de la firma, en el certificado CA raíz del fabricante que se recibió por el cable en comparación con el certificado CA raíz del fabricante conocido, el KDC que establece la comparación DEBE dar por fallida la verificación del certificado.

11.3.2.3.2 Validación de la cadena de verificación de código y de la verificación raíz

Un servidor interno puede comprobar la validez de la cadena de verificación de códigos antes de comenzar el proceso de descarga del soporte lógico. Los detalles se pueden consultar en 11.3.7.

11.3.2.3.3 Validación de la cadena del proveedor de servicios y de la verificación raíz

El elemento PS DEBE validar la cadena vinculada de certificados del proveedor de servicios. El primer certificado de la cadena no suele incluirse explícitamente en la cadena de certificados que se envía por el cable. En los casos en que el certificado CA raíz del proveedor de servicios se incluye explícitamente por el cable, DEBE ser conocido a la parte verificante antes de la verificación de este certificado. El certificado CA raíz del proveedor de servicios NO DEBE contener modificaciones del certificado con la posible excepción del número de serie del certificado, su periodo de validez y el valor de la firma. Si hay modificaciones distintas del número de serie del certificado, del periodo de validez y del valor de la firma, en el certificado CA raíz del proveedor de servicios transmitido por el cable con respecto al certificado CA raíz del proveedor de servicios conocido, el elemento PS que hace la comparación DEBE dar por fallida la verificación del certificado.

11.3.2.4 Revocación de certificados

La revocación de certificados queda en estudio.

11.3.3 Mensajería de gestión segura

El algoritmo de seguridad utilizado para inicializar la mensajería de gestión SNMP depende del modo de configuración del elemento PS (véase 5.5). Hay dos tipos de modo de configuración: el modo de configuración DHCP y el modo de configuración SNMP. El modo de configuración DHCP tiene submodos adicionales que identifican si está configurado para el modo NmAccess o para el modo de coexistencia. El modo de configuración SNMP requiere SNMPv3 para la mensajería de gestión.

Las subcláusulas siguientes describen los algoritmos de seguridad y requisitos necesarios para inicializar la mensajería de gestión SNMP en base al modo de configuración del elemento PS. El elemento PS DEBE soportar los algoritmos de seguridad SNMPv3 especificados en 11.3.3.1.2 y 11.3.3.2.

11.3.3.1 Algoritmos de seguridad para SNMP en el modo de configuración DHCP

El modo de configuración DHCP, el elemento PS puede configurarse para el modo NmAccess o para el modo de coexistencia. En el modo de coexistencia el elemento PS puede configurarse para la mensajería de gestión SNMPv1, SNMPv2 y/o SNMPv3.

11.3.3.1.1 El modo NmAccess

Si el elemento PS se provee en el modo de configuración DHCP con el modo NmAccess, la gestión de la red basada en SNMP dentro del elemento PS no utiliza SNMPv3 y por consiguiente no necesita inicializar las funciones de seguridad SNMPv3. La inicialización del enlace de gestión SNMPv1/v2 se define en 6.3.6.1.

11.3.3.1.2 Modo de coexistencia

Si el elemento PS se presta en el modo de configuración DHCP con el modo de coexistencia y se determina que el protocolo de mensajería de gestión es SNMPv3 (véase 6.3.6.1), el elemento PS DEBE utilizar la seguridad SNMPv3 especificada en RFC 3414. La autenticación SNMPv3 DEBE estar activa en todo momento y PUEDE utilizarse asimismo la privacidad SNMPv3.

A fin de establecer las claves SNMPv3 todas las interfaces SNMP DEBEN utilizar la inicialización SNMPv3 y el procedimiento de modificaciones de claves que se describe a continuación.

Para soportar la inicialización SNMPv3 y las modificaciones de claves, el elemento PS DEBE ser asimismo capaz de recibir TLV de los tipos 34, 34.1 y 34.2 definidos en B.C.1.2.8/J.112 e implementar el mecanismo de modificación de claves especificado en RFC 2786 que incluye el objeto de la MIB usmDHKickstartTable.

11.3.3.1.2.1 Inicialización de SNMPv3

Para cada uno de hasta 5 nombres de seguridad distintos, la autorización final (administrador del PS) genera un par de números. En primer lugar, el administrador del PS genera un número aleatorio Rm.

A continuación, el administrador de CH utiliza la ecuación DH para traducir Rm a un número público z. La ecuación es la siguiente:

$$z = g \text{ ^ } Rm \text{ MOD } p$$

siendo g parte del conjunto de parámetros Diffie-Hellman, y p es el número primo de dichos parámetros.

El fichero de configuración PS se crea para incluir el par (nombre de seguridad, número público). El PS DEBE soportar 5 pares como mínimo. Por ejemplo:

TLV tipo 34.1 (SNMPv3 Kickstart Security Name) = administrador del PS

TLV tipo 34.2 (SNMPv3 Kickstart Public Number) = z

El PS DEBE soportar las anotaciones VACM que se definen en 6.3.6.3. Sólo DEBEN estar activas las anotaciones VACM especificadas por el nombre de seguridad correspondiente en el fichero de configuración del PS.

Los valores anteriores (nombre de seguridad, número público) DEBEN rellenarse en usmDHKickstartTable, durante el proceso de rearranque del PS.

En este momento:

```
usmDHKickstartMgrpublic.1 = "z" (cadena de octetos)
usmDHKickstartSecurityName.1 = "administrador PS"
```

Cuando usmDHKickstartMgrpublic.n se fija a un valor válido durante el proceso de registro, se crea una fila correspondiente en usmUserTable con los valores:

```
usmUserEngineID: localEngineID
usmUserName: usmDHKickstartSecurityName.n value
usmUserSecurityName: usmDHKickstartSecurityName.n value
usmUserCloneFrom: ZeroDotZero
usmUserAuthProtocol: usmHMACMD5AuthProtocol
```

```
usmUserAuthKeyChange: (derived from set value)
usmUserOwnAuthKeyChange: (derived from set value)
usmUserPrivProtocol: usmDESPrivProtocol
usmUserPrivKeyChange: (derived from set value)
usmUserOwnPrivKeyChange: (derived from set value)
usmUserPublic
usmUserStorageType: permanente
usmUserStatus: activo
```

NOTA – En el caso de las anotaciones (PS) dhKickstart en usmUserTable, permanente significa que las mismas DEBEN escribirse pero no suprimirse y que no se conservan durante los rearranques.

Después de que el PS completa la inicialización (indicada mediante un valor de '1' (pase) para cabhPsDevProvState):

1) El PS genera un número aleatorio xa para cada fila ocupada en usmDHKickstartTable que tenga una longitud distinta de cero usmDHKickstartSecurityName y usmDHKickstartMgrPublic.

2) El PS utiliza la ecuación DH para traducir xa a un número público c (en cada fila identificada anteriormente).

$$c = g \text{ ^ } xa \text{ MOD } p$$

siendo g parte del conjunto de los parámetros Diffie-Hellman y p el número primo de esos parámetros.

En este momento:

```
usmDHKickstartMyPublic.1 = "c" (cadena de octetos)
usmDHKickstartMgrPublic.1 = "z" (cadena de octetos)
usmDHKickstartSecurityName.1 = "administrador del PS"
```

3) El PS calcula el secreto compartido sk siendo sk = z ^xa mod p.

4) El PS utiliza sk para deducir las claves de privacidad y de autenticación de cada fila en usmDHKickstartTable y fija los valores en usmUserTable.

Tal y como se especificó en RFC 2786, las claves de privacidad y de autenticación para el username asociado, "PS Administrator" en este caso, se deducen a partir de sk aplicando la función de deducción de claves PBKDF2 definida en PKCS#5 v2.0.

```
privacy key <---     PBKDF2 (salt = 0xd1310ba6,
                     iterationCount = 500,
                     keyLength = 16,
                     prf = id-hmacWithSHA1)
authentication key <----      PBKDF2 (salt = 0x98dfb5ac,
                     iterationCount = 500,
                     keyLength = 16 (usmHMACMD5AuthProtocol),
                     prf = id-hmacWithSHA1)
```

En este momento el PS (CMP) ha completado su proceso de inicialización de SNMPv3 y DEBE permitir el nivel de acceso adecuado a un securityName válido con la clave de autenticación y/o privacidad correcta.

El PS DEBE rellenar adecuadamente las claves en los cuadros adecuados según se indica en las normas RFC relacionadas con SNMPv3 y en RFC 2786.

5) A continuación se describe el proceso que emplea el gestor para deducir las claves de autenticación única del PS y de privacidad.

El gestor del SNMP accede al contenido de usmDHKickstartTable empleando el nombre de seguridad 'dhKickstart' sin autenticación.

El PS DEBE suministrar anotaciones preinstaladas en el cuadro USM y en los cuadros VACM para crear apropiadamente el usuario 'dhKickstart' del nivel de seguridad noAuthNoPriv que tiene acceso de sólo lectura al grupo de sistema y a usmDHkickstartTable.

Si el PS se encuentra en el modo de coexistencia y se configura para que utilice SNMPv3 la especificación de grupo para la vista dhKickstart DEBE implementarse de la siguiente manera:

```
dhKickstart Group
vacmGroupName 'dhKickstart'
vacmAccessContextPrefix ''
vacmAccessSecurityModel 3 (USM)
vacmAccessSecurityLevel NoAuthNoPriv
vacmAccessContextMatch exact
vacmAccessReadViewName 'dhKickstartView'
vacmAccessWriteViewName
vacmAccessNotifyViewName
vacmAccessStorageType permanent
vacmAccessStatus active
```

La vista VACM para la vista dhKickstart DEBE implementarse de la siguiente manera:

dhKickstartView subárbol 1.3.6.1.2.1.1 (Grupo de sistema) y 1.3.6.1.3.101.1.2.1 (usmDHKickstartTable)

El gestor de SNMP obtiene el valor del número usmDHKickstartMypublic del PS asociado con el securityName para el cual el gestor desea deducir claves de autenticación y de privacidad. Utilizando el número aleatorio privado, el gestor podrá calcular el secreto compartido DH. A partir de este último, el gestor puede deducir las claves de autenticación y confidencialidad funcionales para el securityName que el gestor utilizará para comunicarse con el PS.

11.3.3.1.2.2 Modificaciones de la clave Diffie-Hellman

El PS DEBE soportar el mecanismo de modificación de clave especificado en RFC 2786.

11.3.3.2 Algoritmos de seguridad para SNMPv3 en el modo de configuración SNMP

Si el elemento PS se provee en el modo de configuración SNMP, la gestión de red basada en SNMP del interior del elemento PS DEBE funcionar con SNMPv3 con la seguridad especificada por RFC 3414. La autenticación SNMPv3 DEBE estar activa en cualquier instante y la privacidad SNMPv3 PUEDE utilizarse asimismo. Para poder establecer claves SNMPv3, todas las interfaces SNMP de IPCable2Home DEBEN utilizar la gestión de claves SNMPv3 kerberizada, especificada en la cláusula 11.3.3.2.3.

11.3.3.2.1 Algoritmos de criptación SNMPv3

Los identificadores de transformación de criptación para la gestión de claves SNMPv3 kerberizada DEBERÁN seguirse conforme a lo definido en 6.3.1/J.170.

11.3.3.2.2 Algoritmos de autenticación SNMPv3

Los algoritmos de autenticación para la gestión de claves SNMPv3 kerberizada DEBERÁN seguirse conforme a lo definido en 6.3.2/J.170.

11.3.3.2.3 SNMPv3 kerberizada

El perfil de gestión de claves kerberizadas específico para SNMPv3 DEBERÁ seguirse conforme a lo definido en 6.5.7/J.170.

11.3.3.2.4 ID del motor SNMPv3

Como el gestor SNMP y el cliente DEBEN verificar que el ID del motor SNMPv3 en los mensajes de petición AP y en los mensajes de respuesta AP se basa en el oportuno nombre principal de Kerberos del tique [Rec. UIT-T J.170], se define a continuación la regla que debe utilizarse para generar ID de motor SNMPv3 para ser utilizados en esta aplicación:

- El ID de motor SNMPv3 se ajusta al formato definido en RFC 2576, es decir, el primer bit se pone a 1 (uno) y se utiliza el valor adecuado para los primeros cuatro bytes [RFC 2576].
- El quinto byte tiene el valor 4 (cuatro) para indicar que los siguientes bytes, hasta el 27, deben considerarse texto. Estos bytes, hasta el 27, se definen del siguiente modo:
  - Los primeros 25 caracteres del nombre principal Kerberos se utilizan para los bytes de ID del motor comenzando en el sexto byte.
  - La citada secuencia de bytes, que indica el nombre principal Kerberos, viene seguida por un byte para poder considerarse como un valor hexadecimal de 8 bits. Cada uno de los distintos valores identifica un motor SNMP concreto del dispositivo (elemento o servidor NMS). El valor 0 (cero) NO DEBE utilizarse.
  - La cadena de texto que empieza en el sexto byte termina con un carácter nulo.

Obsérvese que se pueden utilizar otros formatos ajustándose a la solución planteada en RFC 2576. No obstante, la anterior selección tiene por objeto reducir la complejidad de la implementación que sería necesaria si se admitiesen todas las soluciones de RFC 2576.

11.3.3.2.5 Relleno de usmUserTable

En 6.3.6.3 se definen los valores de seguridad SNMPv3 para el usuario "CHAdministrator" del operador de cable. El CHAdministrator es la autoridad final para la gestión del elemento de servicios de portal. También se podrán definir otros usuarios. En esta cláusula se define un usuario USM específicamente para el proceso de configuración y en particular para permitir que se especifique un receptor de notificaciones para cabhPsDevProvEnrollTrap y cabhPsDevInitTrap, que debe transmitir el PS durante el proceso de configuración (véanse el cuadro 13-1, etapa CHPSWMD-11; cuadro 13-2, etapa CHPSWMS-11 y etapa CHPSWMS-13; y 13.3.3.

Los msgSecurityParameters de los mensajes SNMPv3 llevan un campo msgUserName que indica el usuario en cuya representación se intercambia el mensaje y con cuya información de seguridad se producen los campos *msgAuthenticationParameters* y *msgPrivacyParameters*. Para que el motor SNMP de un elemento procese estos mensajes, se requiere introducir la información necesaria en *usmUserTable* RFC 3414 para el motor del elemento. El *usmUserTable* DEBE rellenarse en el elemento PS inmediatamente tras la recepción del mensaje de respuesta AP con la siguiente información:

- usmUserEngineID: el ID de motor SNMP local definido en 11.3.3.2.4;
- usmUserName: PS Administrator-XXXXXX;
- usmUserSecurityName: PS Administrator-XXXXXX;
- usmUserCloneFrom: 0.0;
- usmUserAuthProtocol: indica el protocolo de autenticación seleccionado para el usuario, obtenido del mensaje de respuesta AP;
- usmUserAuthKeyChange: valor por defecto "";
- usmUserOwnAuthKeyChange: valor por defecto "";

- usmUserPrivProtocol: indica el protocolo de criptación seleccionado para el usuario, obtenido del mensaje de respuesta AP;
- usmUserPrivKeyChange: valor por defecto "";
- usmUserOwnPrivKeyChange: valor por defecto "";
- usmUserPublic: valor por defecto "";
- usmUserStorageType: permanente;
- usmUserStatus: activo.

PODRÁN crearse nuevos usuarios SNMPv3 mediante clonación SNMPv3 normal como se define en [RFC 3414].

El cuadro de seguridad para el grupo VACM [RFC 3415] DEBERÁ rellenarse con la siguiente información en el PS justo después de que se reciba el mensaje de respuesta AP:

- vacmSecurityModel: 3(usm);
- vacmSecurityName: CHAdministratorxx:xx:xx:xx:xx:xx;
- vacmGroupName: CHAdministratorSNMP;
- vacmSecurityToGroupStatus: activo.

El cuadro de acceso VACM [RFC 3415] DEBERÁ rellenarse con la siguiente información, vinculada a vacmSecurityToGroupTable que se definió anteriormente, en el PS, justo después de que se reciba el mensaje de respuesta AP:

- vacmAccessContentPrefix: "";
- vacmAccessSecurityModel: 3(usm);
- vacmAccessSecurityLevel: AuthNoPriv;
- vacmAccessContextMatch: exact(1);
- vacmAccessReadViewName: CHAdministratorView;
- vacmAccessWriteViewName: CHAdministratorView;
- vacmAccessNotifyViewName: CHAdministratorNotifyView;
- vacmAccessStorageType: permanente;
- vacmAccessStatus: activo.

Se DEBEN rellenar siete filas del árbol de vistas VACM [RFC 3415] con la siguiente información en el PS justo después de que se reciba el mensaje de respuesta AP:

- vacmViewTreeFamilyName: CHAdministratorNotifyView;
- vacmViewTreeFamilySubtree: cabhPsDevProvEnrollTrap;
- vacmViewTreeFamilyType: included;
- vacmViewTreeFamilyMask: "";
- vacmViewTreeFamilyName: CHAdministratorNotifyView;
- vacmViewTreeFamilySubtree: cabhPsDevBase;
- vacmViewTreeFamilyType: included;
- vacmViewTreeFamilyMask: "";
- vacmViewTreeFamilyName: CHAdministratorNotifyView;
- vacmViewTreeFamilySubtree: docsDevSoftware;
- vacmViewTreeFamilyType: included;
- vacmViewTreeFamilyMask: "";
- vacmViewTreeFamilyName: CHAdministratorNotifyView;

- vacmViewTreeFamilySubtree: cabhPsDevInitTrap;
- vacmViewTreeFamilyType: included;
- vacmViewTreeFamily Mask: "";
- vacmViewTreeFamilyName: CHAdministratorNotifyView;
- vacmViewTreeFamilySubtree: cabhPsDevBase;
- vacmViewTreeFamilyType: included;
- vacmViewTreeFamily Mask: "";
- vacmViewTreeFamilyName: CHAdministratorNotifyView;
- vacmViewTreeFamilySubtree: docsDevEventTable;
- vacmViewTreeFamilyType: included;
- vacmViewTreeFamily Mask: "";
- vacmViewTreeFamilyName: CHAdministratorNotifyView;
- vacmViewTreeFamilySubtree: cabhPsDevProv;
- vacmViewTreeFamilyType: included;
- vacmViewTreeFamily Mask: "".

El valor XXXXXX DEBE ser la dirección MAC de la WAN-Man del elemento PS correspondiente a dicho elemento PS.

PUEDEN crearse nuevos usuarios SNMPv3 con la clonación normal SNMPv3 definida en RFC 2475. Para información adicional consúltese 7.1.1.3.1/J.170.

11.3.4 CQoS segura

La CQoS proporciona QoS a las aplicaciones IPCablecom que requieren una dirección transferencia. Los mensajes DQoS IPCablecom entre el MTA y el CMTS, CMS o el CM, se aseguran mediante la especificación de seguridad IPCablecom. Para la seguridad de IPCable2Home es necesario que los mensajes IPCablecom, que ya han sido asegurados por IPCablecom, puedan atravesar la barrera contra fuegos del elemento de servicios de portal (PS). No es objeto de la presente Recomendación la adición de seguridad a los mensajes IPCablecom. Como en esta Recomendación el requisito de seguridad CQoS del elemento PS consiste únicamente en entregar la mensajería de seguridad IPCablecom, no hay dependencia del soporte de esta función por parte del NMS. Por consiguiente, la función de seguridad CQoS es la misma en el modo de configuración DHCP y en el modo de configuración SNMP (véase 5.5).

El requisito para la seguridad CQoS consiste en proporcionar seguridad que no sea excesivamente gravosa para el sistema. El punto clave para asegurar la QoS es lograr que el robo de servicio y la perturbación de red se reduzcan hasta que las pérdidas sean despreciables. Otro concepto crítico consiste en que la CQoS es la pasarela de QoS hacia el interior del hogar y que por consiguiente controlará o soportará con toda probabilidad todas las aplicaciones y dispositivos del hogar que requieran QoS de la red de cable, hacia el PS y a través de éste. Por consiguiente, es especialmente importante lograr que este punto de entrada, especialmente, no sea el eslabón débil del sistema QoS.

11.3.4.1 Arquitectura CQoS

La arquitectura CQoS está integrada por el elemento funcional CQP que facilita el establecimiento de flujos de QoS a través del HFC para las aplicaciones IP. El elemento CQP existe en el HA. Véase la cláusula 10 sobre CQoS. El elemento CQP actúa como puente transparente para la mensajería CQoS entre las aplicaciones homologadas IPCablecom y el CMTS. La barrera contra fuegos de IPCable2Home tendrá que dejar pasar la seguridad homologada IPCablecom y la mensajería QoS.

Véase en la cláusula 10 una exposición más detallada sobre la CQoS.

11.3.4.2 Arquitectura DQoS con seguridad IPCablecom

Cuadro 11-14/J.191 – Arquitectura DQoS segura

E-MTA		
Enlace con el MTA en el hogar	**Protocolo**	**Protocolo de seguridad**
E-MTA/CM – CMS	NCS	IPSec
E-MTA/CM – CMTS	DOCSIS	BPI+

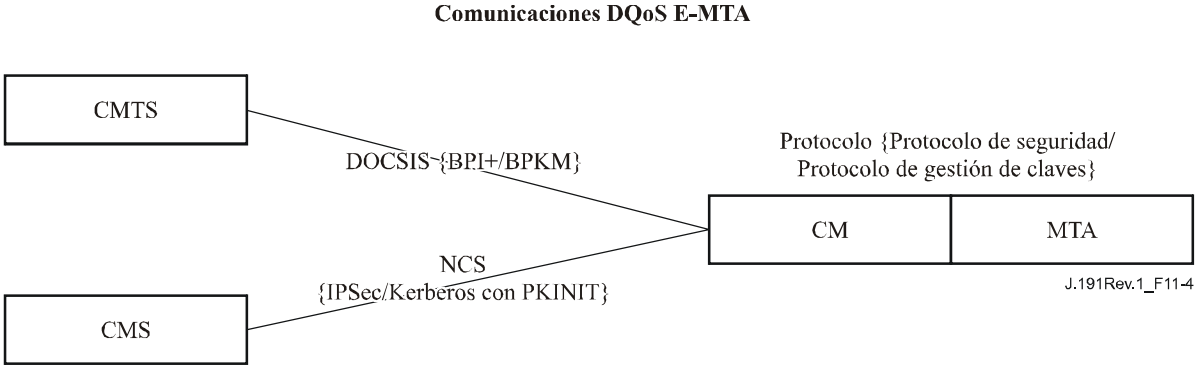


Figura 11-4/J.191 – Arquitectura DQoS segura en el MTA

11.3.4.3 Arquitectura de seguridad del CQoS

El CQoS requiere que la mensajería DQoS de IPCablecom [Rec. UIT-T J.163] pase al E-MTA. Toda la mensajería DQoS DEBE asegurarse conforme a lo descrito en la especificación de seguridad IPCablecom. El diagrama a continuación muestra los protocolos necesarios para soportar el E-MTA para DQoS. La única diferencia entre la arquitectura segura CQoS y la arquitectura segura DQoS de IPCablecom consiste en que el PS se encuentra lógicamente entre el CM y el MTA. No obstante, dado que el PS se comporta como un puente transparente no hay modificaciones en los protocolos ni en los enlaces de comunicaciones.

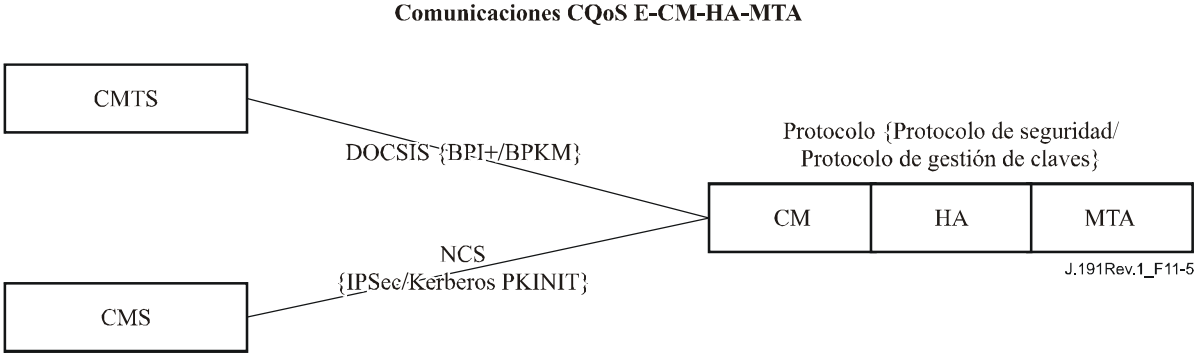


Figura 11-5/J.191 – Arquitectura CQoS segura del MTA

11.3.4.4 Misión del CSP en la CQoS

El portal de seguridad del cable (CSP) es el único punto de control de seguridad de la función de servicios de portal (PS) en la arquitectura de IPCable2Home; por consiguiente el CSP proporciona la seguridad en la arquitectura CQoS. El CQP se comporta como un puente transparente para los mensajes DQoS a los que da soporte; por consiguiente el CSP no proporciona servicios para CQoS.

11.3.5 Gestión de la barrera contra fuegos

Mientras que las cuestiones de seguridad siempre han tenido gran importancia para las empresas que trabajaban con redes, el aumento de la ubicuidad de la conectividad de Internet gracias al módem de cable (CM) plantea problemas de seguridad en el hogar. Como el abonado medio carece de los conocimientos técnicos, de la comprensión de cuestiones de seguridad y del tiempo necesario para mantener los computadores domésticos en funcionamiento seguro al máximo nivel, la barrera contra fuegos se convierte en el elemento necesario de primera línea de defensa para la protección de los computadores inseguros del hogar.

Entre las diversas definiciones de la barrera contra fuegos se encuentran las siguientes:

> "Una barrera contra fuegos es una solución de seguridad que contribuye a la puesta en práctica de una política de seguridad más amplia que define los servicios y los accesos que han de permitirse" [ICSA].
>
> "Una barrera contra fuegos es un agente que examina el tráfico de la red, en alguna medida, y bloquea el tráfico considerado peligroso o inadecuado" [RFC 2979].

Por consiguiente, una barrera contra fuegos implementa una política de seguridad mediante la utilización de algún mecanismo de bloqueo del tráfico considerado indeseable de acuerdo con las especificaciones de la política de seguridad.

Entre los requisitos de manejo del tráfico de la barrera contra fuegos se encuentran los siguientes:

- La barrera contra fuegos NO DEBE interrumpir IPCablecom (véase el cuadro 11-15) ni los protocolos de IPCable2Home definidos en esta Recomendación. Por ejemplo, la barrera contra fuegos debería tener el adecuado soporte de apoderado específico de la aplicación o de filtrado dinámico de paquetes para abrir puertos UDP que se definan como resultado de la señalización IPCablecom.

Cuadro 11-15/J.191 – Especificaciones IPCablecom pertinentes para la barrera contra fuegos de IPCable2Home

Descripción	Recomendación
Especificación de códecs de audio y vídeo	J.161
Especificación de la calidad de servicio dinámica	J.163
Especificación del protocolo de señalización de llamadas basado en la red	J.162
Especificación de la prestación del dispositivo MTA	J.167
Especificación de seguridad	J.170
Especificación del mecanismo de eventos de gestión	J.172
Especificación del protocolo servidor de audio	J.175
Especificación de la señalización del servidor de gestión de llamadas	J.178

Entre los protocolos definidos por IPCablecom se encuentran los siguientes:

- Prestación — SNMPv3, DHCP, DNS, TFTP, SYSLOG
- Secuencias de medios — RTP, RTCP
- QoS — RSVP
- Señalización de llamadas de red — MGCP, SDP
- Seguridad — Mensajería Kerberos, IPSec

Entre los protocolos definidos por IPCable2Home se encuentran los siguientes:

- Prestación SNMPv3, DHCP, DNS, TFTP, SYSLOG
- Gestión ICMP
- Seguridad Kerberos

La barrera contra fuegos DEBERÍA proteger contra la exploración de puertos o de la red ya sea desde el interior como desde el exterior de la red doméstica. DEBERÍA proteger asimismo contra la siguiente lista de denegación de ataques del servicio: "Ping of Death", "Teardrop", "Bonk", "Nestea", "SYN Flood", "LAND Attack", "IP Spoofing", "Smurf Attack" y "WinNuke".

La barrera contra fuegos DEBE permitir el acceso a los mismos protocolos de aplicación de Internet de gran difusión que se definen en el anexo D. A los efectos de esta Recomendación, no basta con un simple filtrado NAT o de paquetes. Para proporcionar una solución flexible y segura, la barrera contra fuegos DEBE implementar ya sea un apoderado específico de la aplicación (ASP) o una barrera contra fuegos de filtrado dinámico de paquetes (SPF).

11.3.5.1 Descarga a distancia del conjunto de reglas de la barrera contra fuegos

Se activarán características en el elemento PS para permitir que el operador gestione a distancia las funciones de la barrera contra fuegos. Esta gestión es la que se lleva a cabo mediante la descarga de un fichero de configuración. El fichero de configuración de la barrera contra fuegos contiene el conjunto de reglas correspondiente a una política de seguridad concreta. La gestión de la barrera contra fuegos se efectúa mediante el acceso a los objetos de gestión de la MIB de seguridad.

La política de seguridad define el nivel deseado de seguridad y funcionalidad para la barrera contra fuegos del abonado. Se puede escoger entre varios de éstos. Los ficheros que contienen los correspondientes conjuntos de reglas para estas políticas de seguridad se encuentran en un servidor de ficheros del operador. El PS DEBE utilizar un cliente TFTP homologado con RFC 1350 para poder descargar el fichero de configuración del conjunto de reglas de la barrera contra fuegos.

La descarga del fichero de configuración de la barrera contra fuegos se activa cuando el valor empleado para FIJAR el objeto MIB cabhSecFwPolicyFileURL, mediante el fichero de configuración del PS o una instrucción SNMP SET, es distinto del valor de la MIB cabhSecFwPolicySuccessfulFileURL. Si el valor utilizado para FIJAR el objeto MIB cabhSecFwPolicyFileURL, mediante el fichero de configuración del PS o una instrucción SNMP SET, es idéntico al valor de la MIB cabhSecFwPolicySuccessfulFileURL, NO DEBERÁ activarse la descarga del fichero de configuración de la barrera contra fuegos.

El procedimiento para verificar la integridad del fichero de configuración de la barrera contra fuegos mediante el elemento PS es:

1) el generador del fichero de configuración de la barrera contra fuegos producirá un troceo SHA-1 de todo el contenido de dicho fichero, considerándolo como una cadena de bytes.
2) el sistema de configuración envía el valor de troceo calculado en el paso anterior al elemento PS en uno de los dos modos siguientes:
   a) modifica el valor del objeto MIB cabhSecFwPolicyFileHash a través de un TLV tipo 28 en el fichero de configuración del PS.
   b) envía una instrucción SNMP SET para actualizar el objeto MIB cabhSecFwPolicyFileHash.
3) El sistema de configuración envía el nombre y la ubicación del fichero de configuración de la barrera contra fuegos para activar la descarga de dicho fichero en uno de dos modos:
   a) modifica el objeto MIB cabhSecFwPolicyFileURL a través de un TLV tipo 28 en el fichero de configuración del PS.

b) envía una instrucción SNMP SET para actualizar el objeto MIB cabhSecFwPolicyFileURL.

4) Si cabhSecFwPolicyFileOperStatus no es inProgress(1) y el valor utilizado para FIJAR el objeto MIB cabhSecFwPolicyFileURL difiere del valor de la MIB cabhSecFwPolicySuccessfulFileURL, el elemento PS DEBE descargar inmediatamente el fichero nombrado del servidor TFTP configurado.

5) El elemento PS DEBE calcular un troceo SHA-1 [FIPS 186-2] de todo el contenido del fichero de configuración de la barrera contra fuegos y comparar el resultado con el troceo representado por el valor del objeto MIB cabhSecFwPolicyFileHash. Si ambos valores son idénticos, se verifica la integridad del fichero de configuración de la barrera contra fuegos y debe utilizarse el fichero de configuración de la barrera contra fuegos, de lo contrario DEBE rechazarse el fichero.

El elemento PS define que la descarga satisfactoria del fichero de configuración de la barrera contra fuegos está completa y se recibió correctamente dentro del periodo de temporización de TFTP y que la validación del fichero estuvo libre de errores mediante el procedimiento de verificación de la integridad descrito anteriormente. Tras el éxito de la descarga del fichero de configuración de la barrera contra fuegos el PS DEBE actualizar la MIB cabhSecFwPolicySuccessfulFileURL con el mismo valor de la MIB cabhSecFwPolicyFileURL.

Si fracasa la descarga del fichero de configuración de la barrera contra fuegos, el PS NO DEBE actualizar la MIB cabhSecFwPolicySuccessfulFileURL con el mismo valor de la MIB cabhSecFwPolicyFileURL. En todo caso, el objeto MIB cabhSecFwPolicyFileURL DEBE incluir el valor FIJADO (SET) por el fichero de configuración del PS o por una instrucción SNMP SET. Cuando se reactiva el PS, el objeto MIB cabhSecFwPolicyFileURL DEBE rellenarse con su valor por defecto.

Los valores de la política del fichero de configuración de la barrera contra fuegos DEBEN conservarse durante los rearranques del elemento PS.

La activación y la desactivación de la barrera contra fuegos del PS se controla mediante el objeto MIB cabhSecFwPolicyEnable. Si el valor de este objeto es enable(1) la barrera contra fuegos del PS DEBE activarse después, y no antes, de que la MIB cabhPsDevProvState tenga el valor 'pass(1)' indicando que el proceso de configuración se ha completado. Esto permitirá modificar la política de la barrera contra fuegos a través de un ciclo de alimentación del PS cuando se restringe accidentalmente el acceso a la gestión de la red WAN. La barrera contra fuegos del PS NO DEBE habilitarse si el valor de cabhSecFwPolicyEnable es disable(2)

La MIB cabhSecFwPolicyCurrentVersion DEBE reflejar siempre la versión de la política correspondiente al PS sin tener en cuenta si está habilitada o deshabilitada actualmente en la MIB cabhSecFwPolicyEnable.

11.3.5.2 Parámetros de gestión del conjunto de reglas de la barrera contra fuegos

Los siguientes parámetros de gestión DEBEN implementarse en el PS conforme a la MIB de seguridad para soportar el fichero del conjunto de reglas de la barrera contra fuegos:

- **cabhSecFwPolicyFileURL** – Contiene el nombre del fichero del conjunto de reglas de política y la dirección IP del servidor TFTP que incluye dicho fichero, en un formato TFTP URL. Cuando el valor utilizado para FIJAR (SET) esta MIB sea distinto del valor en la MIB cabhSecFwPolicySuccessfulFileURL, se activa la descarga del fichero del conjunto de reglas de política.
- **cabhSecFwPolicySuccessfulFileURL** – Contiene el nombre del fichero del conjunto de reglas de política y la dirección IP del servidor TFTP que incluía dicho fichero, en un formato TFTP URL, que se utilizó para activar la última descarga satisfactoria. Si no se ha producido aún una descarga con éxito, esta MIB debería tener un valor Nulo.

- **cabhSecFwPolicyFileHash** – Define el resumen SHA-1 del fichero del conjunto de reglas correspondiente.
- **cabhSecFwPolicyFileOperStatus** – Este objeto indica el estado de la descarga del fichero de configuración de la barrera contra fuegos y se define como InProgress(1), indicando que la descarga del fichero de configuración de la barrera contra fuegos se encuentra en proceso. Complete(2) indica que dicho fichero se descargó y se procesó con éxito. Failed(4) indica que fracasó el último intento para descargar el citado fichero.
- **cabhSecFwPolicyFileCurrentVersion** – Indica la versión del fichero del conjunto de reglas que funciona actualmente en el elemento PS. Este objeto debería representarse con la sintaxis utilizada por el fabricante particular para identificar las versiones del fichero del conjunto de reglas. El elemento PS DEBE devolver una cadena descriptiva de la carga del fichero del conjunto de reglas actual. De no poder aplicarse, este objeto DEBE contener una cadena vacía.
- **cabhSecFwPolicyFileEnable** – Permite la activación y desactivación de la política de seguridad de la barrera contra fuegos.

11.3.5.3 Registro histórico de eventos de la barrera contra fuegos

La barrera contra fuegos DEBE poder efectuar anotaciones históricas correspondientes a los siguientes tipos de eventos:

TIPO 1: Intentos de clientes públicos y privados de atravesar la barrera contra fuegos, que violen la política de seguridad.

TIPO 2: Intentos de ataques de denegación de servicio identificados.

TIPO 3: Modificaciones aplicadas a cualquiera de los siguientes parámetros de configuración de la barrera contra fuegos:

- cabhSecFwPolicyFileURL;
- cabhSecFwPolicyFileCurrentVersion;
- cabhSecFwPolicyFileEnable.

Los tipos de eventos de la barrera contra fuegos que deben registrarse en el histórico se configuran mediante la interfaz de la MIB de seguridad descrita en 11.3.5.4.

La barrera contra fuegos DEBE efectuar el registro histórico de los eventos asociados con la descarga a través del TFTP del fichero de política de la barrera contra fuegos según proceda. Véase el anexo B, cuadro B-1 (proceso CSP, subproceso TFTP de la barrera contra fuegos).

Los operadores pueden supervisar los eventos de la barrera contra fuegos utilizando el mecanismo de mensajería de eventos definido en 6.5. Los parámetros de gestión de las anotaciones históricas de eventos son accesibles a través de la MIB de seguridad y se definen en 6.5.

El registro histórico de mensajes de eventos de la barrera contra fuegos permite que el operador evalúe el nivel de actividad de la piratería informática a través de la red del operador y las modificaciones de la política de seguridad de la barrera contra fuegos. Cuando se hayan establecido los tipos de mensaje de eventos mediante los parámetros de gestión de la MIB de seguridad, dichos eventos de la barrera contra fuegos DEBEN registrarse en el histórico con entradas de mensajes de eventos por medio del mecanismo de anotaciones históricas de eventos definido en 6.5.

Una anotación de mensajes de eventos de la barrera contra fuegos contendrá la siguiente información:

- Prioridad del evento.
- Fecha y hora en que ocurrió el evento.
- Protocolo indicado en el campo de cabecera IP (TCP, UDP, ICMP).

- Dirección IP de origen.
- Dirección IP de destino.
- Puerto de destino (TCP y UDP) o tipo de mensaje (ICMP).
- Regla de política aplicable.
- Descripción del evento (opcional).

La cláusula 6.5.2.1 define un campo de prioridad de eventos que describe distintos niveles de prioridad para los eventos registrados en el histórico. Cuando el campo no sea aplicable deberá dejarse en blanco. El elemento PS DEBE formatear los mensajes de eventos de la barrera contra fuegos de acuerdo con lo definido en el anexo B.

Para ayudar a la supervisión de la actividad de piratería en la barrera contra fuegos del abonado, se han definido en la MIB de seguridad objetos de gestión de alertas de piratería. Esta función alerta al operador cuando el número de eventos de la barrera contra fuegos TIPOS 1 y 2 supera un umbral de alerta durante un periodo de alerta determinado (en horas). El umbral de alertas y el periodo de alertas son configurables por el operador. El elemento PS acumula el número de eventos de la barrera contra fuegos TIPOS 1 y 2 producidos durante el número de horas anteriores definido por el periodo de alerta. Si dicho número excediese el umbral de alertas, se registraría una mensaje de eventos de alertas de piratería para informar al operador.

11.3.5.4 Parámetros de gestión para el registro histórico de eventos

Los siguientes parámetros de gestión DEBEN implementarse en el PS, de acuerdo con la definición de la MIB de seguridad, para supervisar/configurar la anotación histórica de eventos de la barrera contra fuegos:

- **cabhSecFwEventType1Enable** – Activa o desactiva el registro histórico de los mensajes de eventos de la barrera contra fuegos del Tipo 1. Default = disable(2);
- **cabhSecFwEventType2Enable** – Activa o desactiva el registro histórico de los mensajes de eventos de la barrera contra fuegos del Tipo 2. Default = disable(2);
- **cabhSecFwEventType3Enable** – Activa o desactiva el registro histórico de los mensajes de eventos de la barrera contra fuegos del Tipo 3. Default = disable(2);
- **cabhSecFwEventAttackAlertThreshold** – Si el número de ataques piratas tipos 1 ó 2 supera este umbral en el periodo definido por el objeto cabhSecFwEventAttackAlertPeriod, DEBE registrarse un evento de mensaje de la barrera contra fuegos. El valor por defecto se pone al valor entero más alto permitido. Esta MIB NO SE DEBE tener en cuenta si cabhSecFwEventAttackAlertPeriod se pone a 0 y NO DEBE enviarse un mensaje de evento. Default = 65535.
- **cabhSecFwEventAttackAlertPeriod** – Indica el periodo a utilizar en horas anteriores para el objeto cabhSecFwEventAttackAlertThreshold. Default = 0.

11.3.6 Las MIB

El PS autónomo DEBE soportar las siguientes MIB de soporte a la descarga de soporte lógico definidas en RFC 2669:

- **docsDevSwAdminStatus** – Si tiene el valor upgradeFromMgt(1), el dispositivo iniciará la descarga de la imagen de soporte lógico TFTP utilizando docsDevSwFilename.
- **docsDevSwFilename** – Nombre del fichero de la imagen de soporte lógico a cargar en el dispositivo.
- **docsDevSwCurrentVers** – Versión de soporte lógico que funciona actualmente en el dispositivo.
- **docsDevSwServer** – Dirección del servidor TFTP utilizada para las actualizaciones de soporte lógico.

- **docsDevSwOperStatus** – Estado de la descarga de soporte lógico.

El PS autónomo DEBE soportar las MIB de soporte a la descarga de soporte lógico definidas en [draft-ietf-ipcdn-bpiplus-mib-12]:

- **docsBpi2CodeDownloadGroup** – Colección de objetos de soporte a la descarga de soporte lógico autenticado. El docsBpi2CodeDownloadGroup incluye lo siguiente:
  - **docsBpi2CodeDownloadStatusCode** – Indica el resultado de la verificación CVC del último fichero de configuración, la verificación CVC del SNMP o la verificación del fichero de código.
  - **docsBpi2CodeDownloadStatusString** – Información adicional al código de estado.
  - **docsBpi2CodeMfgOrgName** – El organizationName del fabricante del dispositivo.
  - **docsBpi2CodeMfgCodeAccessStart** – Valor actual del codeAccessStart del fabricante del dispositivo con relación a la hora del meridiano de Greenwich (GMT).
  - **docsBpi2CodeMfgCvcAccessStart** – Valor actual del cvcAccessStart del fabricante del dispositivo relativo a la hora del meridiano de Greenwich (GMT).
  - **docsBpi2CodeCoSignerOrgName** – organizationName del cofirmante.
  - **docsBpi2CodeCoSignerCodeAccessStart** – Valor actual del codeAccessStart del cofirmante relativo a la hora del meridiano Greenwich (GMT).
  - **docsBpi2CodeCoSignerCvcAccessStart** – Valor actual del cvcAccessStart del cofirmante relativo a la hora del meridiano de Greenwich (GMT).
  - **docsBpi2CodeCvcUpdate** – Activa el dispositivo para verificar el CVC y actualiza el valor cvcAccessStart.
- **docsBpi2CmPublicKey** – Una cadena tipo ASN.1 RSAPublicKey codificada DER, definida de acuerdo con la norma de criptación RSA [RFC 2437].
- **docsBpi2CmDeviceCmCert** – Certificado de dispositivo codificado DER X.509.
- **docsBpi2CmDeviceManufCert** – Certificado CA del fabricante codificado DER X.509 correspondiente al que firmó el certificado del dispositivo.

El PS autónomo DEBE soportar la siguiente MIB de soporte de descarga de configuración:

- **cabhPsDevProvConfigHash** – Troceado SHA-1 [FIPS 186-2] de todo el contenido del fichero de configuración, considerado como una cadena de bytes. Véase 7.3.3.

11.3.7 Descarga segura de soporte lógico

El elemento PS autónomo de un dispositivo DEBE poder descargar remotamente una imagen de soporte lógico por la red. Como se describe en 6.3.7, el módem de cable controla la descarga segura de soporte lógico a un PS integrado. La nueva imagen de soporte lógico permitirá al operador mejorar la calidad de funcionamiento, acomodar nuevas funciones y características, corregir defectos de diseño y aceptar un trayecto de migración para los dispositivos conforme a la evolución de la presente Recomendación. La capacidad de descarga de soporte lógico DEBE aceptar la modificación de la funcionalidad del elemento PS sin que sea necesario que el personal del sistema de cable visite personalmente y reconfigure cada unidad. El proceso de descarga segura de soporte lógico del PS autónomo contempla los siguientes requisitos primarios del sistema:

- El mecanismo utilizado para la descarga de soporte lógico DEBE ser la transferencia de ficheros TFTP.
- La descarga de soporte lógico DEBE iniciarse de una de las maneras siguientes:
  1) una petición SNMP SET emitida por el NMS al docsDevSwAdminStatus;
  2) a través del fichero de configuración del elemento PS.

Si el nombre del fichero de actualización de soporte lógico que figura en el fichero de configuración no concuerda con la actual imagen de soporte lógico del dispositivo, el elemento PS DEBE solicitar el fichero en cuestión a través del servidor de soporte lógico vía TFTP.

- El elemento PS DEBE verificar que la imagen de soporte lógico descargada sea adecuada para sí mismo. Si la imagen de soporte lógico descargada es adecuada, el elemento PS DEBE salvar la nueva imagen de soporte lógico en almacenamiento no volátil. Una vez completada la transferencia de ficheros con éxito, el dispositivo DEBE rearrancarse con la nueva imagen de código.
- Si el elemento PS no puede completar la transferencia del fichero por alguna razón, el elemento PS DEBE seguir admitiendo nuevas descargas de soporte lógico (sin interacción del operador ni del usuario, aunque se interrumpa la alimentación o la conexión entre intentos).
- El elemento PS DEBE anotar en el registro histórico los fallos de las descargas de soporte lógico y PUEDE comunicar los fallos de modo asíncrono al gestor de la red.
- Una vez actualizado el soporte lógico para adaptarse a una nueva versión de la presente Recomendación, el soporte lógico DEBE poder trabajar con la versión anterior para permitir la transición paulatina de las unidades de la red.
- El elemento PS DEBE autenticar el origen de la descarga de soporte lógico.
- El elemento PS DEBE verificar que el código descargado no ha sido modificado respecto a la forma original suministrada por la fuente de confianza.
- El proceso de descarga de soporte lógico DEBE dotar al operador de mecanismos de actualización o retrotracción de las versiones de código de los elementos de IPCable2Home.
- El proceso de descarga de soporte lógico DEBE dotar al operador de opciones que le permitan establecer sus propias políticas de descarga.
- El fabricante del fichero de código DEBE aplicar una signatura de verificación de código (CVS, *code verification signature*) a la imagen de código y a cualquier otro atributo autenticado como los que se definen en esta especificación para la firma digital de estructura PKCS#7 del fichero de código; la clave privada utilizada para aplicar la firma DEBE estar vinculada a un certificado de clave pública que arranque de la raíz CVC. La firma del fabricante autentica el origen e integridad del fichero de código.
- El cofirmante (operador u organismo de certificación) PUEDE rubricar el fichero de código adicionalmente a la firma del fabricante.
- El elemento PS DEBE poder procesar la firma digital PKCS#7 y un certificado X.509 IPCable2Home como se define en 11.3.7.2.1.1 y 11.3.7.3 respectivamente.
- (Opcional): El elemento PS DEBERÍA poder actualizar el certificado CA de raíz CVC almacenado en el dispositivo.
- (Opcional): El elemento PS DEBERÍA poder sustituir los certificados CA del fabricante almacenados en el dispositivo.
- (Opcional): El elemento PS DEBERÍA poder actualizar el certificado CA CVC almacenado en el dispositivo.
- (Opcional): El elemento PS DEBERÍA poder actualizar el certificado CA de raíz del proveedor de servicio almacenado en el dispositivo.

La descarga facultativa del certificado CA de raíz del proveedor de servicio, el certificado CA de raíz CVC, el certificado CA CVC y/o el certificado CA del fabricante como parte del fichero de código permite la discriminación sin lugar a dudas de la imagen de código del resto de los parámetros en el fichero de descarga de código. Existe la posibilidad de modificar los cuatro

certificados que acaban de indicarse y que son comprendidos por el elemento PS incluyendo los nuevos certificados en la imagen de código. La inclusión del certificado CVC del fabricante y/o un CVC de confirmante y la CVS correspondiente permiten que el elemento PS pueda verificar que la imagen de código no ha sido alterada desde que se agregó a la imagen de código lo siguiente: certificado CA de raíz del proveedor de servicio, certificado CA de raíz CVC, certificado CA CVC y/o el certificado CA del fabricante o los parámetros SignedData.

11.3.7.1 Descarga de soporte lógico en elementos de PS integrado o autónomo

Como se ilustra en la figura 11-6 a continuación, un dispositivo conforme al acceso a la vivienda (HA) puede implementar el módem de cable y el elemento PS como entidades independientes o integradas tal y como se define en 5.1.3.1.

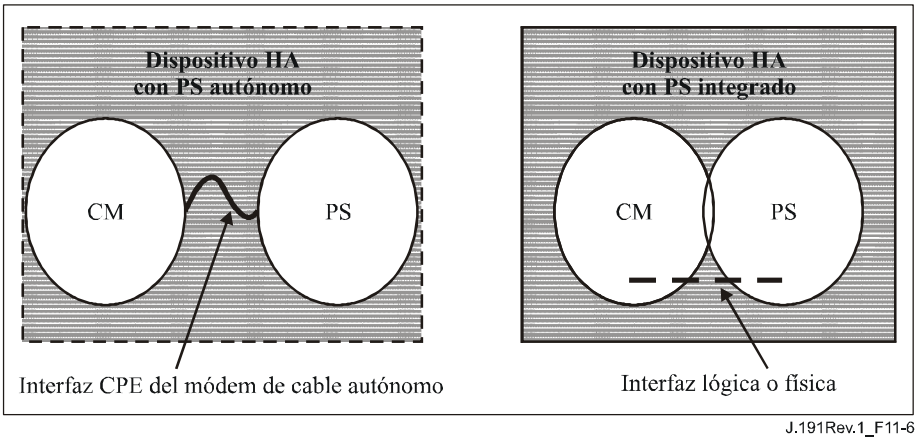


Figura 11-6/J.191 – Dispositivo HA

Para IPCable2Home:

- Si el elemento PS está integrado en el módem de cable, la imagen PS/CM DEBE ser simple, y la descarga del soporte lógico DEBERÁ ejecutarse únicamente a través del módem de cable.
- Si el elemento PS está compuesto de entidades autónomas independientes, será el elemento PS quien DEBA ejecutar la descarga del soporte lógico para los elementos de IPCable2Home como se describe más adelante.

11.3.7.2 Requisitos del fichero de código

11.3.7.2.1 Estructura del fichero de descarga de código para la descarga segura de soporte lógico

Para poder descargar soporte lógico con seguridad, el fichero de descarga de código se construye utilizando una estructura homologada con RFC 2315 que se haya definido en un formato específico para ser utilizado con los elementos PS. El fichero de código DEBE cumplir RFC 2315 y DEBE estar codificado en DER. El fichero de código DEBE ajustarse a la estructura que muestra el cuadro 11-16.

Cuando los certificados se descargan como parte del fichero de código, estos PODRÁN incluirse en los campos como se especifica en el cuadro 11-16, independientes de la imagen de código real contenida en el campo CodeImage.

Cuadro 11-16/J.191 – Estructura del fichero de código

Fichero de código	Descripción
Firma digital PKCS#7 {	
ContentInfo	
ContentType	SignedData
SignedData ()	El valor del contenido de datos firmados EXPLICIT: incluye CVS que cumplen CVS y X.509
} *Fin de la firma digital PKCS#7*	
SignedContent {	
Download Parameters {	Formato TLV obligatorio (Tipo 28). (De longitud cero si no hay subTLV.)
MfgCACerts ()	TLV opcional para uno o varios certificados codificados en DER utilizando el formato TLV del certificado CA del fabricante (Tipo 17).
clabServProvRootCACert ()	TLV opcional para un certificado codificado en DER utilizando el formato TLV del certificado CA de raíz del proveedor de servicio (Tipo 50).
clabCVCRootCACert ()	TLV opcional para un certificado codificado en DER utilizando el formato del TLV del certificado CA de raíz CVC (Tipo 51).
clabCVCCACertificate ()	TLV opcional para un certificado codificado en DER utilizando el formato TLV del certificado CA CVC (Tipo 52).
}	
CodeImage ()	Actualizar imagen de código.
} *Fin de SignedContent*	

11.3.7.2.1.1 Datos firmados

El fichero de descarga de código contendrá la información con un tipo de contenido de datos firmados [RFC 2315] como se muestra en el cuadro 11-17. Aun manteniendo la conformidad con [RFC 2315], la estructura utilizada se ha restringido en cuanto a su formato para facilitar el procesamiento efectuado por el PS para validar la firma. Los datos firmados [RFC 2315] DEBEN estar codificados en DER y ajustarse exactamente a la estructura mostrada más adelante excepto por las modificaciones de orden exigidas por la codificación DER (por ejemplo, la ordenación de los atributos SET OF). El elemento PS DEBERÍA rechazar la firma [RFC 2315] si los datos firmados [RFC 2315] no concuerdan con la estructura codificada en DER.

Cuadro 11-17/J.191 – Datos firmados PKCS#7

Campo PKCS#7	Descripción
Datos firmados {	
version	versión = 1
DigestAlgorithmIdentifiers	SHA-1
ContentInfo	
ContentType	Datos (SignedContent está concatenado al final de la estructura PKCS#7)
certificates {	(certificado de verificación de código CableLabs (CVC))

Cuadro 11-17/J.191 – Datos firmados PKCS#7

Campo PKCS#7	Descripción
mfgCVC	(REQUERIDO para todos los ficheros de código)
co-signerCVC	(OPCIONAL; requerido para las cofirmas)
} *fin de certificados*	
SignerInfo{	
MfgSignerInfo {	(REQUERIDO para todos los ficheros de código)
version	versión = 1
issuerAndSerialNumber	
issuerName	
CountryName	US
organizationName	CableLabs
CommonName	CableLabs CVC Root CA
certificateSerialNumber	<número de serie CVC del fabricante >
digestAlgorithm	SHA-1
AuthenticatedAttributes	
contentType	datos (contentType de signedContent)
signingTime	UTCTime (GMT), YYMMDDhhmmssZ
messageDigest	(compendio del contenido definido en [PKCS#7])
digestEncryptionAlgorithm	rsaEncryption
EncryptedDigest	
} *end mfg signer info*	
CoSignerInfo {	(OPCIONAL; requerido para las cofirmas)
version	versión = 1
issuerAndSerialNumber	
issuerName	
CountryName	US
organizationName	CableLabs
CommonName	CA raíz CVC CableLabs
certificateSerialNumber	<número de serie CVC CoSigner >
digestAlgorithm	SHA-1
AuthenticatedAttributes	
contentType	datos (contentType de signedContent)
signingTime	UTCTime (GMT), YYMMDDhhmmssZ
messageDigest	(compendio del contenido definido en [PKCS#7])
digestEncryptionAlgorithm	rsaEncryption
EncryptedDigest	
} *end mso signer info*	
} *end signer info*	
} *end signed data*	

11.3.7.2.1.2 Contenido firmado

El campo de contenido firmado del fichero de código contiene la imagen de código y el campo de parámetros de descarga que contendrá probablemente elementos opcionales adicionales como certificado CA raíz del proveedor de servicio, certificado CA raíz CVC del laboratorio de prueba de certificación (CTL, *certification testing laboratory*), un certificado CA CVC CTL y/o un certificado CA del fabricante.

La imagen de código final estará en un formato compatible con el elemento PS de destino. Para soportar los requisitos de la firma PKCS#7, el contenido del código se introduce como datos; es decir, una simple cadena de octetos. El formato de la imagen de código final no se especifica aquí y lo definirá cada fabricante de acuerdo con sus propias necesidades.

Cada fabricante DEBERÍA construir su propio código con mecanismos adicionales que verificasen que la actualización de la imagen de código es compatible con el elemento PS de destino.

Si se incluye en el campo de contenido firmado, un certificado se destina a sustituir el certificado que figura actualmente en el elemento PS. Si se llevan a buen fin la descarga y la instalación del código, el elemento PS DEBE sustituir su certificado actualmente almacenado por el nuevo certificado recibido en el campo de contenido firmado. Este nuevo certificado se utilizará para la verificación subsiguiente.

11.3.7.2.1.3 Claves de firma de código

La firma digital conforme a [RFC 2315] utiliza el algoritmo de criptación RSA [RFC 2437] con SHA-1 [FIPS 186-2]. El elemento PS DEBE poder verificar las firmas del fichero de código. El exponente público es F_4 (65537 decimal).

11.3.7.2.1.4 Certificado CA del fabricante

Se trata de un atributo tipo cadena que contiene un certificado CA X.509, que se define en la Rec. UIT-T X.509 | ISO/CEI 9594-8.

Tipo	Longitud	Valor
17	Variable	Certificado CA X.509 (ASN.1 codificada en DER)

11.3.7.2.1.5 Certificado CA raíz del proveedor de servicio

Se trata de un atributo tipo cadena que contiene un certificado CA raíz de proveedor de servicio X.509, según se define en la Rec. UIT-T X.509 | ISO/CEI 9594-8. El elemento PS debe utilizar ese certificado en el modo de configuración SNMP para efectos de autenticación mutua.

Tipo	Longitud	Valor
50	Variable	Certificado CA X.509 (ASN.1 codificada en DER)

11.3.7.2.1.6 Certificado CA raíz CVC

Se trata de un atributo tipo cadena que contiene un certificado CA raíz CVC X.509, que se define en la Rec. UIT-T X.509 | ISO/CEI 9594-8. El elemento PS autónomo debe utilizar este certificado durante el proceso de descarga segura de soporte lógico.

Tipo	Longitud	Valor
51	Variable	Certificado CA X.509 (ASN.1 codificada en DER)

11.3.7.2.1.7 Certificado CA CVC

Se trata de un atributo tipo cadena que contiene un certificado CA CVC X.509, que se define en la Rec. UIT-T X.509 | ISO/CEI 9594-8. El elemento PS autónomo debe utilizar este certificado durante el proceso de descarga segura de soporte lógico.

Tipo	Longitud	Valor
52	Variable	Certificado CA X.509 (ASN.1 codificada en DER)

11.3.7.3 Formato del certificado de verificación de código (CVC)

11.3.7.3.1 Formato CVC para la descarga segura de soporte lógico

Para la descarga segura de soporte lógico, el formato utilizado para el CVC cumple X.509. No obstante, la estructura X.509 se ha restringido para facilitar el procesamiento que debe efectuar el elemento PS para validar el certificado y extraer la clave pública utilizada para verificar el CVS. El CVC DEBE venir codificado en DER y ajustarse exactamente a la estructura del cuadro 11-18 salvo para las modificaciones de secuencia necesarias para la codificación DER (por ejemplo, el orden de los atributos SET OF). El elemento PS DEBERÍA rechazar el CVC si no concuerda con la estructura codificada en DER representada en el cuadro 11-18. La codificación DER DEBE satisfacer los requisitos de la cláusula 11.3.2.

Cuadro 11-18/J.191 – Certificado de verificación de código homologado con X.509

Certificado X.509	Descripción
Certificate {	
version	2 (o sea, Rec. UIT-T X.509 versión 3)
serialNumber	Entero, número igual a 20 octetos (es decir un número único asignado por la CA de raíz)
signature	RSA SHA-1, parámetros nulos
issuer	
countryName	US
organizationName	
commonName	CA de raíz CVC
validity	
notBefore	utcTime (GMT), YYMMDDhhmmssZ (es decir, instante de emisión)
notAfter	utcTime (GMT), YYMMDDhhmmssZ
subject	
countryName	<Nombre del país>
organizationName	<Nombre de la empresa>
commonName	<Nombre común>
subjectPublicKeyInfo	
algorithm	Criptación RSA, parámetros nulos
subjectPublicKey	Módulo de 2048 bits
extensions	
KeyUsage	<Utilización de clave>
authorityKeyIdentifier	<Identificador de clave de autoridad>
signatureAlgorithm	RSA SHA-1, parámetros nulos
signatureValue	<Valor de firma>
} *end certificate*	

11.3.7.3.2 Revocación de certificados

Esta Recomendación no requiere ni define la utilización de las listas de revocación de certificados (CRL, *certificate revocation lists*). No es necesario que el elemento PS soporte las CRL. Los operadores podrían tener interés en definir y utilizar CRL fuera de la red HFC como ayuda a la gestión de los ficheros de código que les proporcionan los fabricantes. No obstante, hay un método de revocación de certificados basado en la fecha inicial de validez del certificado. Este método requiere la entrega al elemento PS de un CVC actualizado con un instante de comienzo de validez actualizado. Una vez se consigue validar el CVC, el instante de comienzo de la validez X.509 actualizará el valor actual cvcAccessStart del elemento PS.

11.3.7.4 Controles de acceso al fichero de código

Para poder efectuar la descarga segura del soporte lógico, se incluyen en el fichero de código valores de control especiales para que el elemento PS los compruebe antes de validar la imagen de código. Las condiciones que figuran en los valores de estos parámetros de control DEBEN satisfacerse antes de que el elemento PS valide el CVC o el CVS, y acepte la imagen de código.

11.3.7.4.1 Nombres de la organización sujeto

El elemento PS reconocerá un máximo de dos nombres en el campo sujeto de un CVC del fichero de código en cualquier instante, si los considera agentes de firma de códigos de confianza. Esto incluye:

- Al fabricante del dispositivo: el nombre del fabricante en el campo sujeto CVC de fabricante DEBE concordar exactamente con el nombre de fabricante almacenado en la memoria no volátil del elemento PS por el fabricante. Un CVC de fabricante DEBE estar siempre presente en el fichero de código.
- A un agente cofirmante: se permite que otra organización de confianza cofirme los ficheros de código destinados al dispositivo. La mayor parte de los casos se tratará del operador que controla el actual dominio de explotación del dispositivo. El nombre de organización del cofirmante se comunica al elemento PS mediante un CVC de cofirmante en el fichero de configuración cuando se inicializa el proceso de verificación de código del elemento PS. El nombre de organización cofirmante que figura en el campo sujeto CVC del cofirmante DEBE concordar exactamente con el nombre de organización de cofirmante recibido previamente en el CVC de inicialización del cofirmante y almacenado por el elemento PS.

El elemento PS PUEDE comparar los nombres de organización mediante una comparación binaria.

11.3.7.4.2 Controles variables en el tiempo

Para reducir la probabilidad de que un elemento PS reciba un fichero de código anterior gracias a un intento de repetición, los ficheros de código incluyen un valor del instante de la firma en la estructura PKCS#7 que puede utilizarse para indicar el momento en que se firmó la imagen de código. El elemento PS DEBE tener dos valores horarios UTC asociados a cada agente firmante de código. Un conjunto DEBE almacenarse y mantenerse siempre para el fabricante del dispositivo. Adicionalmente, si el fichero de código está cofirmado, el elemento PS DEBE también almacenar y mantener un conjunto independiente de valores horarios para el cofirmante.

Estos valores se utilizan para controlar el acceso del fichero de código al elemento PS mediante el control individual de la validez del CVS y del CVC. Estos valores son:

- codeAccessStart: valor temporal UTC de 12 bytes relativo al tiempo medio de Greenwich (GMT, *Greenwich mean time*).
- cvcAccessStart: valor horario UTC de 12 bytes relativo a GMT.

Los valores UTCTime del CVC DEBEN expresarse como GMT y DEBEN incluir segundos. Es decir, DEBEN expresarse en la siguiente forma: YYMMDDhhmmssZ. El campo de año (YY) DEBE interpretarse del siguiente modo:

- Cuando YY sea igual o mayor que 50, el año se interpretará como 19YY.
- Cuando YY sea inferior a 50, el año se interpretará como 20YY.

Estos valores serán siempre relativos al tiempo medio de Greenwich, de modo que el carácter ASCII final (Z) pueda suprimirse cuando lo almacena el elemento PS como codeAccessStart y cvcAccessStart.

El elemento PS DEBE mantener cada uno de estos valores horarios en un formato que contenga la información horaria equivalente y la precisión correspondiente al formato UTV de 12 caracteres (es decir, YYMMDDhhmmss). El elemento PS DEBE comparar con exactitud estos valores almacenados con los valores horarios UTC recibidos por el elemento PS en un CVC. Estos requisitos se exponen más adelante en la presente especificación.

Los valores codeAccessStart y cvcAccessStart correspondientes al fabricante del elemento PS NO DEBEN disminuir. Los valores de codeAccessStart y cvcAccessStart correspondientes al cofirmante NO DEBEN disminuir mientras el cofirmante siga siendo el mismo y el elemento PS mantenga los valores de control del cofirmante variables en el tiempo.

11.3.7.5 Inicialización de la actualización del código

11.3.7.5.1 Inicialización del fabricante

Es responsabilidad del fabricante instalar correctamente en el elemento PS la versión inicial del código.

Para soportar la descarga segura de soporte lógico, los valores de los controles del fabricante variables en el tiempo DEBEN cargarse en la memoria no volátil del elemento PS:

- organizationName del fabricante del elemento PS;
- valores de control del fabricante variables en el tiempo:
  a) valor de inicialización codeAccessStart;
  b) valor de inicialización cvcAccessStart.

El nombre de organización del fabricante del elemento PS DEBE estar siempre presente en el dispositivo. El organizationName del fabricante del elemento PS PUEDE almacenarse en la imagen de código del dispositivo. El nombre del fabricante utilizado para la actualización de código no tiene por qué coincidir con el nombre utilizado en el certificado CA del fabricante.

Los valores de control variables en el tiempo, codeAccessStart y cvcAccessStart, DEBEN inicializarse a un UTCTime compatible con el instante de comienzo de la validez del último CVC del fabricante. Estos valores variables en el tiempo se actualizarán periódicamente durante el funcionamiento normal a través de los CVC recibidos del fabricante y verificados por el elemento PS.

El fabricante DEBE inicializar los siguientes certificados en la memoria no volátil del elemento PS autónomo:

- Certificado CA de raíz del proveedor de servicio.
- Certificado CA de raíz CVC.
- Certificado CA CVC.
- Certificado CA del fabricante.
- Certificado del elemento PS.

El fabricante debe inicializar los siguientes certificados en la memoria no volátil del elemento PS integrado:

- Certificado CA de raíz del proveedor de servicio.
- Certificado CA del fabricante.
- Certificado del elemento PS.

11.3.7.5.2 Inicialización de la red

Para poder llevar a cabo la verificación del código, el fichero de configuración PS se utiliza como medio autenticado en el que inicializará el proceso de verificación del código. En el fichero de configuración del elemento PS, el elemento PS recibe los valores de configuración pertinentes a la verificación de la actualización de código.

El fichero de configuración DEBERÍA incluir siempre la CVC más reciente aplicable al elemento PS destino; pero cuando el fichero de configuración se utiliza para iniciar una actualización de código, DEBE incluir un certificado de verificación de código (CVC) para inicializar el elemento PS a fin de que acepte ficheros de código acordes con esta Recomendación. Independientemente de si se requiere una actualización de código, el CVC del fichero de configuración DEBE procesarlo el elemento PS. Un fichero de configuración PUEDE contener:

- Ningún CVC – El elemento PS NO DEBE aceptar el fichero de código.
- Únicamente el CVC del fabricante – El elemento PS DEBE verificar que el CVC del fabricante arranque de la raíz CVC antes de aceptar el fichero de código. Cuando el fichero de configuración del elemento PS únicamente contenga un CVC válido de fabricante, el dispositivo sólo requerirá una firma del fabricante en los ficheros de código. En tal caso, el elemento PS NO DEBE aceptar ficheros de código que estén cofirmados.
- Únicamente un CVC cofirmado – El elemento PS DEBE verificar que el CVC del cofirmante arranca del CVC raíz antes de aceptar el fichero de código. Cuando el fichero de configuración del elemento PS contenga un CVC de cofirmante válido, se utilizará para inicializar el dispositivo con un cofirmante. Una vez validado el nombre organizationName del sujeto del CVC, se convertirá en el cofirmante del código asignado al elemento PS. Para que un elemento PS pueda aceptar posteriormente una imagen de código, el fichero de código DEBE estar firmado por el fabricante del dispositivo IPCable2Home y además por el cofirmante.
- Un CVC del fabricante y un CVC del cofirmante. El elemento PS DEBE verificar que ambos CVC arrancan del CVC raíz antes de aceptar el fichero de código.

Antes de que el elemento PS pueda ser capaz de actualizar ficheros de código en la red, DEBE recibir un CVC válido en un fichero de configuración. Además, si el fichero de configuración del elemento PS no conviene un CVC válido y se ha inhabilitado para actualizar ficheros de código, el elemento PS DEBE rechazar cualquier información recibida posteriormente mediante SNMP.

El nombre de la organización del fabricante del elemento PS y los valores de control variables en el tiempo del fabricante DEBEN estar siempre en el elemento PS. Si el elemento PS se inicializa para aceptar código cofirmado por un firmante de código adicional, el nombre de la organización y sus correspondientes variables de control variables en el tiempo DEBEN almacenarse y mantenerse mientras sean operativos. DEBE asignarse espacio en la memoria del elemento PS para los siguientes valores de control del cofirmante:

1) organizationName del agente cofirmante;
2) valores de control del cofirmante variables en el tiempo:
   a) cvcAccessStart;
   b) codeAccessStart.

De estos valores, el conjunto del fabricante DEBE almacenarse en la memoria no volátil del elemento PS y no desaparecer cuando se interrumpe la alimentación de corriente del dispositivo ni durante los rearranques.

Cuando se asigna un cofirmante al elemento PS, el conjunto de valores CVC del cofirmante, DEBE almacenarse en la memoria del elemento PS. El elemento PS PUEDE retener estos valores en memoria no volátil que no se borre cuando se interrumpa la alimentación de energía ni durante los rearranques. No obstante, cuando se asigne un elemento PS a un cofirmante, el CVC estará siempre en el fichero de configuración. Por consiguiente, el elemento PS recibirá siempre los valores de control del cofirmante durante la fase de inicialización no siendo necesario almacenar los valores de control del cofirmante variables en el tiempo cuando se interrumpe la alimentación eléctrica ni durante los procesos de rearranque.

11.3.7.6 Procesamiento del CVC

Para facilitar la entrega de una actualización del CVC sin que sea necesario que el HA procese una actualización de código, el CVC PUEDE entregarse ya sea en el fichero de configuración o en una SNMP MIB. El formato del CVC es idéntico independientemente de que se trate de un fichero de código, de un fichero de configuración o de una SNMP MIB.

11.3.7.6.1 Procesamiento del CVC del fichero de configuración

Cuando se incluye un CVC en el fichero de configuración, el elemento PS DEBE verificar el CVC antes de aceptar los valores de actualización de código que contenga. Cuando se recibe el CVC en el fichero de configuración, el elemento PS DEBE ejecutar los siguientes pasos de validación y de procedimiento. Si falla cualquiera de las comprobaciones de verificación siguientes, el elemento PS DEBE detener inmediatamente el proceso de verificación CVC y anotar en el registro histórico el error, en su caso. Si el fichero de configuración del elemento PS no incluye un CVC que se valide adecuadamente, el elemento PS NO DEBE descargar ficheros de código de actualización ya sean activados por el fichero de configuración del elemento PS o por una SNMP MIB. Además, si los ficheros de configuración de un elemento PS no incluye una CVC que se valide adecuadamente, no es necesario que el elemento PS procese las CVC recibidas posteriormente a través de una SNMP MIB y NO DEBE aceptar información de una CVC recibida posteriormente a través de una SNMP MIB.

Cuando recibe un CVC en un fichero de configuración, el elemento PS DEBE:

1) Verificar que la extensión de utilización de clave ampliada está en el CVC con arreglo a lo definido en 11.3.2.2.2.
2) Comprobar el nombre de la organización sujeto del CVC.
    a) Si el CVC es un CVC de fabricante (Tipo 32) entonces:
        i) SI el organizationName es idéntico al nombre del fabricante del dispositivo ENTONCES se trata del CVC del fabricante. En este caso, el elemento PS DEBE verificar que el instante inicial de validez del CVC del fabricante es anterior o igual al valor cvcAccessStart del fabricante que contiene actualmente el elemento PS.
        ii) SI el organizationName no coincide con el nombre del fabricante del dispositivo ENTONCES DEBE rechazarse este CVC y registrarse el error.
    b) Si el CVC es un CVC de cofirmante (Tipo 33) entonces:
        i) SI el organizationName coincide exactamente con el cofirmante del código actual del elemento PS ENTONCES éste es el CVC del cofirmante actual y el elemento PS DEBE verificar que el instante de comienzo de validez es posterior o igual al valor cvcAccessStart del cofirmante que actualmente figura en el elemento PS.

ii) SI el organizationName no coincide totalmente con el actual nombre del cofirmante ENTONCES una vez validado el CVC (y completado su registro) este nombre de organización sujeto se convertirá en el nuevo cofirmante de código del elemento PS. El elemento PS NO DEBE aceptar un fichero de código a no ser que haya sido firmado por el fabricante y cofirmado por dicho cofirmante de código.

3) Validar la firma del expedidor del CVC utilizando la clave pública CA del CVC de CTL que figura en el elemento PS.

4) Validar la firma CA del CVC de CTL utilizando la clave pública CA del CVC de CTL raíz que figura en el elemento PS. La verificación de la firma autenticará la fuente y validará la confianza en los parámetros CVC.

5) Actualizar el valor actual cvcAccessStart del elemento PS correspondiente al organizationName sujeto del CVC (es decir del fabricante o del cofirmante) con el valor horario de inicio de la validez del CVC validado. Si el valor horario de inicio de la validez es mayor que el valor actual del elemento PS de codeAccessStart, actualizar el valor codeAccessStart del elemento PS con el valor horario de inicio de la validez. El elemento PS DEBERÍA rechazar los residuos del CVC del cofirmante.

11.3.7.6.2 Procesamiento del SNMP CVC

El elemento PS DEBE procesar los CVC recibidos mediante SNMP cuando esté capacitado para actualizar ficheros de código; de lo contrario, DEBEN rechazarse los CVC recibidos mediante SNMP. Cuando se valide un CVC recibido mediante SNMP, el elemento PS DEBE efectuar los siguientes pasos de validación y de procedimiento. Si falla la comprobación de verificación siguiente, el elemento PS DEBE detener inmediatamente el proceso de verificación del CVC, registrar el error en su caso y eliminar los restos del proceso hasta dicho paso.

El elemento PS DEBE:

1) Verificar que la extensión de uso de clave ampliada está en el CVC con arreglo a lo definido en 11.3.2.2.2.

2) Comprobar el nombre de la organización sujeto del CVC.

   a) SI el organizationName es idéntico al nombre del fabricante del dispositivo ENTONCES éste es el CVC del fabricante. En tal caso, el elemento PS DEBE verificar que el instante inicial de validez del CVC del fabricante es posterior al valor cvcAccessStart del fabricante que actualmente figura en el elemento PS.

   b) SI el organizationName es idéntico al actual cofirmante de código del elemento PS ENTONCES se trata de un CVC de cofirmante actual y el instante de comienzo de la validez DEBE ser posterior al valor cvcAccessStart del cofirmante que figura actualmente en el elemento PS.

   c) SI el organizationName no es idéntico al fabricante del dispositivo o al actual nombre del cofirmante ENTONCES el elemento PS DEBE rechazar inmediatamente este CVC.

3) Validar la firma del expedidor del CVC utilizando la clave pública CA CVC de CTL que figura en el elemento PS.

4) Validar la firma del expedidor del CVC utilizando la clave pública CA del CVC de CTL raíz que tiene el elemento PS. La verificación de la firma autenticará el certificado y confirmará la confianza en el instante de comienzo de validez del CVC.

5) Actualizar el último valor de los cvcAccessStar del sujeto con el valor de instante de comienzo de la validez del CVC validado. Si el instante de comienzo de validez es posterior al valor actual de codeAccessStart, del elemento PS, actualizar el valor codeAccessStart del elemento PS con el valor de comienzo de la validez.

11.3.7.7 Requisitos de la firma de código

11.3.7.7.1 Requisitos de la autoridad del certificado (CA)

Los certificados de verificación de código (CVC) los firma y expide la CA del CVC del laboratorio de prueba de certificación (CTL). El CVC DEBE ajustarse exactamente a lo especificado en 11.3.7.3. La CA del CVC de CTL NO DEBE firmar ningún CVC salvo que sea idéntico al formato especificado en 11.3.7.3. Antes de firmar un CVC, la CA del CVC de CTL DEBE verificar que la solicitud del certificado es auténtica.

La CA del CVC de CTL será la encargada del registro de los nombres de los abonados autorizados del CVC. Entre los abonados del CVC se encuentran los fabricantes del elemento PS y los operadores cofirmantes de las imágenes de código. Es responsabilidad de la CA del CVC de CTL garantizar que el nombre de organización de cada uno de los abonados del CVC sea diferente. DEBEN aplicarse las siguientes directrices para asignar los nombres de organización para los cofirmantes de los ficheros de código:

- El nombre de organización utilizado para su propia identificación como agente cofirmante de un CVC DEBE asignarse por la organización que emitió el certificado raíz.
- El nombre DEBE ser una cadena imprimible de ocho dígitos hexadecimales que distinga de modo exclusivo un agente firmante de código de los demás.
- Cada uno de los dígitos hexadecimales del nombre DEBE seleccionarse del conjunto de caracteres 0-9 (0x30-0x39) o A-F (0x41-0x46).
- La cadena compuesta por ocho dígitos cero no está permitida y NO DEBE utilizarse en los CVC.

En cualquier formato alternativo se DEBE mantener toda la información y reproducir el formato original; por ejemplo, como un entero de 32 bits distinto de cero, con un valor entero de 0 que representa la ausencia de un firmante de código.

11.3.7.7.1.1 Requisitos del CVC del fabricante

Para firmar sus ficheros de código, el fabricante DEBE obtener un CVC válido de la CA del CVC de CTL. Todas las imágenes de código del fabricante proporcionadas a un operador para actualizar a distancia un dispositivo DEBEN estar firmadas de acuerdo con los requisitos definidos en esta Recomendación. Al firmar un fichero de código, el fabricante PUEDE optar por no actualizar el valor signingTime PKCS#7 de la información de firma del fabricante. Esta Recomendación requiere que el valor signingTime PKCS#7 sea igual o mayor que el instante del comienzo de validez del CVC. Si el fabricante utiliza un signingTime igual al instante de comienzo de validez del CVC cuando firma una serie de ficheros de código, éstos pueden utilizarse repetidas veces. Esto permite que el operador utilice el fichero de códigos para actualizar o retrotraer la versión de códigos para los dispositivos del fabricante. Estos ficheros de códigos serán validos hasta que se genere un nuevo CVC y lo reciba el elemento PS.

11.3.7.7.1.2 Requisitos del operador

Cuando un operador reciba ficheros de código de actualización de soporte lógico de un fabricante, deberá validar la imagen de código utilizando la clave pública de la CA del CVC de CTL. Esto permitirá que el operador verifique si la imagen de código la ha construido un fabricante de confianza. El operador puede volver a verificar el fichero de código en cualquier instante repitiendo dicho proceso.

Si un operador desea ejercer la opción de cofirmar la imagen de código destinada a un dispositivo de la red, el operador DEBE obtener un CVC válido de la CA del CVC de CTL.

Cuando firma un fichero de código, el operador DEBE cofirmar el contenido del fichero conforme a la norma de firma PKCS#7, e incluir su CVC de operador de acuerdo con lo definido en

11.3.7.2.1.1. Esta Recomendación no requiere que un operador cofirme los ficheros de código, pero cuando el operador cumple con todas las reglas definidas en esta Recomendación para la preparación del fichero de código, el elemento PS DEBE aceptarlo.

11.3.7.8 Proceso de activación

Las descargas de código, independientemente del modo de configuración, pueden iniciarse durante el proceso de prestación y registro a través de una descarga iniciada por el fichero de configuración; o durante el funcionamiento normal utilizando un mandato de descarga iniciado por SNMP. El elemento PS DEBE soportar ambos métodos.

NOTA – Antes de activar una descarga segura de soporte lógico, DEBE incluirse en el fichero de configuración la información CVC adecuada. Si el operador decide utilizar la descarga iniciada por SNMP como método para activar una descarga segura de soporte lógico, se recomienda que la información CVC esté siempre presente en el fichero de configuración de modo que el elemento PS tenga siempre la información CVC inicializada cuando sea necesario. Si el operador decide utilizar la descarga iniciada por el fichero de configuración como método de activar la descarga segura de soporte lógico, la información CVC debe estar presente en el fichero de configuración en el momento en que se rearranca el dispositivo para obtener el fichero de configuración que active la actualización.

11.3.7.8.1 Descarga de soporte lógico iniciada por SNMP

Desde una estación de gestión de la red:

- Dar a docsDevSwServer el valor de la dirección del servidor TFTP que se encarga de las actualizaciones de soporte lógico.
- Dar a docsDevSwFilename el valor del nombre del trayecto del fichero de la imagen de actualización de soporte lógico.
- Dar a docsDevSwAdminStatus el valor Upgrade-from-mgt. docsDevSwAdminStatus, que DEBE mantenerse tras las reactivaciones y los rearranques hasta que se sobreescriba por un gestor SNMP o por el fichero de configuración del elemento PS.

El estado por defecto de docsDevSwAdminStatus DEBE ser el allowProvisioningUpgrade{2} hasta que sea sobreescrita por ignoreProvisioningUpgrade{3} tras una actualización con éxito de soporte lógico iniciada por SNMP o alterada por otro procedimiento por la estación de gestión. docsDevSwOperStatus DEBE mantenerse a través de las reactivaciones para informar del resultado del último intento de actualización de soporte lógico.

Si un elemento PS sufre un corte de energía o se reactiva durante una actualización iniciada por SNMP, el elemento PS DEBE reanudar la actualización sin que sea necesaria la intervención manual, y cuando el elemento PS reanude el proceso de actualización:

- docsDevSwAdminStatus DEBE ser Upgrade-from-mgt{1}.
- docsDevSwFilename DEBE ser el nombre del fichero de la imagen de soporte lógico a actualizar.
- docsDevSwServer DEBE ser la dirección del servidor TFTP que contiene la imagen de actualización del soporte lógico a actualizar.
- docsDevSwOperStatus DEBE ser inProgress{1}.
- docsDevSwCurrentVers DEBE ser la versión actual de soporte lógico que opera en el dispositivo.

Cuando el elemento PS alcance el máximo número de reintentos (número máximo de reintentos = 3) como consecuencia de varios fallos de la alimentación o de reactivaciones durante una actualización iniciada por SNMP, el estado del elemento PS DEBE cumplir los siguientes requisitos una vez registrado:

- docsDevSwAdminStatus DEBE ser el allowProvisioningUpgrade{2}.

- docsDevSwFilename DEBE ser el nombre del fichero de soporte lógico cuyo proceso de actualización resultó fallido.
- docsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el soporte lógico cuyo proceso de actualización resultó fallido.
- docsDevSwOperStatus DEBE ser other{5}.
- docsDevSwCurrentVer DEBE ser la versión actual de soporte lógico que opera en el dispositivo IPCable2Home.

Si un elemento PS agota el número necesario de reintentos TFTP al efectuar 16 reintentos consecutivos, el elemento PS DEBE retroceder hasta la última imagen de trabajo operativa y pasar a un estado operacional, cumpliendo los siguientes requisitos:

- docDevSwAdminStatus DEBE ser allowProvisioningUpgrade{2}.
- docDevSwFilename DEBE ser el nombre del fichero del soporte lógico cuyo proceso de actualización resultó fallido.
- docsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el soporte lógico cuyo proceso de actualización resultó fallido.
- docsDevSwOperStatus DEBE ser failed{4}.
- docsDevSwCurrentVer DEBE ser la versión actual de soporte lógico que funciona en el dispositivo.

Una vez que el elemento PS ha completado la actualización del soporte lógico segura iniciada por SNMP, el elemento PS DEBE rearrancarse y ser operativo con la imagen de soporte lógico correcta y una vez que el dispositivo es operativo DEBE cumplir los siguientes requisitos:

- dar el valor ignoreProvisioningUpgrade{3} a su docsDevSwAdminStatus;
- dar el valor completeFromMgt{3} a su docsDevSwOperStatus;
- rearrancar.

El elemento PS DEBE utilizar adecuadamente el estado de ignoreProvisioningUpgrade para ignorar el valor de actualización de soporte lógico que pueda incluirse en el fichero de configuración del elemento PS y empezar a funcionar con la imagen de soporte lógico correcta y, una vez que el dispositivo sea operacional, DEBE cumplir los siguientes requisitos:

- docsDevSwAdminStatus DEBE ser ignoreProvisioningUpgrade{3}.
- docsDevSwFilename PUEDE ser el nombre de fichero de soporte lógico que funciona actualmente en el elemento PS.
- docsDevSwServer PUEDE ser la dirección del servidor TFTP que contiene el soporte lógico que actualmente funciona en el elemento PS.
- docsDevSwOperStatus DEBE ser completeFromMgt{3}.
- docsDevSwCurrentVer DEBE ser la versión actual de soporte lógico que funciona en el elemento PS.

Cuando el elemento PS consiga descargar con éxito (o detecte durante la descarga) una imagen no destinada al dispositivo IPCable2Home:

- DocsDevSwAdminStatus DEBE ser allowProvisioningUpgrade{2}.
- DocsDevSwFilename DEBE ser el nombre de fichero de soporte lógico cuya actualización resultó fallida.
- DocsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el soporte lógico cuyo proceso de actualización resultó fallido.
- DocsDevSwOperStatus DEBE ser other{5}.

- DocsDevSwCurrentVer DEBE ser la versión actual de soporte lógico que funciona en el dispositivo.

Cuando el elemento PS determina que la imagen de descarga está dañada o corrompida, el elemento PS DEBE rechazar la imagen descargada. El elemento PS PUEDE reintentar la descarga si no se ha alcanzado el número MAX de reintentos de la secuencia TFTP. Si el elemento PS opta por no reintentar y no se hubiera alcanzado el número MAX de reintentos de la secuencia TFTP, el elemento PS DEBE retroceder a la última imagen de trabajo conocida y pasar a un estado operacional, generar la notificación de evento adecuada especificada en 11.3.7.10, y cumplir los siguientes requisitos:

- DocsDevSwAdminStatus DEBE ser allowProvisioningUpgrade{2}.
- DocsDevSwFilename DEBE ser el nombre de fichero de soporte lógico cuya actualización resultó fallida.
- DocsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el soporte lógico cuyo proceso de actualización resultó fallido.
- DocsDevSwOperStatus DEBE ser other{5}.
- DocsDevSwCurrentVer DEBE ser la versión actual de soporte lógico que funciona en el dispositivo.

Cuando el elemento PS determina que la imagen está dañada o corrompida, el elemento PS DEBE rechazar la nueva imagen descargada. El elemento PS PUEDE reintentar la descarga de la nueva imagen si no se hubiera alcanzado el número MAX de reintentos de secuencia TFTP. En el 16º intento consecutivo de descarga del soporte lógico, el elemento PS DEBE retroceder a la última imagen de trabajo conocida y pasar a un estado operacional. En tal caso se requiere que el elemento PS envíe dos notificaciones, una para notificar que se ha alcanzado el límite de reintentos MAX TFTP y la otra para notificar que la imagen está dañada. Inmediatamente después de que el elemento PS haya alcanzado el estado operacional, el elemento PS DEBE cumplir los siguientes requisitos:

- DocsDevSwAdminStatus DEBE ser allowProvisioningUpgrade{2}.
- DocsDevSwFilename DEBE ser el nombre del fichero de soporte lógico cuya actualización resultó fallida.
- DocsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el soporte lógico cuyo proceso de actualización resultó fallido.
- DocsDevSwOperStatus DEBE ser other{5}.
- DocsDevSwCurrentVer DEBE ser la versión actual de soporte lógico que funciona en el dispositivo.

11.3.7.8.2 Descarga de soporte lógico iniciada por el fichero de configuración

La descarga de soporte lógico iniciada por el fichero de configuración se inicia por el envío del nombre de fichero de actualización del soporte lógico dentro del fichero de configuración del elemento PS. Si el nombre del fichero de actualización de soporte lógico dentro del fichero de configuración del elemento PS no concuerda con la imagen de soporte lógico actual del dispositivo, el elemento PS DEBE solicitar el fichero especificado a través de TFTP al servidor de soporte lógico.

NOTA – La dirección IP del servidor de soporte lógico es un parámetro independiente. De estar presente, el elemento PS DEBE intentar descargar el fichero especificado de este servidor. Si no estuviera presente, el elemento PS DEBE intentar descargar el fichero especificado del servidor del fichero de configuración.

Si el elemento PS alcanza el número máximo de reintentos (número máximo de reintentos = 3) como consecuencia de varios fallos de alimentación o rearranques durante una actualización

iniciada por el fichero de configuración, el estado del elemento PS DEBE cumplir los siguientes requisitos una vez registrados:

- docsDevSwAdminStatus DEBE ser allowProvisioningUpgrade{2}.
- docsDevSwFilename DEBE ser el nombre de fichero de soporte lógico cuy proceso de actualización resultó fallido.
- docsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el soporte lógico cuyo proceso de actualización resultó fallido.
- docsDevSwOperStatus DEBE ser other{5}.
- docsDevSwCurrentVer DEBE ser la versión actual de soporte lógico que funciona en el dispositivo.

Si el elemento PS agota el número necesario de reintentos TFTP por haber efectuado un total de 16 reintentos consecutivos, el elemento PS debe retroceder a la última imagen de trabajo y proceder a un estado operacional, cumpliendo los siguiente requisitos:

- docDevSwAdminStatus DEBE ser allowProvisioningUpgrade{2}.
- docDevSwFilename DEBE ser el nombre de fichero de soporte lógico cuyo proceso de actualización resultó fallido.
- docsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el soporte lógico cuyo proceso de actualización resultó fallido.
- docsDevSwOperStatus DEBE ser failed{4}.
- docsDevSwCurrentVer DEBE ser la versión actual de soporte que funciona en el dispositivo.

Una vez completada por el elemento PS la actualización de soporte lógico segura iniciada por el fichero de configuración, el elemento PS DEBE rearrancarse y situarse en un estado operacional con la imagen de soporte lógico correcta. Una vez registrado el elemento PS:

- docsDevSwAdminStatus DEBE ser allowProvisioningUpgrade{2}.
- docsDevSwFilename PUEDE ser el nombre de fichero de soporte lógico que actualmente funciona en el dispositivo IPCable2Home.
- docsDevSwServer PUEDE ser la dirección del servidor TFTP que contiene el soporte lógico que actualmente funciona en el dispositivo IPCable2Home.
- docsDevSwOperStatus DEBE ser completeFromProvisioning{2}.
- docsDevSwCurrentVer DEBE ser la versión actual de soporte lógico que funciona en el dispositivo.

11.3.7.9 Verificación de código

Para la descarga segura de soporte lógico, el elemento PS DEBE ejecutar las comprobaciones de verificación presentadas en esta cláusula. Sin falla alguna de las comprobaciones de verificación, o si se rechaza alguna porción del fichero de código debido a la presencia de un formato no válido, el elemento PS DEBE interrumpir inmediatamente el proceso de descarga, registrar el error en su caso, suprimir todos los residuos del proceso hasta dicho paso y continuar funcionando con el código de que disponía hasta dicho momento. Las comprobaciones de verificación pueden llevarse a cabo en cualquier orden, siempre que se efectúen todas las comprobaciones aplicables presentadas en esta cláusula.

1) El elemento PS DEBE validar la información de firma del fabricante verificando que el valor signingTime PKCS#7 es:
   a) igual o mayor que el valor codeAccessStart del fabricante que actualmente tiene el elemento PS;

b) igual o mayor que el instante de comienzo de validez del CVC del fabricante;

c) menor o igual que el instante de finalización de la validez del CVC del fabricante.

2) El elemento PS DEBE validar el CVC del fabricante verificando que:

a) el organizationName sujeto del CVC es idéntico al nombre del fabricante almacenado actualmente en la memoria del elemento PS;

b) el instante de inicio de la validez del CVC es igual o mayor que el valor cvcAccessStart del fabricante que actualmente tiene el elemento PS;

c) la extensión de utilización de clave ampliada está en el CVC con arreglo a lo definido en 11.3.2.2.2.

3) El elemento PS DEBE validar la firma del certificado utilizando la clave pública CA de CVC de CTL del elemento PS. A su vez, la clave pública CA del CVC de CTL raíz del elemento PS valida la firma del certificado CA de CVC de CTL. La verificación de la firma autenticará el origen de la clave de verificación de código (CVK, *code verification key*) pública y confirmará la confianza en dicha clave.

4) El elemento PS DEBE verificar la firma del fichero de código de fabricante:

a) el elemento PS DEBE ejecutar un nuevo troceado SHA-1 sobre el SignedContent. Si el valor del messageDigest no concuerda con el nuevo troceado, el elemento PS DEBE considerar la firma del fichero de código como no válida;

b) si no se verifica la firma, todos los componentes del fichero de código (incluida la imagen de código) y los valores derivados del proceso verificación DEBEN rechazarse y DEBERÍAN descartarse.

5) Si se verifica la firma del fabricante y se requiere la firma de un agente cofirmante:

a) El elemento PS DEBE validar la información de firma del cofirmante verificando que:

i) la información de firma del cofirmante está incluida en el fichero de código;

ii) el valor signingTime PKCS#7 es igual o mayor que el correspondiente valor codeAccessStart que actualmente figura en el elemento PS;

iii) el valor signingTime PKCS#7 es igual o mayor que el correspondiente instante de comienzo de validez del CVC;

iv) el valor signingTime PKCS#7 es menor o igual que el correspondiente instante de finalización de la validez CVC.

b) El elemento PS DEBE validar el CVC del cofirmante, verificando que:

i) el organizationName sujeto del CVC es idéntico al nombre de la organización del cofirmante que figura actualmente almacenada en la memoria del elemento PS;

ii) el instante de comienzo de validez del CVC es igual o mayor que el valor cvcAccessStart que figura actualmente en el elemento PS para el correspondiente organizationName sujeto;

iii) la extensión de uso de clave ampliada está en el CVC con arreglo a lo definido en 11.3.2.2.2.

c) El elemento PS DEBE validar la firma del certificado mediante la clave pública CA del CVC de CTL que figura en el elemento PS. A su vez, la firma del certificado CA del CVC de CTL se valida por parte de la clave pública CA de raíz CVC de CTL del elemento PS. La verificación de la firma autenticará el origen de la clave de verificación de código (CVK) pública del cofirmante y confirmará la confianza en dicha clave.

d) El elemento PS DEBE verificar la firma de fichero de código del cofirmante.

e) El elemento PS DEBE ejecutar un nuevo troceado SHA-1 sobre el SignedContent. Si el valor del messageDigest no concuerda con el nuevo troceado, el elemento PS DEBE considerar la firma del fichero de código como no válida.

f) Si no se verifica la firma, todos los componentes del fichero de código (incluida la imagen de código) y los valores derivados del proceso de verificación DEBEN rechazarse y DEBERÍAN descartarse inmediatamente.

6) Si se ha verificado la firma del fabricante, y opcionalmente la del cofirmante, la imagen de código puede considerarse de confianza y se puede proceder a su instalación. Antes de instalar la imagen de código, todos los demás componentes del fichero de código y los valores derivados del proceso de verificación con la excepción de los valores signingTime PKCS#7 y la fecha de comienzo de la validez del CVC DEBERÍAN descartarse inmediatamente.

7) Si la instalación del código no llega a buen fin, el elemento PS DEBE rechazar los valores signingTime PKCS#7 y los valores de comienzo de la validez del CVC recibidos en el fichero de código.

8) Cuando se consigue completar con éxito la instalación del fichero de código, el elemento PS DEBE actualizar los controles del fabricante variables en el tiempo con los valores obtenidos de la información de firma del fabricante y del CVC:

a) actualizando el valor actual codeAcessStart con el valor signingTime de PKCS#7;

b) actualizando el valor actual de cvcAccessStart con el valor de comienzo de la validez del CVC.

9) Cuando se completa con éxito la instalación del código, SI el fichero de código está cofirmado, el elemento PS DEBE actualizar los controles del cofirmante variables en el tiempo con los valores de la información de la firma del cofirmante y del CVC:

a) actualizando el valor actual de codeAccessStart con el valor signingTime PKCS#7;

b) actualizando el valor actual de cvcAccessStart con el valor de comienzo de validez del CVC.

11.3.7.10 Códigos de error

Los códigos de error se definen para poner de manifiesto los estados de fallo que pueden presentarse durante el proceso de verificación del código de descarga segura de soporte lógico.

1) Controles inadecuados del fichero de código:

a) El organizationName sujeto del CVC correspondiente al fabricante no concuerda con el nombre de fabricante del elemento PS.

b) El organizationName sujeto del CVC correspondiente al agente cofirmante no concuerda con el agente cofirmante de código actual del elemento PS.

c) El valor signingTime PKCS#7 del fabricante es inferior al valor codeAccessStart que tiene actualmente el elemento PS.

d) El valor horario de comienzo de validez PKCS#7 del fabricante es inferior que el valor cvcAccessStart que tiene actualmente el elemento PS.

e) El instante de comienzo de la validez del CVC del fabricante es inferior al valor cvcAccessStart que tiene actualmente el elemento PS.

f) El valor signingTime PKCS#7 del fabricante es inferior al instante de comienzo de la validez del CVC.

g) No existe la extensión de uso de clave ampliada en el CVC del fabricante, o ésta es inadecuada.

h) El valor signingTime PKCS#7 del cofirmante es inferior al valor codeAccessStart que figura actualmente en el elemento PS.

i) El valor horario de comienzo de validez PKCS#7 del cofirmante es inferior al valor cvcAccessStart que figura actualmente en el elemento PS.

j) El instante de comienzo de validez del CVC del cofirmante es inferior al valor cvcAccessStart que figura actualmente en el elemento PS.

k) El valor signingTime PKCS#7 del cofirmante es inferior al instante de comienzo de validez del CVC.

l) No existe la extensión de uso de clave ampliada en el CVC del cofirmante, o es inadecuada.

2) Fallo en la validación del CVC del fabricante del fichero de código.

3) Fallo en la validación del CVS del fabricante del fichero de código.

4) Fallo en la validación del CVC del cofirmante del fichero de código.

5) Fallo en la validación del CVS del cofirmante del fichero de código.

6) Formato inadecuado del CVC del fichero de configuración (por ejemplo, faltan los atributos de utilización de claves o son incorrectos).

7) Fallo en la validación del CVC del fichero de configuración.

8) Formato incorrecto del SNMP CVC:

   a) el organizationName sujeto del CVC correspondiente al fabricante no concuerda con el nombre del fabricante del dispositivo;

   b) el organizationName sujeto del CVC correspondiente al agente cofirmante no concuerda con el agente cofirmante del código actual del elemento PS;

   c) el instante de comienzo de validez del CVC es inferior o igual que el correspondiente valor cvcAccessStart del sujeto que figura actualmente en el elemento PS;

   d) faltan los atributos de utilización de claves o son incorrectas.

9) Fallo en la validación del SNMP CVC.

11.3.7.11 Retrotracción del soporte lógico

La retrotracción del soporte lógico define el proceso de retirar la versión actualizada de la descarga de imagen del soporte lógico devolviendo al dispositivo al estado inmediato anterior.

Cuando el elemento PS recibe un fichero de código con un instante de firma posterior al instante de firma que conserva en su memoria, el dispositivo DEBE actualizar su memoria interna con el valor recibido.

Como el elemento PS no acepta ficheros de código con un instante de firma anterior al valor que almacena internamente, para actualizar un dispositivo con un nuevo fichero de código sin denegar el acceso a los ficheros de códigos anteriores, el firmante (por ejemplo, el fabricante, el operador, el organismo de certificación) debe optar por no actualizar el instante de firma. De este modo, la posibilidad de que varios ficheros de código tengan el mismo instante de firma de código permite al operador retrotraer a voluntad la imagen de código del dispositivo a una versión anterior (es decir, hasta que se actualice el CVC). Esto tiene ciertas ventajas para el operador que deben sopesarse con la posibilidad de un intento de repetición del fichero de código.

Otra solución consistiría en firmar el fichero de código anterior con un instante de firma igual o mayor que el instante de firma de la última actualización.

11.3.8 Seguridad física

Esta Recomendación requiere que el PS mantenga en memoria, las claves y otras variables criptográficas relativas a la seguridad de la red. Todos los elementos y dispositivos DEBEN impedir el acceso físico no autorizado a dicho material criptográfico.

El nivel de protección física del material de criptación que requieren los elementos y dispositivos de red se especifica en términos de los niveles de seguridad definidos en la norma FIPS PUBS 140-2, requisitos de seguridad para los módulos criptográficos. Concretamente, los elementos de IPCable2Home DEBEN cumplir los requisitos del nivel de seguridad 1 de FIPS PUBS 140-2.

El nivel de seguridad 1 de FIPS PUBS 140-2 requiere un mínimo de protección física que se conseguirá mediante la utilización de cajas de protección con calidad de fabricación y prácticas recomendadas de utilización del soporte lógico.

11.3.9 Algoritmos criptográficos

11.3.9.1 SHA-1

La implementación de SHA-1 en IPCable2Home DEBE utilizar el algoritmo de troceo SHA-1 que se define en FIPS 180-2.

12 Procesos de gestión

12.1 Introducción y presentación

Esta cláusula contiene ejemplos de los procesos asociados a la utilización de las herramientas descritas en la cláusula 6 (Herramientas de gestión) y los procesos adicionales que facilitan otras funciones de gestión requeridas definidas en esta Recomendación. El acceso a la base de datos del PS y demás operaciones del PS del portal de gestión del cable (CMP) se describen en la cláusula 6. Las reglas más representativas del acceso a la MIB figuran en 6.3.6.

Se exponen procesos relativos a la gestión y otros procesos descriptivos correspondientes a las siguientes situaciones:

- Procesos de las herramientas de gestión.
- Funcionamiento del CTP:
  - herramienta de velocidad de la conexión;
  - herramienta de verificación de direcciones de Internet (ping).
- Funcionamiento del PS.
- Acceso a la base de datos del PS.
- Reconfiguración:
  - descarga de soporte lógico del PS;
  - descarga del fichero de configuración del PS.
- Acceso a la MIB.
- Configuración del VACM.
- Configuración de la mensajería de eventos de gestión:
  - funcionamiento de la notificación de eventos CMP;
  - funcionamiento del estrangulamiento y limitación de eventos del CMP.

12.1.1 Objetivos

Esta cláusula está integrada principalmente por texto informativo, destinada a facilitar la comprensión del mismo por parte del lector y no contiene ningún requisito. Los ejemplos describen la forma de utilizar las herramientas de gestión para poder conseguir funciones de gestión típicas. Se proporcionan asimismo gráficos secuenciales de procesos adicionales relativos a la gestión (es decir, los no definidos en la cláusula 6), incluidos los procesos de gestión o las etapas de proceso asociadas al uso de las herramientas de gestión. Todos los procesos mostrados implican la interacción del elemento PS con los sistemas de cabecera.

12.2 Proceso de las herramientas de gestión

Los procesos de las herramientas de gestión son los asociados con las herramientas de gestión necesarias definidas en la cláusula 6.

12.2.1 Funcionamiento del CTP

El portal de prueba del cable (CTP) proporciona capacidades para la herramienta de velocidad de la conexión y para la herramienta ping, descritas en 6.4.3.1 y 6.4.3.2 respectivamente.

12.2.1.1 Prueba de velocidad de conexión distante

La prueba de velocidad de conexión distante puede ser útil para la validación de los niveles de calidad de funcionamiento, la identificación de posibles errores de configuración y la determinación de otras características orientadas a la calidad de funcionamiento.

- El sistema de gestión de red (NMS) comienza la prueba inicializando los parámetros de la prueba y activando la bandera de prueba de comienzo, a través de una petición SNMP SET.
- El agente SNMP CMP actualiza la base de datos del PS con los parámetros de prueba y notifica al CTP el comienzo de la prueba.
- El CTP consulta la base de datos del PS para obtener los parámetros de la prueba.
- El CTP emite una ráfaga de paquetes UDP con destino al puerto 7 del dispositivo IP de LAN especificado. El puerto 7 se reserva para el servicio de eco.
- El dispositivo IP de LAN objetivo se limita a devolver al CTP un eco de la parte útil del paquete UDP.
- Una vez recibidos todos los paquetes, o alcanzado el límite temporal de la prueba, el CTP actualiza la base de datos del PS con los resultados de la prueba y activa la bandera de terminación de la prueba.
- El NMS verifica la terminación del mandato comprobado que Status = complete.
- El NMS solicita los resultados de la prueba mediante una petición SNMP GET.
- El agente SNMP del CMP consulta la base de datos del PS para obtener los resultados de la prueba y los comunica en la respuesta SNMP GET. Si no se hubiera completado la prueba, los datos de prueba indicarían que la prueba continúa efectuándose. El NMS debe repetir la petición SNMP GET hasta que los resultados de la prueba indiquen la terminación de la misma.

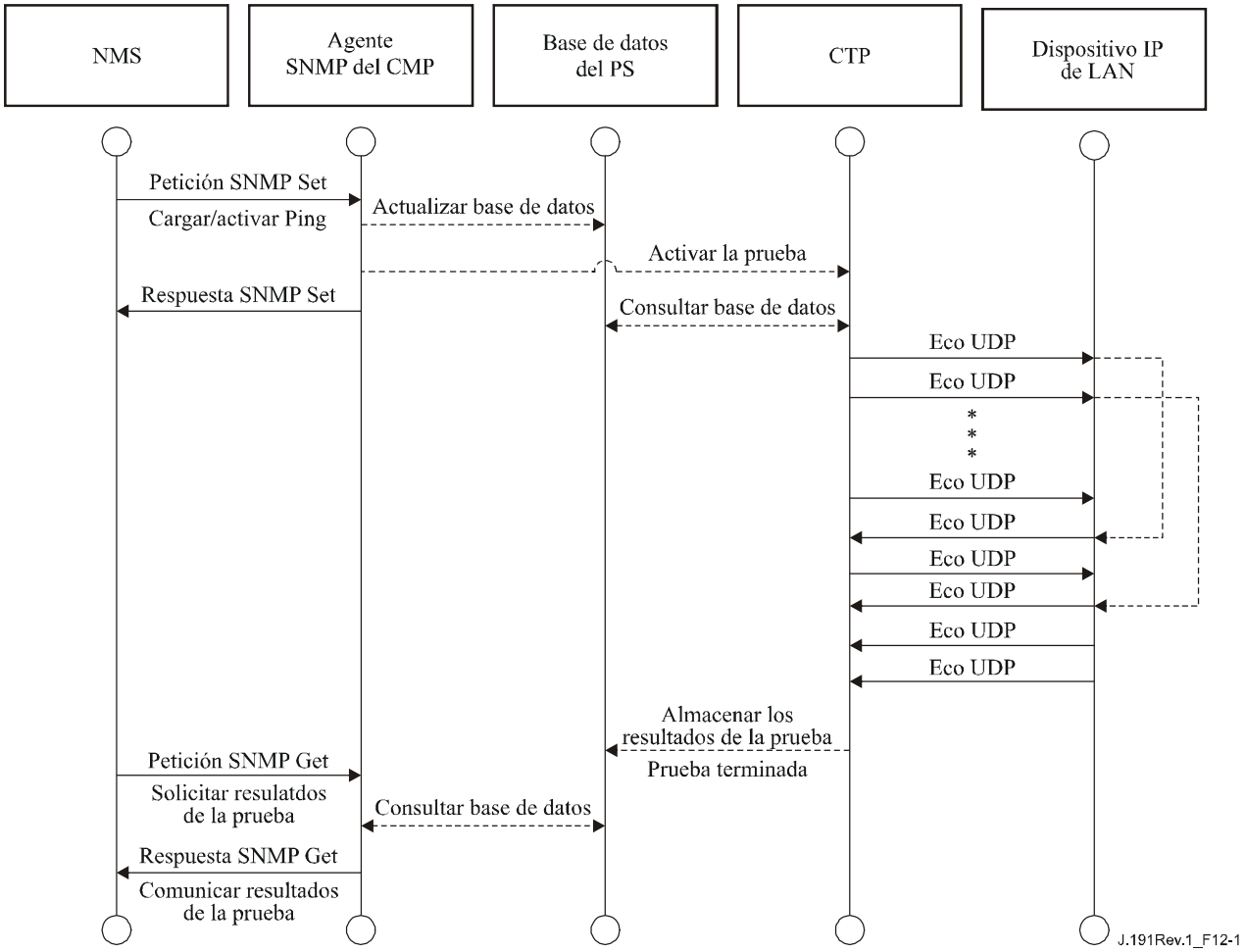


Figura 12-1/J.191 – Diagrama secuencial del proceso de la herramienta de la velocidad de la conexión

12.2.1.2 Proceso de la herramienta Ping

La herramienta ping distante puede servir para validar el estado de la conectividad, los niveles de la calidad de funcionamiento e identificar posibles errores de configuración.

- El NMS comienza la prueba inicializando los parámetros de la prueba y activando la bandera de comienzo de la prueba, mediante la petición SNMP SET.
- El agente SNMP de CMP actualiza la base de datos del PS con los parámetros de la prueba y notifica al CTP el comienzo de la prueba.
- El CTP consulta la base de datos del PS en busca de los parámetros de la prueba.
- El CTP emite un paquete de petición de eco ICMP con destino al dispositivo IP de LAN especificado.
- El dispositivo IP de LAN objetivo responde con una respuesta de eco ICMP.
- El CTP actualiza la base de datos del PS con los resultados de la prueba y activa la bandera de terminación de la prueba.
- El NMS verifica que se ha completado el mandato comprobando que Status = complete.
- El NMS solicita los resultados de la prueba mediante una petición SNMP GET.
- El agente SNMP del CMP consulta la base de datos del PS para obtener los resultados de la prueba y los comunica en la respuesta SNMP GET. Si no se hubiese completado la prueba, los datos de la prueba indicarían que la prueba sigue en marcha. El NMS debe repetir la

petición SNMP GET hasta que los resultados de la prueba indiquen que se ha completado la misma.

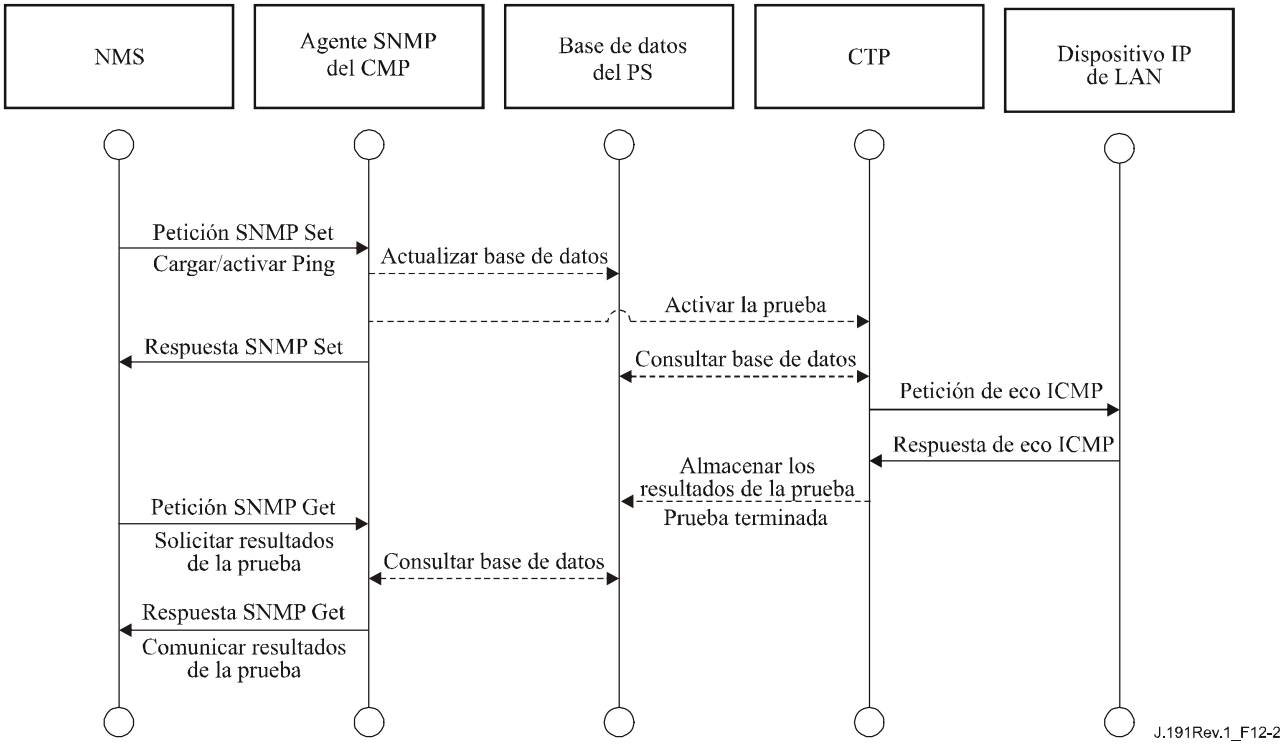


Figura 12-2/J.191 – Diagrama secuencial del proceso de la herramienta Ping

12.3 Funcionamiento del PS

El portal de gestión del cable (CMP) permite el acceso a la base de datos del PS a través de la interfaz WAN-Man del PS, de acuerdo con lo descrito en la cláusula 6. A continuación se describe la secuencia de mensajes para una operación típica de acceso a la base de datos del PS desde la interfaz WAN-Man del PS.

12.3.1 Acceso a la base de datos del PS

Los parámetros de configuración y gestión almacenados en la base de datos del PS son accesibles por el NMS a través de las MIB del SNMP. Los parámetros se recuperan mediante los mensajes SNMP Get Request, SNMP Get Next Request y SNPM Get Bulk emitidos por el NMS teniendo como destino la dirección WAN-Man del PS. Los parámetros pueden modificarse y pueden ejecutarse acciones (como por ejemplo las herramientas de velocidad de la conexión y del Ping) mediante la emisión por parte del NMS de mensajes de petición SNMP SET con los parámetros adecuados, con destino a la dirección WAN-Man del PS.

La figura 12-3 describe la secuencia de mensajes de gestión correspondiente a un acceso típico a la base de datos del PS desde la interfaz WAN-Man del PS. La secuencia de mensajes supone que se ha establecido un enlace seguro SNMPv3.

- El NMS lee datos de la base de datos del PS utilizando la petición SNMP GET. La petición enumera los objetos específicos que el NMS desea obtener de la base de datos.
- El agente SNMP del CMP consulta la base de datos del PS para obtener los parámetros especificados.
- El SNMP del CMP comunica los datos al NMS mediante la respuesta SNMP GET.

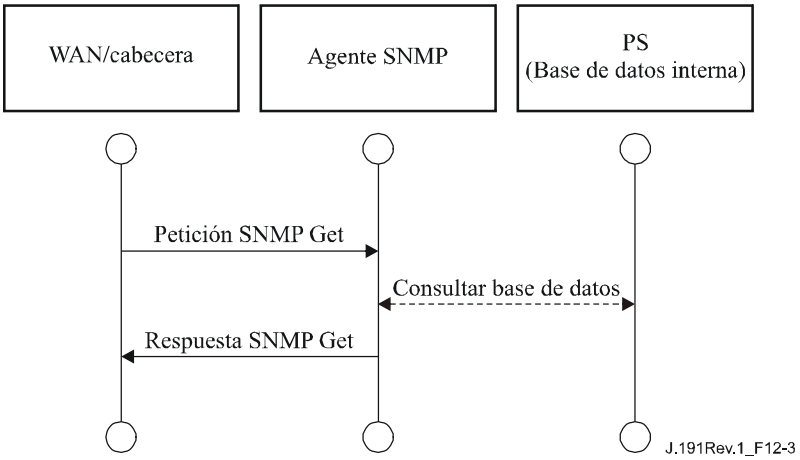


Figura 12-3/J.191 – Diagrama secuencial del acceso a la base de datos del PS desde la interfaz WAN-Man del PS

12.3.2 Reconfiguración

12.3.2.1 Descarga de soporte lógico del PS

La figura 12-4 ilustra el proceso de descarga de soporte lógico y de microprogramas con destino a un PS en el modo de configuración SNMP. Este proceso lo activa el NMS. Se comunica al PS dónde puede conseguir el nuevo fichero de código de soporte lógico. Una vez completada la descarga del fichero de código, el PS comprobará que no se ha corrompido la imagen durante la descarga. Se efectúa la autenticación para verificar que el fichero de código es de confianza. Tras dicho paso, se rearranca el sistema.

Tras el rearranque, el PS reanuda su funcionamiento con la nueva imagen de soporte lógico. Es posible que el PS necesite volver a configurarse tras la actualización del soporte lógico, y que haya que proporcionar de nuevo las interfaces de la WAN (no se indica). Si el PS no acepta la nueva imagen de soporte lógico, regresará a la versión de soporte lógico anterior (copia de seguridad) e informará al NMS de lo ocurrido.

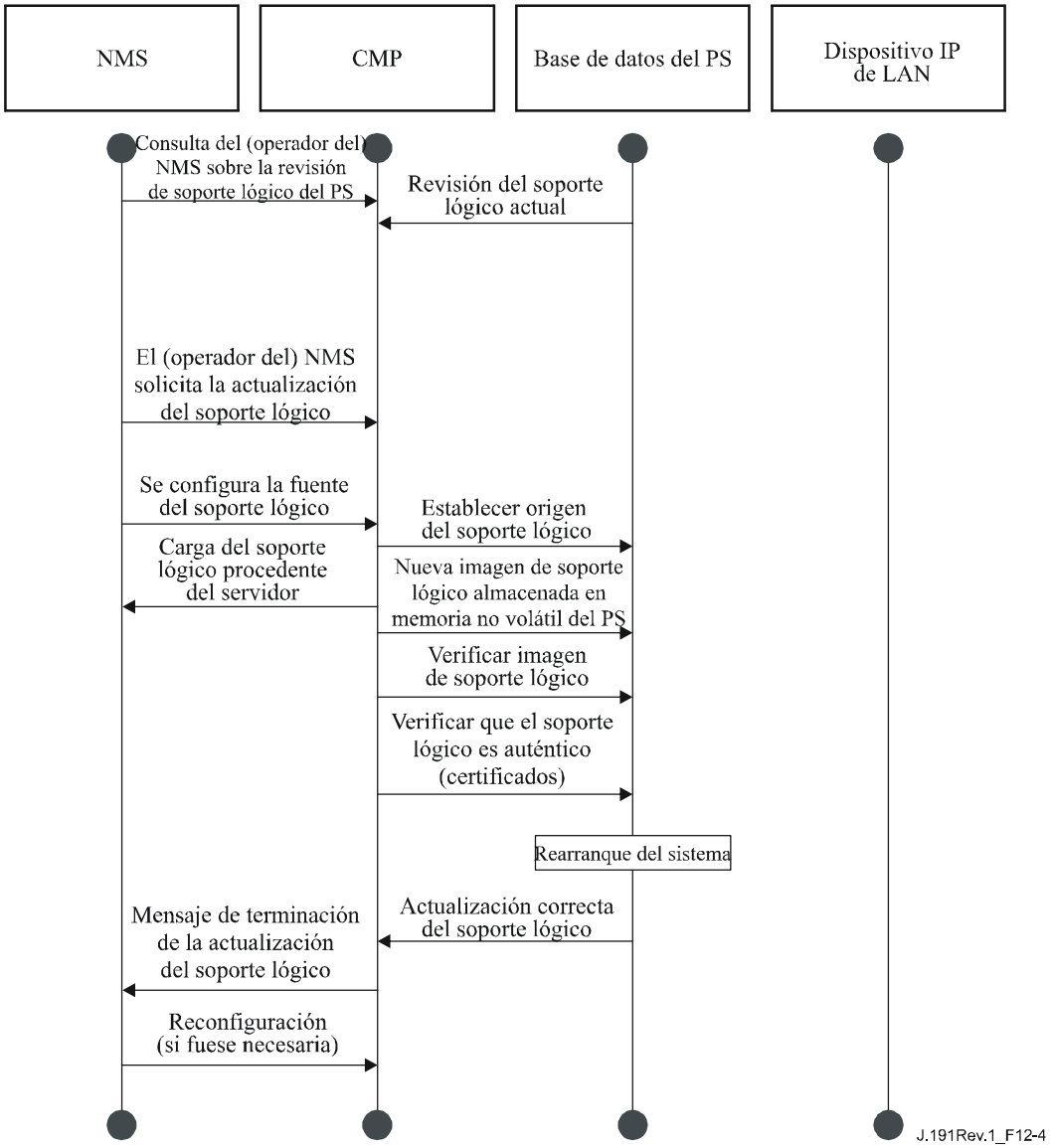


Figura 12-4/J.191 – Diagrama secuencial de la descarga de soporte lógico del PS

12.3.2.2 Descarga del fichero de configuración del PS

La figura 12-5 ilustra la reconfiguración de un PS en el modo de configuración SNMP, mediante la descarga del fichero configuración. Este proceso lo activa el NMS. El fichero de configuración llega al PS escribiendo en el PS el nombre del servidor y del fichero y activando en el PS la descarga del fichero. Una vez cargado el fichero de configuración, se interpretan los mandatos que contiene. Si no se entiende alguno de los mandatos o no son aplicables, se saltan y se genera un evento. Cuando el PS ha completado el proceso del fichero configuración, graba el número de tuplas TLV procesadas y omitidas de los objetos correspondientes de la MIB.

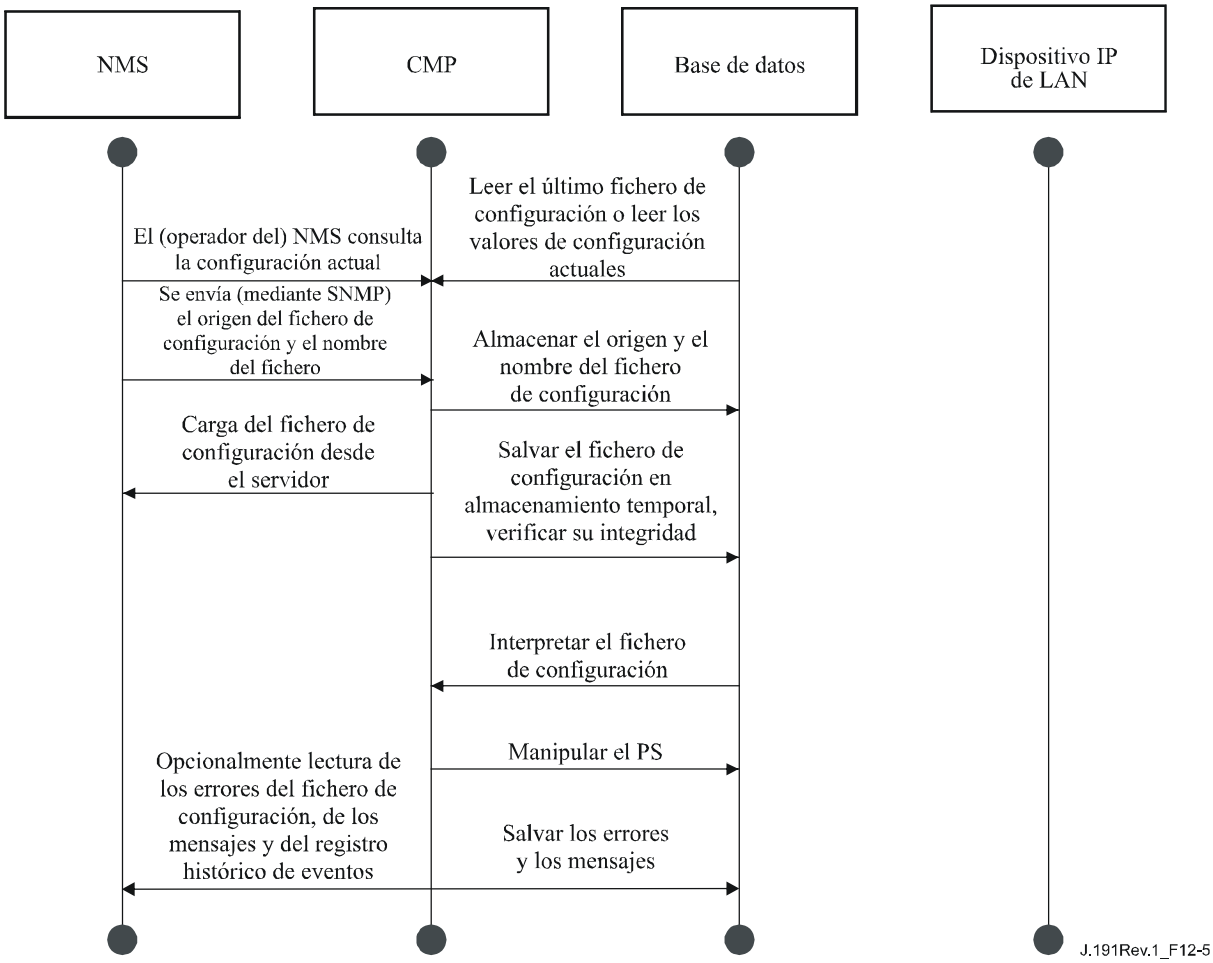


Figura 12-5/J.191 – Diagrama secuencial de la reconfiguración del PS (descarga del fichero de configuración)

12.4 Acceso a la MIB

12.4.1 Configuración del VACM

El operador de cable controla el dominio de gestión. En la figura 12-6 se muestra un ejemplo de configuración de los parámetros del VACM.

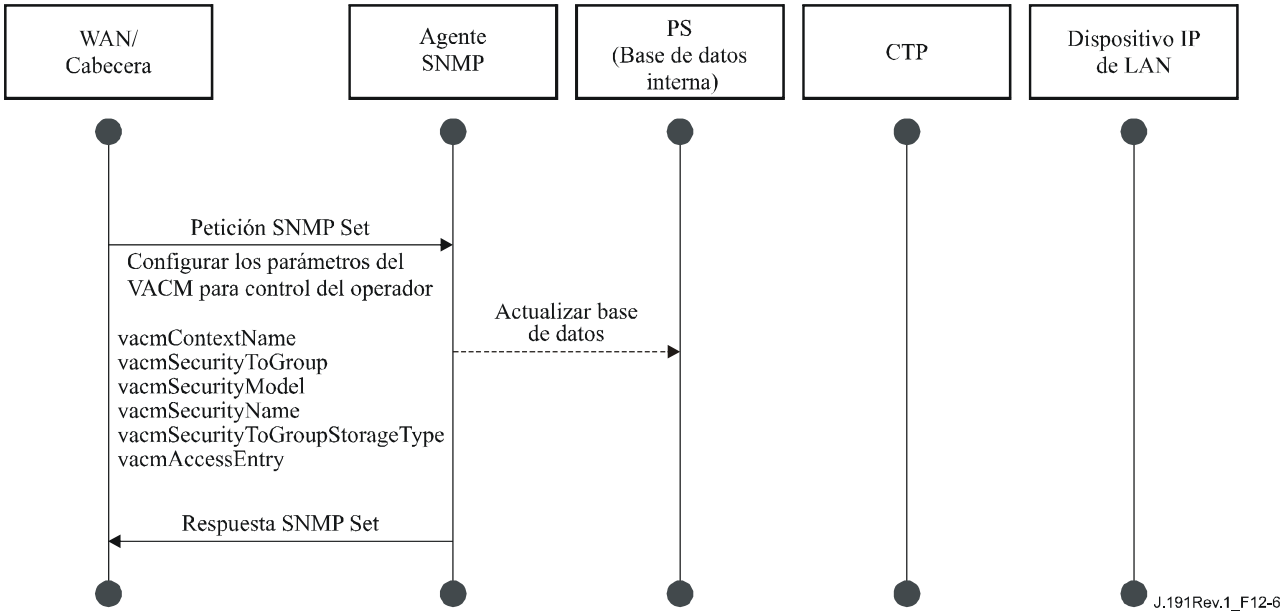


Figura 12-6/J.191 – Secuencia de configuración del PS (parámetros del VACM)

12.4.2 Configuración de la mensajería de eventos de gestión

12.4.2.1 Funcionamiento de la notificación de eventos del CMP

Los eventos se comunican mediante la anotación histórica local de eventos, los mensajes SNMP TRAP y SNMP INFORM y mediante SYSLOG. El mecanismo de notificación de eventos puede fijarlo o modificarlo el NMS mediante la emisión de un mensaje de petición SNMP Set dirigido a la dirección WAN-Man del PS.

La figura 12-7 ilustra la configuración de la base de datos del PS para almacenar eventos en ficheros de registro histórico local. Los eventos históricos locales son de dos tipos: no volátiles locales y volátiles locales. El NMS lee el contenido del registro histórico local y escribe dicho contenido en el sistema de anotaciones históricas de eventos de la cabecera. El rearranque del PS provoca que los eventos volátiles desaparezcan de la base de datos del PS. Los eventos no volátiles se mantienen tras los rearranques.

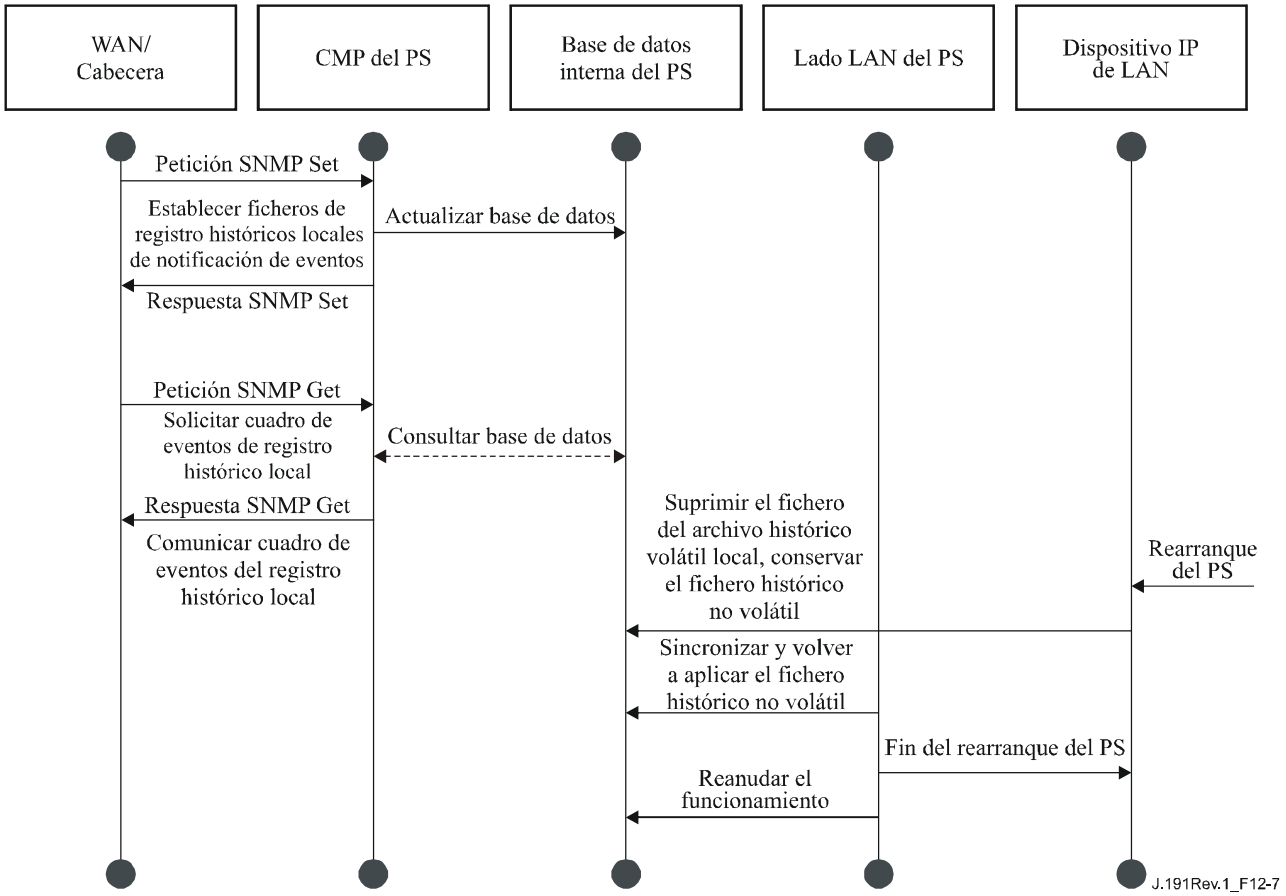


Figura 12-7/J.191 – Secuencia de la configuración del PS (control de eventos)

La figura 12-8 ilustra la descarga de un fichero de configuración para un PS que se encuentra en el modo de configuración SNMP. Este proceso se activa mediante una petición SNMP Set. El PS debe verificar este fichero antes de aceptarlo. En el ejemplo, existe un error TLV que se comunica. Como la notificación de eventos se ha puesto en el modo SNMP TRAP, la dirección del servidor TRAP se recupera de la base de datos del PS y el evento se envía al servidor TRAP.

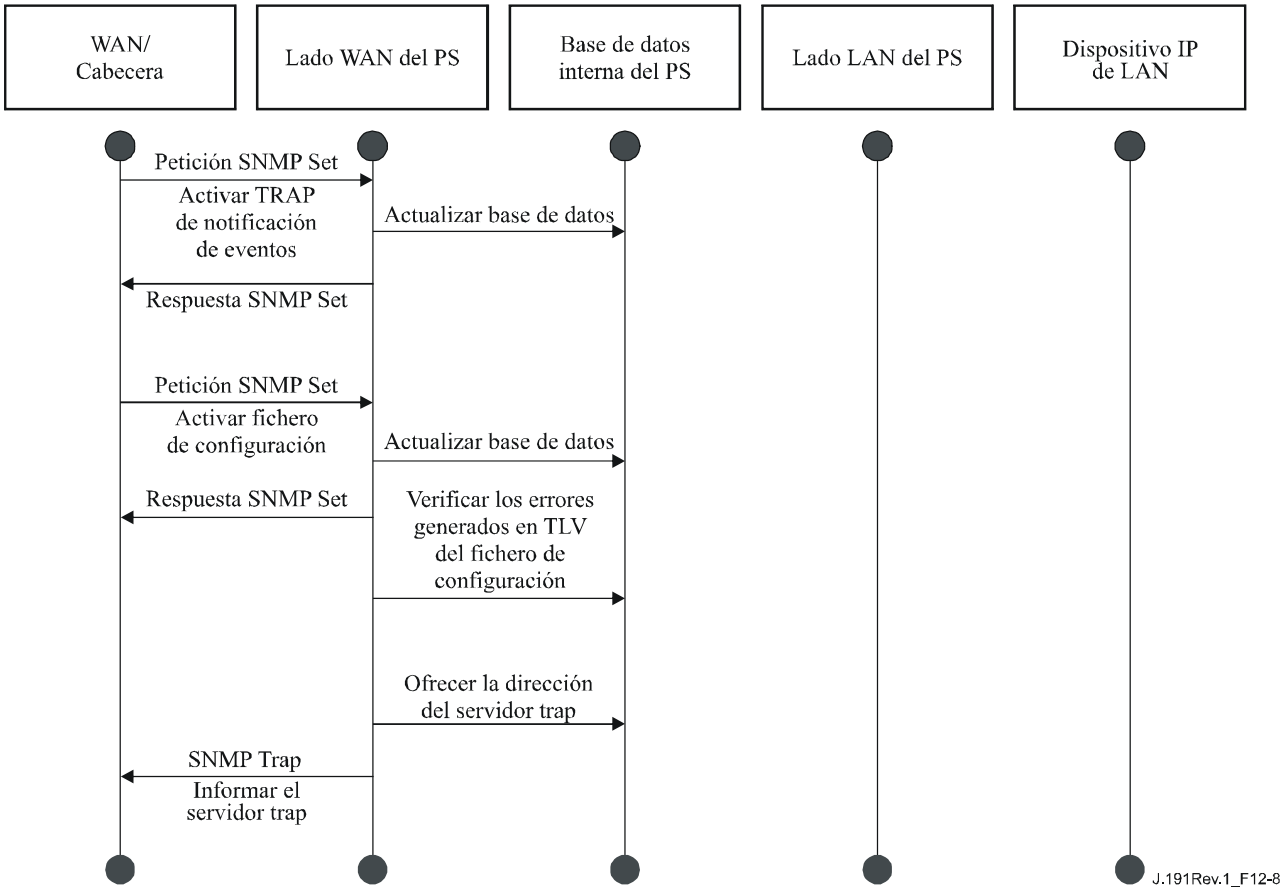


Figura 12-8/J.191 – Secuencia de descarga del fichero de configuración del PS (con TLV no válidos)

En la figura 12-9 se ilustra el proceso de obtención por parte de un dispositivo IP de LAN de una dirección IP del servidor DHCP local (CDS). La función CDS comprueba si hay direcciones IP disponibles en la base de datos del PS. En este caso, el CDS detecta que no hay direcciones IP disponibles del grupo de direcciones y genera un evento para el SYSLOG.

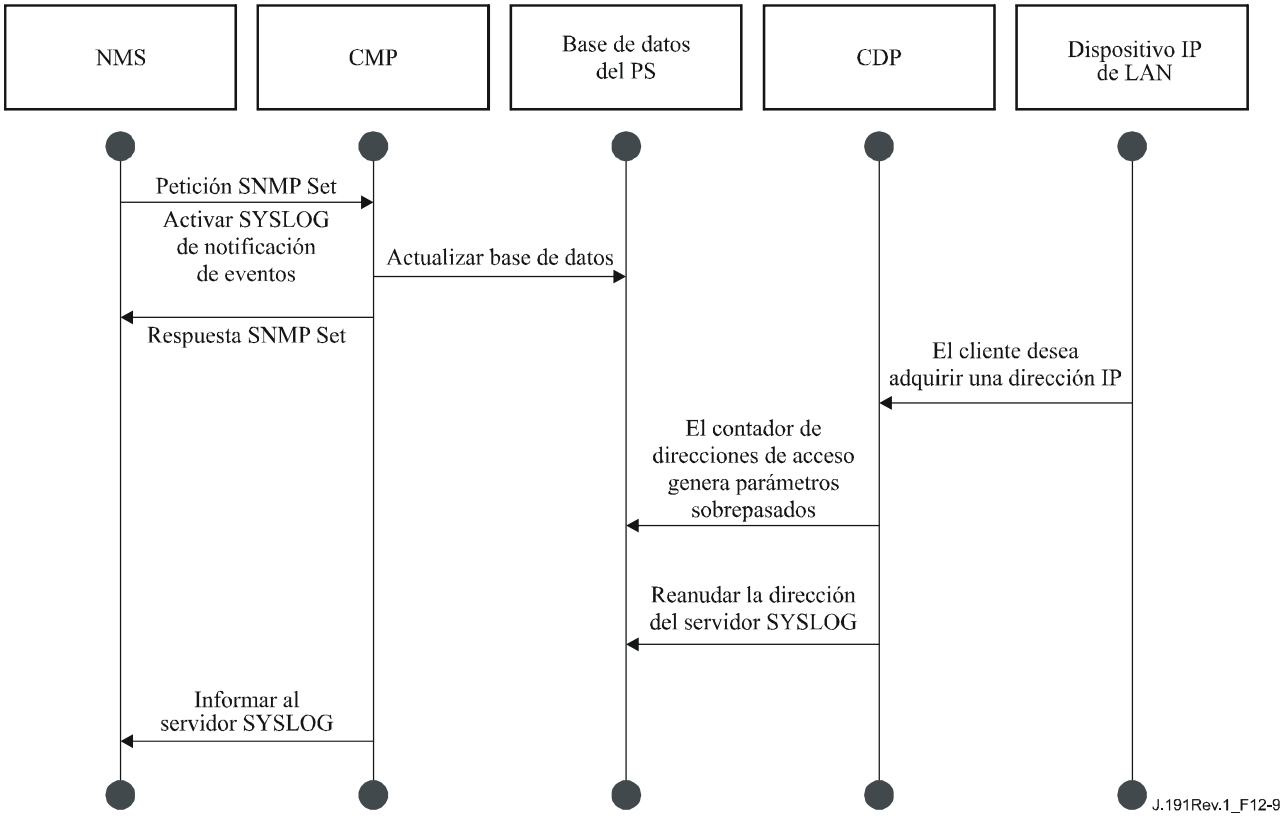


Figura 12-9/J.191 – Secuencia de adquisición de direcciones del dispositivo IP de LAN (la petición sobrepasa el contador suministrado)

12.4.2.2 Ejemplo de funcionamiento del estrangulamiento y limitación de eventos del CMP

Se proporciona un mecanismo de estrangulamiento a través de la funcionalidad CMP del PS. El estrangulamiento y la limitación de eventos son muy flexibles pudiendo incluir casos en los que todos los eventos se comuniquen y casos en los que no se comunique ningún evento al NMS. En 6.5.3 se describe el mecanismo de estrangulamiento y limitación de eventos del CMP.

La figura 12-10 ilustra la configuración de la base de datos del PS para que devuelva eventos mediante el método SNMP INFORM. Inicialmente, se escriben varios mensajes INFORM en el fichero histórico local y se entregan al NMS. El mecanismo de estrangulamiento de eventos establece el límite del número de eventos que pueden enviarse al NMS en un determinado periodo de tiempo. Cuando se alcanza dicho límite, el PS detiene el envío de mensajes INFORM al NMS. Para reiniciar la notificación de eventos, el NMS debe reactivar la comunicación de eventos.

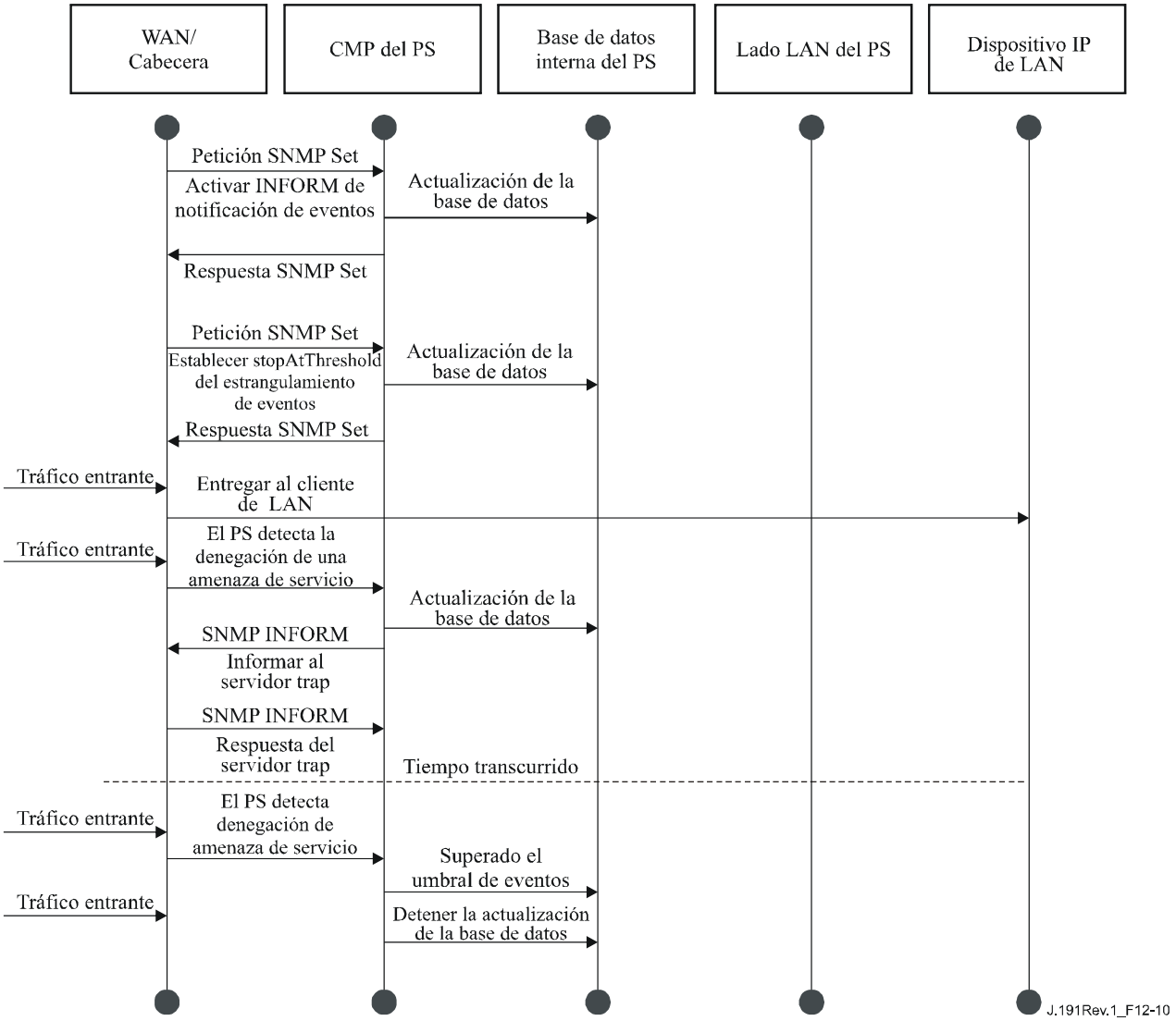


Figura 12-10/J.191 – Operación de estrangulamiento y limitación de eventos del CMP

13 Procesos de configuración

Esta cláusula describe los procesos implicados en la utilización de las herramientas de prestación, descritas en la cláusula 7, para la prestación inicial del dispositivo IP de LAN y del elemento PS. La prestación se descompone en las tres tareas siguientes:

1) Adquisición de las direcciones de red.

2) Adquisición de información del servidor.

3) Descarga y procesamiento seguros del fichero de configuración del PS.

Los procesos de prestación descritos en esta cláusula corresponden a cada uno de los siguientes casos de interés:

- Prestación WAN-Man del PS de la funcionalidad de gestión basada en la WAN del PS.
- Prestación WAN-Data del PS de las direcciones IP WAN-Data del PS que sirven para crear correspondencias CAT con dispositivos IP de LAN del sector de direcciones LAN-Trans.
- Prestación de dispositivo IP de LAN en el sector LAN-Trans correspondiente a un dispositivo IP de LAN con una dirección IP traducida.

- Prestación de dispositivo IP de LAN en el sector LAN-Pass correspondiente un dispositivo IP de LAN con dirección IP que se hace llegar a la WAN.

La prestación del elemento módem de cable de un PS integrado es independiente y distinta de la prestación del PS y ajena al objeto de la presente Recomendación. Se remite al lector a las Recomendaciones relativas a módems de cable que describen la prestación del módem de cable.

Los elementos funcionales con los que interactúa el elemento de servicios de portal durante los procesos de prestación enumerados anteriormente se identifican en la figura 13-1. El elemento funcional centro de distribución de claves (KDC) se muestra con un perfil discontinuo ya que se utiliza en el modo de configuración SNMP aunque no en el modo de configuración DHCP. Los demás elementos funcionales se utilizan en ambos modos de prestación.

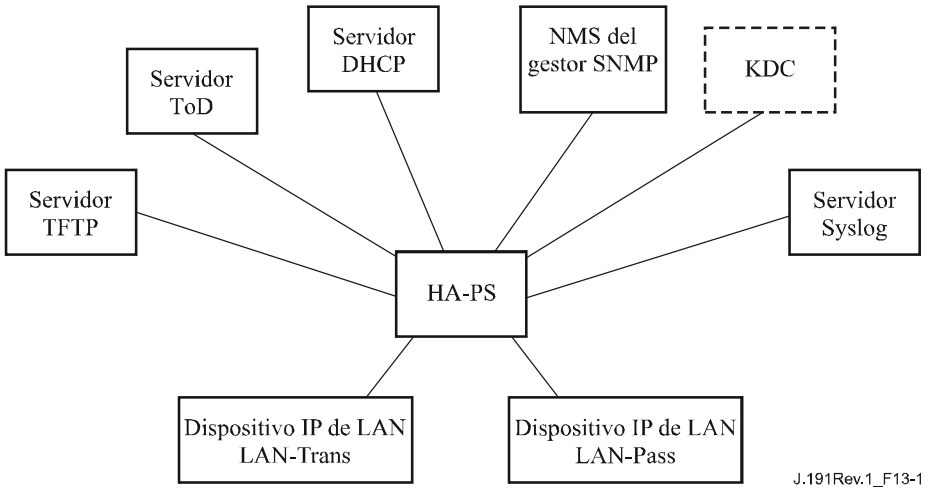


Figura 13-1/J.191 – Elementos funcionales de la prestación

El servidor del protocolo de transferencia de fichero trivial (TFTP, *trivial file transfer protocol*) permite al PS el acceso al fichero de configuración del PS y cumple las reglas descritas en RFC 1350. El servidor de hora del día (ToD) proporciona al PS los medios de adquirir la hora actual en formato UTC como se explica en RFC 868. El protocolo dinámico de configuración de anfitrión (DHCP) proporciona al PS direcciones IP mundiales y/o privadas de acuerdo con RFC 2131 y proporciona asimismo otra información mediante las opciones del DHCP de acuerdo con RFC 2132. El gestor del protocolo simple de gestión de red (SNMP, *simple network management protocol*) del sistema de gestión de la red (NMS, *network management system*) cumple RFC 1157 y probablemente con versiones más recientes del SNMP, por ejemplo [RFC 2576], [RFC 3412], [RFC 3414] y [RFC 3415]. El centro de distribución de claves (KDC) gestiona las claves de autorización y criptación que permiten establecer la confianza entre los elementos en red y las reglas implementadas definidas en RFC 1949. El servidor del registro de sistema (SYSLOG, *system log*) maneja los mensajes de eventos generados por el PS y por los dispositivos IP de LAN en el hogar. El PS implementa clientes para estos servidores de cabecera y utiliza estas funciones de cliente durante los procesos de prestación descritos en esta cláusula para llevar a cabo las tareas enumeradas al principio de esta cláusula.

13.1 Modos de configuración

Las cláusulas 5.5 y 7.1.1 introducen dos modos de prestación soportados por el elemento de servicio de portal: el modo de configuración DHCP y el modo de configuración SNMP. Esta cláusula expone con más detalle dichos modos. La figura 13-2 ilustra un posible flujo de eventos de los dos modos de prestación. El punto clave de la figura 13-2 es la disyuntiva utilizada por el PS para determinar el modo de configuración en el que operar.

El PS funciona en el modo de configuración DHCP (modo DHCP) si el servidor DHCP de la red de cable proporciona una dirección IP válida para el servidor TFTP en el campo 'siaddr' del mensaje DHCP, proporciona un nombre de fichero válido para el fichero de configuración del PS en el campo 'file' del mensaje DHCP y NO proporciona la subopción 51 de la opción 177 del DHCP a la CDC del PS, durante la fase DHCPOFFER del proceso de inicialización. El modo de configuración DHCP tiene por objeto permitir que el PS funcione en una infraestructura J.112 con pocas o ninguna modificación a la red DOCSIS.

El modo de configuración SNMP del PS se activa cuando el servidor DHCP de la red de cable NO proporciona valores para 'siaddr' y 'file', y cuando el servidor DHCP de la red de cable SÍ envía la subopción 51 de la opción 177 del DHCP. El modo de configuración SNMP tiene por objeto permitir que el PS aproveche las características avanzadas de la infraestructura IPCablecom.

El PS utilizará por defecto el modo CableHome aletargado si no recibe ninguno de los campos o las subopciones que se han definido como activadores de los modos de configuración DHCP y de configuración SNMP, o si recibe una combinación inválida de los campos y las subopciones.

En la figura 13-2 no se muestran todas las condiciones de error. Véase 7.2.3.3 para obtener una descripción del comportamiento del PS en el caso de criterios de decisión incorrectos en el modo de configuración.

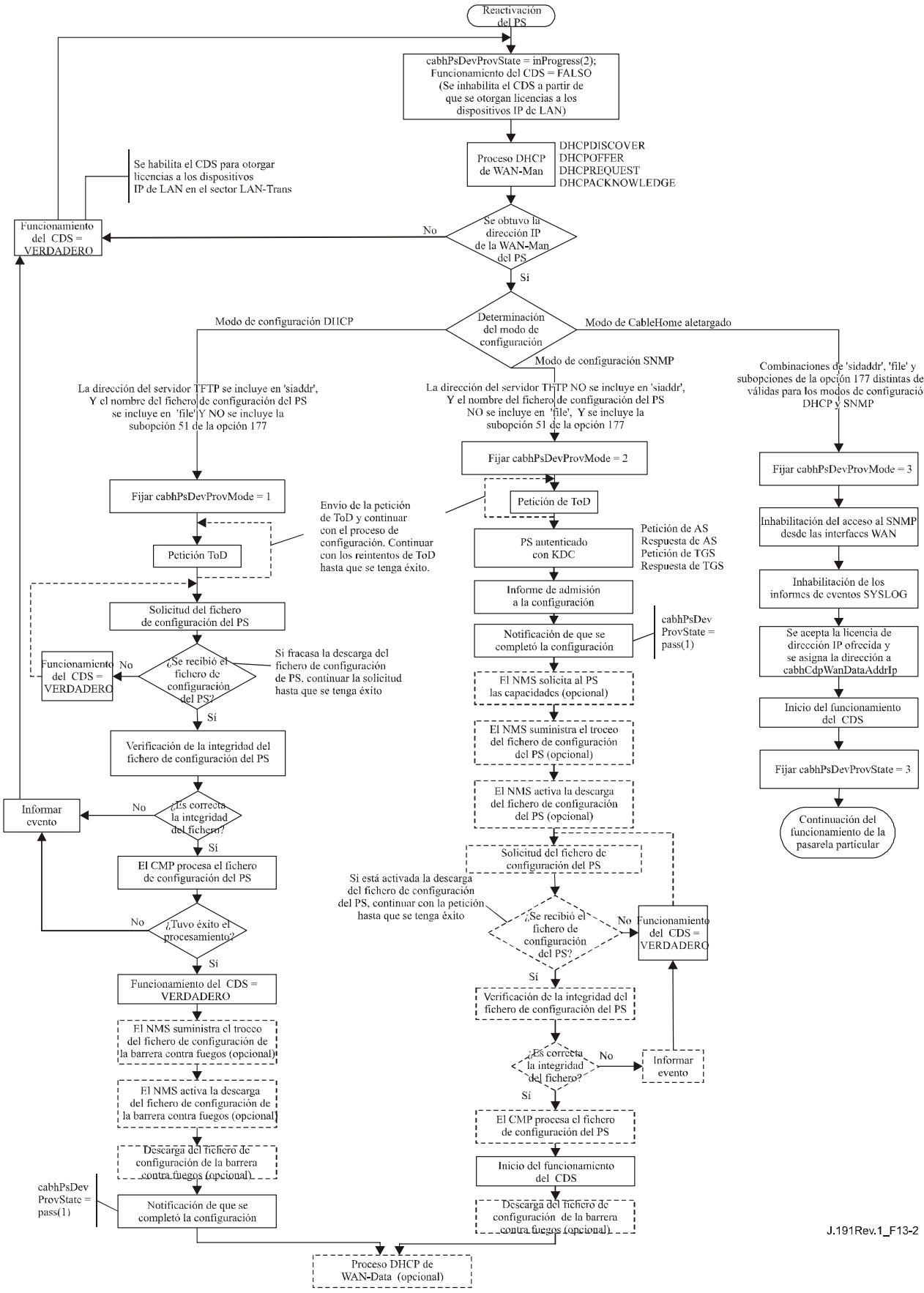


Figura 13-2/J.191 – Modos de configuración

13.2 Proceso de prestación de la gestión del PS: modo de configuración DHCP

El PS solicita del sistema de prestación de cabecera una dirección IP para el intercambio de los mensajes de gestión entre el NMS y el PS. El PS analiza el mensaje DHCP devuelto en el DHCP OFFER y toma una decisión en cuanto al modo de configuración bajo el que va a funcionar (véase 7.2.3.3). La cláusula 7.2.2.2.2 describe tres modos de direcciones WAN soportados para la adquisición de direcciones IP por parte del PS a obtener del servidor DHCP de la red de cable.

Si el PS adopta la decisión de que va a funcionar en el modo de configuración DHCP, utiliza la información del fichero de configuración del PS recibida en el mensaje DHCP como activador para descargar el fichero de configuración del PS de acuerdo con lo descrito en 7.2. La descarga del fichero de configuración del PS es un requisito para el PS cuando funciona en el modo de configuración DHCP pero es opcional para el PS cuando funciona en el modo de configuración SNMP.

En el modo de configuración DHCP el PS (CMP) utiliza por defecto el modo NmAccess para el intercambio de mensajes de gestión con el NMS, no obstante lo cual el NMS puede configurar el modo de coexistencia en el CMP. Estos modos de mensajería de gestión se describen en 6.3.3.

En la figura 13-3 y el cuadro 13-1 se describen las secuencias de los mensajes necesarios para inicializar el funcionamiento del PS en el modo de configuración DHCP. El proceso de configuración de un PS que funciona en dicho modo es el mismo para el PS integrado en un módem de cable que para el PS autónomo. La configuración para el PS integrado NO DEBE producirse antes del proceso de configuración del módem de cable. La configuración de la gestión del PS autónomo DEBERÍA producirse justo después de la puesta en marcha/reactivación.

El proceso opcional de descarga del fichero de configuración de la barrera contra fuegos se muestra sombreado en la figura 13-3.

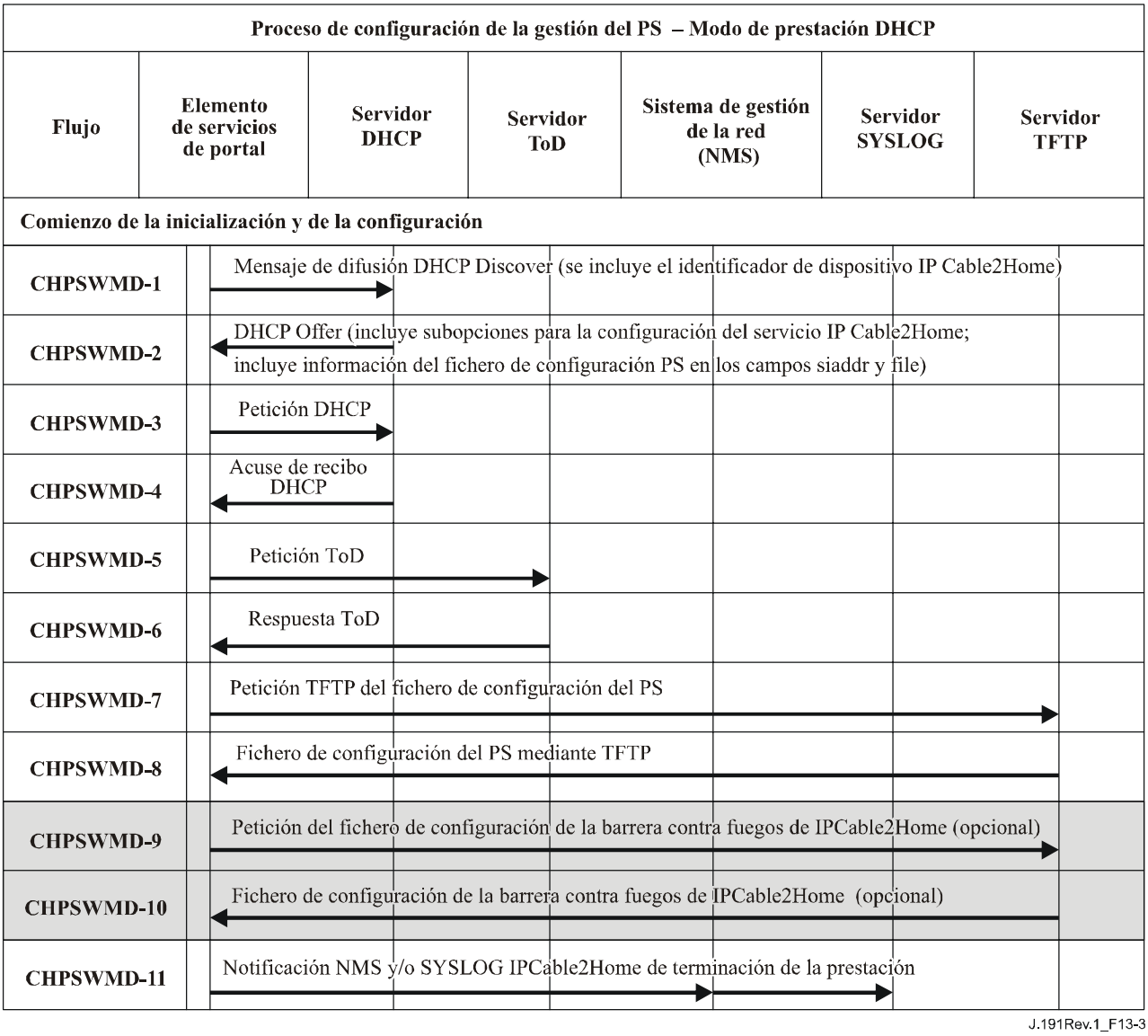


Figura 13-3/J.191 – Proceso de prestación de la gestión del PS – Modo de prestación DHCP

El cuadro 13-1 describe los mensajes CHPSWMD-1 a CHPSWMD-11 mostrados en la figura 13-3.

Cuadro 13-1/J.191 – Descripciones del flujo del proceso de prestación PS WAN-Man en el modo de configuración DHCP

Fase	Prestación WAN-Man del PS: Modo de prestación DHCP	Secuencia normal	Secuencia de fallo
CHPSWMD-1	*Mensaje de difusión DHCP discover* El CDP (CDC) envía un mensaje de difusión DHCP DISCOVER para conseguir la dirección IP de WAN-M que se describe en 7.2.3.3. El mensaje de difusión DHCP DISCOVER enviado por el CDP (CDC) incluye las opciones obligatorias que recoge el cuadro 7-7. El PS pone cabhPsDevProvState en la condición 'inProgress (2)' cuando el CDC envía un mensaje de difusión DHCP DISCOVER. El PS DEBE iniciar el temporizador de prestación con el valor inicial accesible a través de cabhPsDevProvTimer Y otorgar a cabhPsDevProvState el estado 'inProgress' (2) cuando el CDC envía un mensaje de difusión DHCP DISCOVER.	Comenzar la secuencia de prestación.	Si ha fallado de acuerdo con el protocolo DHCP comunicar un error y continuar reintentando mensajes DHCP Broadcast Discover hasta tener éxito (volver a la fase CHPSWMD-1). Si fracasa el primer intento para conseguir una dirección IP de la WAN-Man, el PS inicia el funcionamiento del CDS como se especifica en 7.2.3.3.
CHPSWMD-2	*DHCP OFFER* El DHCP OFFER emitido por el servidor DHCP de la red de cable no debe incluir el código de opción CableHome 177 con las subopciones 3, 6 y 51 Y debe incluir información del fichero de configuración del PS en los campos siaddr y file del mensaje DHCP. (Véase 7.2.3.3.)	CHPSWMD-2 DEBE tener lugar una vez completada CHPSWMD-1.	Si se falla respecto al protocolo DHCP volver a CHPSWMD-1 y comunicar el error.
CHPSWMD-3	*DHCP REQUEST* El CDP DEBE enviar al servidor DHCP adecuado un mensaje DHCP REQUEST para aceptar el DHCP OFFER.	CHPSWMD-3 DEBE tener lugar una vez completada CHPSWMD-2.	Si se falla respecto al protocolo DHCP volver a CHPSWMD-1 y comunicar el error.
CHPSWMD-4	*DHCP ACK* El servidor DHCP envía al CDP un mensaje DHCP ACK que contiene una dirección IPv4 del PS. El PS modifica cabhPsDevProvMode basándose en la información que recibe en el DHCP ACK (véase 7.2.3.3). El PS DEBE guardar la dirección del servidor de hora del día en cabhPsDevTimeServerAddr.	CHPSWMD-4 DEBE tener lugar una vez completada CHPSWMD-3.	Si se falla respecto al protocolo DHCP volver a CHPSWMD-1 y comunicar el error. Si no se recibe la información prevista del fichero de configuración en el mensaje DHCP ACK después del quinto intento, el PS funcionará en el "modo CableHome aletargado" que se describe en 5.5 y 7.2.3.3.

Cuadro 13-1/J.191 – Descripciones del flujo del proceso de prestación PS WAN-Man en el modo de configuración DHCP

Fase	Prestación WAN-Man del PS: Modo de prestación DHCP	Secuencia normal	Secuencia de fallo
CHPSWMD-5	*Petición de hora del día (ToD) conforme a RFC 868* El PS emite una petición ToD al servidor ToD identificado en el DHCP OFFER.	CHPSWMD-5 DEBE tener lugar una vez completada CHPSWMD-4.	Continuar en CHPSWMD-6.
CHPSWMD-6	*Respuesta ToD* El servidor ToD debe responder la hora actual en formato UTC.	CHPSWMD-6 DEBE tener lugar una vez completada CHPSWMD-5.	Continuar en CHPSWMD-7, comunicar el error y volver a CHPSWMD-5 (continuar reintentando ToD hasta que tenga éxito).
CHPSWMD-7	*Petición TFTP* El PS funcionando en el modo de configuración DHCP envía al servidor TFTP un TFTP Get Request solicitando el fichero de datos de configuración especificado descrito en 7.3.3.	CHPSWMD-7 DEBE tener lugar una vez completada CHPSWMD-5. CHPSWMD-7 PUEDE tener lugar antes de completar CHPSWMD-6.	Continuar en CHPSWMD-8.
CHPSWMD-8	*El servidor TFTP envía el fichero de configuración del PS* Tras la recepción del fichero de configuración del PS, se verifica el troceo. Véase 7.3.3.3. El fichero de configuración del PS se procesa acto seguido. Consúltese 7.3.3 en relación con el contenido del fichero de configuración del PS. Opcionalmente, la dirección IP del servidor TFTP del fichero de configuración de la barrera contra fuegos, el nombre del fichero de configuración de la barrera contra fuegos y el troceo del fichero de configuración de la barrera contra fuegos se incluyen en el fichero de configuración del PS si ha de cargarse un fichero de configuración de la barrera contra fuegos, y éste es el método seleccionado para especificarlo.	CHPSWMD-8 DEBE tener lugar una vez completada CHPSWMD-7	Si falla la descarga TFTP, comunicar un error y volver a CHPSWMD-7 (continuar reintentando la descarga del fichero de configuración del PS). Si el proceso del fichero de configuración del PS provoca un error continuar en CHPSWMD-9 y comunicar el error como evento. Si expira el temporizador de prestación antes de la descarga con éxito del fichero de configuración del PS, el PS DEBE comunicar un error y volver a CHPSWMD-1.

Cuadro 13-1/J.191 – Descripciones del flujo del proceso de prestación PS WAN-Man en el modo de configuración DHCP

Fase	Prestación WAN-Man del PS: Modo de prestación DHCP	Secuencia normal	Secuencia de fallo
CHPSWMD-9	*Petición TFTP – fichero de configuración de la barrera contra fuegos (Opcional)* Si el PS recibe información del fichero de configuración de la barrera contra fuegos (servidor TFTP de la barrera contra fuegos y nombre del fichero de configuración de la barrera contra fuegos) en el fichero de configuración del PS, el PS envía al servidor TFTP de configuración de la barrera contra fuegos un TFTP Get Request solicitando un fichero de configuración de la barrera contra fuegos (véase 11.3.5.1). Si el PS no recibe información de un fichero de configuración de la barrera contra fuegos en el fichero de configuración del PS, el proceso de prestación del PS (en el modo de configuración DHCP) DEBE saltarse las fases CHPSWMD-9 y CHPSWMD-10 y continuar en la fase CHPSWMD-11.	Si CHPSWMD-9 tiene lugar, DEBE hacerlo una vez terminada CHPSWMD-8.	Si falla el TFTP, continuar el funcionamiento del PS pero comunicar un error y continuar reintentado CHPSWMD-9.
CHPSWMD-10	*El servidor TFTP envía el fichero de configuración de la barrera contra fuegos (Opcional)* Si tiene lugar la fase CHPSWMD-9, el servidor TFTP envía al PS una respuesta TFTP con el fichero solicitado. Tras la recepción del fichero de configuración de la barrera contra fuegos se calcula el troceo del fichero de configuración y se compara con el valor recibido en el fichero de configuración del PS. A continuación se procesa el fichero. Consúltese 11.3.5.	CHPSWMD-10 DEBE tener lugar una vez completada CHPSWMD-9	Si falla el TFTP continuar con el funcionamiento del PS pero comunicar un error y continuar reintentando CHPSWMD-9. Si el proceso del fichero de configuración de la barrera contra fuegos provoca un error, continuar y comunicar el error como evento.

Cuadro 13-1/J.191 – Descripciones del flujo del proceso de prestación PS WAN-Man en el modo de configuración DHCP

Fase	Prestación WAN-Man del PS: Modo de prestación DHCP	Secuencia normal	Secuencia de fallo
CHPSWMD-11	*Fin de la prestación* Si lo solicita el sistema de prestación, se requiere al PS que informe al sistema de prestación del estado de prestación del PS. El sistema de prestación podría solicitar al PS que enviase un mensaje SYSLOG, una trampa SNMP, o ambos. Si el PS completa con éxito todas las fases requeridas desde CHPSWMD-1 hasta CHPSWMD-10 Y el PS recibió una dirección de servidor SYSLOG en el DHCP OFFER, el PS DEBE enviar un mensaje de prestación completa al servidor SYSLOG con el estado de prestación PASS. Si el PS completa con éxito todas las fases de prestación desde CHPSWMD-1 a CHPSWMD-10 Y el PS recibió parámetros válidos para docsDevNmAccessGroup identificando el receptor de trampas (docsDevNmAccessIP) y configurando la trampa de prestación completa (cabhPsDevInitTrap) para 'read only with Traps' (establecer el control docsDevNmAccess en '4'. Consúltese RFC 2669), el PS DEBE enviar una trampa de prestación completa (cabhPsDevInitTrap) con los parámetros adecuados al receptor de trampas. Si el temporizador de prestación del PS expira antes de completar las fases necesarias desde CHPSWMD-1 a CHPSWMD-10 Y el PS recibió una dirección de servidor SYSLOG en el DHCP OFFER, el PS DEBE enviar un mensaje de prestación completa al servidor SYSLOG con el estado de prestación fijado en FAIL.	CHPSWMD-11 DEBE tener lugar una vez completada CHPSWMD-10	Si falla la trampa SNMP, el servidor de prestación puede desconocer que se ha completado el proceso de prestación salvo que consulte el objeto cabhPsProvState.

Cuadro 13-1/J.191 – Descripciones del flujo del proceso de prestación PS WAN-Man en el modo de configuración DHCP

Fase	Prestación WAN-Man del PS: Modo de prestación DHCP	Secuencia normal	Secuencia de fallo
	Si el temporizador de prestación del PS expira antes de completar todos los pasos necesarios desde CHPSWMD-1 a CHPSWMD-10 Y si el PS recibió parámetros válidos para el receptor de notificaciones, el PS DEBE enviar una notificación de prestación fallida (cabhPsDevInitTrap) al receptor de notificaciones. El PS DEBE actualizar el valor de cabhPsDevProvState con el estado 'pass' (1) cuando las fases de la prestación CHPSWMD-1 a CHPSWMD-11 se completen con éxito. El PS DEBE actualizar el valor de cabhPsDevProvState con el estado 'fail' (3) Y comunicar un evento que indique el fallo del proceso de prestación si el temporizador de prestación del PS expira antes de actualizar el valor de cabhPsDevProvState con el estado 'pass'.		

13.3 Proceso de prestación de la gestión del PS: Modo de prestación SNMP

El PS solicita una dirección de red WAN-Man del servidor DHCP de cabecera para el intercambio de los mensajes de gestión entre las funciones de gestión del PS y el NMS de la red de cable. Si, en base el procedimiento descrito en 7.3.3.3, el PS determina que ha de operar en el modo de configuración SNMP, el PS asegura sus mensajes de gestión mediante SNMPv3, ciñéndose al procedimiento de autenticación descrito en 11.3.3.

El NMS de la red de cable puede opcionalmente encargar al PS (CMP) funcionando en el modo de configuración SNMP que descargue un fichero de configuración del PS del servidor TFTP. La notificación de la terminación del proceso de prestación se efectúa mediante el proceso de comunicación de eventos descrito en 6.5.

La figura 13-4 ilustra los flujos de mensajes que han de utilizarse para la prestación del PS cuando funciona en el modo de configuración SNMP. El proceso de prestación para la interfaz WAN-Man del PS es idéntico para el PS integrado y para el PS autónomo. La prestación del PS autónomo DEBERÍA tener lugar justo después de la puesta en marcha/reactivación.

El proceso de prestación para la interfaz WAN-Man de un PS que funciona en el modo de configuración SNMP DEBE tener lugar de acuerdo con la secuencia descrita en la figura 13-4 y definida en detalle en el cuadro 13-2. Los pasos opcionales se muestran sombreados en la figura 13-4. Estos pasos opcionales pueden tener lugar inmediatamente después de la fase CHPSWMS-13 con posterioridad a ésta o no tener lugar en absoluto.

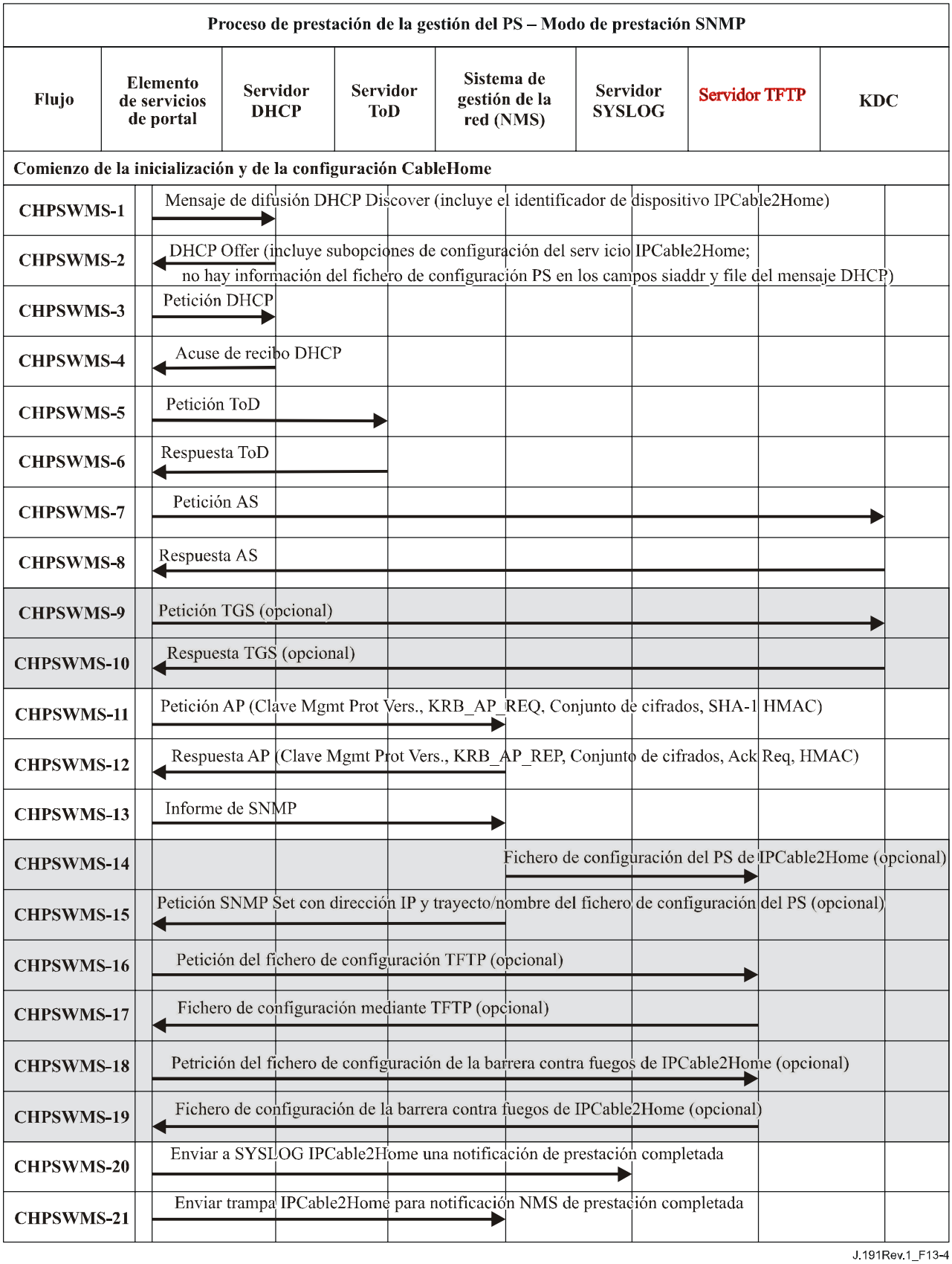


Figura 13-4/J.191 – Proceso de prestación de la gestión del PS – Modo de prestación SNMP

En el cuadro 13-2 se describen los pasos del proceso de configuración mostrado en la figura 13-4.

Cuadro 13-2/J.191 – Descripciones del flujo del proceso de configuración WAN-Man del PS en el modo de configuración SNMP

Fase	Configuración WAN-Man del PS: Modo de configuración SNMP	Secuencia ordinaria	Secuencia de fallo
CHPSWMS-1	*Mensaje de difusión DHCP Discover* El CDP (CDC) difunde un mensaje DHCP DISCOVER para conseguir la dirección IP de WAN-Man como se describe en 7.2.3. Esta difusión incluye las opciones obligatorias relacionadas en el cuadro 7-7. El PS inicia la supervisión del tiempo transcurrido Y pone cabhPsDevProvState en el estado 'inProgress' (2) cuando el CDC difunde su mensaje inicial DHCP DISCOVER.	Comenzar la secuencia de configuración.	Si el fallo ocurre en relación con el protocolo DHCP comunicar un error y continuar reintentando el mensaje de difusión DHCP Discover hasta tener éxito (volver a CHPSWMS-1). Si fracasa el primer intento para conseguir una licencia de dirección del servidor DHCP de cabecera, se inicia el funcionamiento del CDS como se especifica en 7.2.3.3.
CHPSWMS-2	*DHCP OFFER* El DHCP OFFER emitido por el servidor DHCP de la red de cable debe incluir el código de opción 177 con las subopciones 3, 6 y 51 Y no debe figurar información del fichero de configuración del PS en los campos siaddr y file del mensaje DHCP.	CHPSWMS-2 DEBE tener lugar tras completarse CHPSWMS-1.	Si el fallo ocurre en virtud del protocolo DHCP volver a CHPSWMS-1 y comunicar un error.
CHPSWMS-3	*DHCP REQUEST* El CDC envía al servidor DHCP adecuado un mensaje DHCP REQUEST para aceptar el DHCP OFFER.	CHPSWMS-3 DEBE tener lugar tras completarse CHPSWMS-2.	Si el fallo ocurre en virtud del protocolo DHCP volver a CHPSWMS-1.
CHPSWMS-4	*DHCP ACK* El servidor DHCP envía al CDC un mensaje DHCP ACK que contiene la dirección IPv4 de la interfaz WAN-Man del PS y se prevé que incluirá la opción código 177 de CableHome con la subopciones 3, 6 y 51 Y no incluirá información del fichero de configuración del PS en los campos siaddr y file del mensaje DHCP. El PS modifica cabhPsDevProvMode basándose en la información recibida en el mensaje DHCP ACK (véase 7.2.3.3). El PS debe guardar la dirección del servidor de hora del día en cabhPsDevTimeServerAddr.	CHPSWMS-4 DEBE tener lugar tras completarse CHPSWMS-3.	Si el fallo ocurre en virtud del protocolo DHCP volver a CHPSWMS-1 y comunicar un error.

Cuadro 13-2/J.191 – Descripciones del flujo del proceso de configuración WAN-Man del PS en el modo de configuración SNMP

Fase	Configuración WAN-Man del PS: Modo de configuración SNMP	Secuencia ordinaria	Secuencia de fallo
CHPSWMS-5	*Petición de la hora del día (ToD) con arreglo a [RFC 868]* El PS envía una petición ToD al servidor de ToD identificado en el mensaje DHCP ACK.	CHPSWMS-5 DEBE tener lugar tras completarse CHPSWMS-4.	Continuar en CHPSWMS-6.
CHPSWMS-6	*Respuesta ToD* El servidor ToD debe contestar con la hora actual en formato UTC.	CHPSWMS-6 DEBE tener lugar tras completarse CHPSWMS-5.	Continuar en CHPSWMS-7, comunicar un error y volver a CHPSWMS-5 (continuar reintentando ToD hasta tener éxito).
CHPSWMS-7	*Petición AS (nota)* El PS envía el mensaje de petición AS al operador KDC de IPCable2Home para solicitar un tique Kerberos.	CHPSWMS-7 DEBE tener lugar tras completarse CHPSWMS-6.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.
CHPSWMS-8	*Respuesta AS* El mensaje de respuesta AS se recibe procedente del operador KDC de IPCable2Home con el tique Kerberos.	CHPSWMS-8 DEBE tener lugar tras completarse CHPSWMS-7.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.
CHPSWMS-9	*Petición TGS (opcional)* Si el PS obtiene un ticke de concesión de ticke (TGT, *ticket granting ticket*) en la fase CHPSWMS-8, debe enviar el mensaje de petición TGS al servidor KDC del operador cuya dirección fue transferida al PS (CDC) en la subopción 51 de la opción 177 del DHCP.	CHPSWMS-9 DEBE tener lugar tras completarse CHPSWMS-8.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.
CHPSWMS-10	*Respuesta TGS (opcional)* Se recibe el mensaje de respuesta TGS con el tique procedente del operador KDC.	CHPSWMS-10 DEBE tener lugar tras completarse CHPSWMS-9.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.
CHPSWMS-11	*Petición AP* El PS envía el mensaje de petición AP al NMS (gestor de SNMP) para solicitar la información de claves para SNMPv3, como se describe en 11.3.3.2.	CHPSWMS-11 DEBE tener lugar tras completarse CHPSWMS-10.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.

Cuadro 13-2/J.191 – Descripciones del flujo del proceso de configuración WAN-Man del PS en el modo de configuración SNMP

Fase	Configuración WAN-Man del PS: Modo de configuración SNMP	Secuencia ordinaria	Secuencia de fallo
CHPSWMS-12	*Respuesta AP* Se recibe el mensaje de respuesta AP procedente del NMS con la información de claves para SNMPv3. NOTA – El PS DEBE establecer las claves SNMPv3 y rellenar los cuadros SNMPv3 asociados antes de enviar un mensaje de informe SNMPv3. Las claves y los cuadros se establecen con la información de la respuesta AP (véase 11.3 para obtener mayores detalles).	CHPSWMS-12 DEBE tener lugar tras completarse CHPSWMS-11.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.
CHPSWMS-13	*SNMP Inform* Una vez que el PS que funciona en el modo de configuración SNMP establece las claves de SNMPv3, DEBE enviar un INFORME (INFORM) de SNMPv3 (cabhPsDevProvEnrollTrap) solicitando la admisión a la SNMP ENTITY cuya dirección IP fue proporcionada en la subopción 3 de la opción 177, en el mensaje DHCP ACK.	CHPSWMS-13 DEBE tener lugar tras completarse CHPSWMS-12.	Volver a CHPSWMS-1.
CHPSWMS-14	*Creación del fichero de configuración (opcional)* El sistema de configuración utiliza información de las fases anteriores de configuración del PS para crear un fichero de configuración PS. El sistema de configuración efectúa un troceo del contenido del fichero de configuración PS. Dicho troceo se envía al PS en la fase siguiente.	Si CHPSWMS-14 tiene lugar, DEBE tener lugar, en su caso, tras completarse CHPSWMS-13.	N/A

Cuadro 13-2/J.191 – Descripciones del flujo del proceso de configuración WAN-Man del PS en el modo de configuración SNMP

Fase	Configuración WAN-Man del PS: Modo de configuración SNMP	Secuencia ordinaria	Secuencia de fallo
CHPSWMS-15	*SNMP Set (opcional)* El sistema de configuración puede encargar al NMS que envíe un mensaje SNMP Set al PS con la dirección IP del servidor TFTP, el nombre del fichero de configuración del PS y el troceo del fichero de configuración descrito en 7.3.3.2 (modo de configuración SNMP). Opcionalmente, la dirección IP del servidor TFTP del fichero de configuración de la barrera contra fuegos, el nombre del fichero de configuración de la barrera contra fuegos y el troceo del fichero de configuración de la barrera contra fuegos se incluyen en el SNMP Set si ha de cargarse un fichero de configuración de la barrera contra fuegos y se selecciona este método para especificarlo.	Si CHPSWMS-15 tiene lugar, DEBE tener lugar tras completarse CHPSWMS-14.	Volver a CHPSWMS-1 si se recibió el Set pero tuvo lugar un error de proceso.
CHPSWMS-16	*Petición TFTP (opcional)* Si el NMS activa la descarga por parte del PS del fichero de configuración del PS descrito en 7.3.3.2, el PS envía al servidor TFTP una petición TFTP Get para solicitar el fichero de configuración del PS especificado.	Si CHPSWMS-16 tiene lugar, DEBE tener lugar tras completarse CHPSWMS-15.	Continuar en CHPSWMS-17.

Cuadro 13-2/J.191 – Descripciones del flujo del proceso de configuración WAN-Man del PS en el modo de configuración SNMP

Fase	Configuración WAN-Man del PS: Modo de configuración SNMP	Secuencia ordinaria	Secuencia de fallo
CHPSWMS-17	*El servidor TFTP envía el fichero de configuración (opcional)* Una vez recibido por el PS el fichero de configuración del PS, calcula el troceo de éste y lo compara con el valor recibido en la fase CHPSWMS-15. A continuación el PS procesa el fichero de configuración del PS. El contenido del fichero de configuración del PS se describe en 7.3.3. Opcionalmente, la dirección IP del servidor TFTP del fichero de configuración de la barrera contra fuegos, el nombre del fichero de configuración de la barrera contra fuegos y el troceo del fichero de configuración de la barrera contra fuegos se incluyen en el fichero de configuración del PS cuando hay que cargar un fichero de configuración de la barrera contra fuegos, y éste es el método seleccionado para especificarlo.	Si CHPSWMS-17 tiene lugar, DEBE tener lugar tras completarse CHPSWMS-16.	Si falla la descarga TFTP, comunicar el error, continuar en CHPSWMS-18, y continuar reintentando CHPSWMS-16 (continuar reintentando la descarga del fichero de configuración del PS). Si el procesamiento del fichero de configuración provocase un error, continuar y comunicar el error como evento.
CHPSWMS-18	*Petición TFTP – Fichero de configuración de la barrera contra fuegos (opcional)* El PS envía al servidor TFTP de configuración de la barrera contra fuegos una petición TFTP Get para solicitar el fichero de datos de configuración de la barrera contra fuegos especificado.	Si CHPSWMS-18 tiene lugar, DEBE tener lugar tras completarse CHPSWMS-17.	Continuar en CHPSWMS-19.
CHPSWMS-19	*El servidor TFTP envía el fichero de configuración de la barrera contra fuegos (opcional)* El servidor TFTP envía al PS una respuesta TFTP con el fichero solicitado. Una vez que el PS recibe el fichero de configuración de la barrera contra fuegos, calcula el troceo de éste y lo compara con el valor recibido en las fases CHPSWMS-15 o CHPSWMS-17. A continuación se procesa el fichero. Consúltese en 11.3 para obtener mayores detalles.	Si CHPSWMS-19 tiene lugar, DEBE tener lugar tras completarse CHPSWMS-18.	Si falla la descarga TFTP, continuar el funcionamiento del PS pero comunicar el error y continuar reintentando CHPSWMS-18. Si el procesamiento del fichero de configuración de la barrera contra fuegos provoca un error, continuar y comunicar el error como evento.

Cuadro 13-2/J.191 – Descripciones del flujo del proceso de configuración WAN-Man del PS en el modo de configuración SNMP

Fase	Configuración WAN-Man del PS: Modo de configuración SNMP	Secuencia ordinaria	Secuencia de fallo
CHPSWMS-20	*Notificación SYSLOG* Si el PS recibió una dirección de servidor SYSLOG en el mensaje DHCP ACK, DEBE enviar al servidor SYSLOG una notificación "provisioning complete". El formato general de esta notificación se define en 6.5.1.	CHPSWMS-20 DEBE tener lugar tras completarse CHPSWMS-19.	N/A
CHPSWMS-21	*Trampa SNMP* El PS DEBE enviar al NMS una SNMP TRAP (cabhPsDevInitTrap) que incluya una notificación "provisioning complete". FAIL tiene lugar si falla el procesamiento del fichero de configuración. De lo contrario el estado de la configuración es PASS. El PS DEBE actualizar el valor de cabhPsDevProvState con el estado 'pass' (1) cuando se configuran satisfactoriamente las fases de los flujos de configuración CHPSWMS-1 a CHPSWMS-13. El PS DEBE actualizar el valor de cabhPsDevProvState con el estado 'fail' (3) Y notificar un evento indicando el fallo del proceso de configuración si el temporizador de configuración del PS expira antes de que se actualice el valor de cabhPsDevProvState con el estado 'pass'.	CHPSWMS-21 DEBE tener lugar tras completarse CHPSWMS-20.	N/A
NOTA – Los pasos CHPSWMS-5 a CHIPSWMS-8 son opcionales en ciertos casos. Pueden consultarse los detalles en la cláusula 11.			

13.3.1 Descarga del fichero de configuración WAN-Man del PS

El PS funcionando en el modo de configuración SNMP PUEDE contener suficiente información por defecto desde fábrica para mantener el funcionamiento del lado LAN, del WAN o de ambos, sin necesidad de descargar el fichero de configuración del PS. Si el PS funciona en el modo de configuración SNMP, PUEDE descargarse del fichero de configuración del PS para que la configuración inicial sustituya los valores por defecto de fábrica o suministre información adicional.

El fichero de configuración de la barrera contra fuegos contiene información para proveer la función de barrera contra fuegos. La indicación de descarga del fichero de configuración de la barrera contra fuegos vendrá en el fichero de configuración del PS o en un SNMP Set durante la inicialización.

13.3.2 Temporizador de configuración del PS

Se proporciona un temporizador de configuración para que el PS continúe los ciclos del proceso de configuración cuando queda incompleta alguna operación. El objeto temporizador, cabhPsDevProvTimer, tiene un valor de inicialización por defecto de 5 minutos.

13.3.3 Informe de terminación de la admisión a configuración y de la configuración

Sólo para el PS funcionando en el modo de configuración SNMP, el informe de admisión de configuración (cabhPsDevProvEnrollTrap) permite que el servidor de configuración determine si el PS está preparado para el fichero de configuración del PS.

Tanto en el modo de configuración DHCP como en el modo de configuración SNMP, la trampa de terminación de la configuración (cabhPsDevInitTrap) indica si se ha completado o no la secuencia de configuración.

13.3.4 Configuración de SYSLOG

La dirección IP del servidor de syslog DEBE proveerse mediante el proceso DHCP. El evento SYSLOG no se enviará si no se configura la dirección IP del servidor syslog.

13.3.5 Estado de configuración y comunicación de errores

Como indican los cuadros 13-1 y 13-2, el fallo de las fases del proceso de configuración se suele traducir en la repetición del proceso desde la primera fase, CHPSWMD-1 o CHPSWMS-1.

13.4 Proceso de configuración WAN-Data del PS

El PS solicita cero o más direcciones de red WAN-Data al servidor DHCP de la red de cable para utilizarlas en el intercambio de datos entre los elementos conectados a Internet y a los dispositivos IP de LAN.

No hay diferencia entre el funcionamiento WAN-Data del PS en los modos de configuración DHCP y SNMP.

Los siguientes diagramas ilustran el flujo de mensajes que ha de utilizarse para la configuración de direcciones WAN-Data del PS. El proceso de configuración para las direcciones de la WAN-Data del PS es idéntico para el PS integrado en el módem de cable como para el PS autónomo.

Si tiene lugar el proceso de configuración de direcciones WAN-Data del PS, DEBE seguir la secuencia que muestra la figura 13-5 y describe el cuadro 13-3 detalladamente.

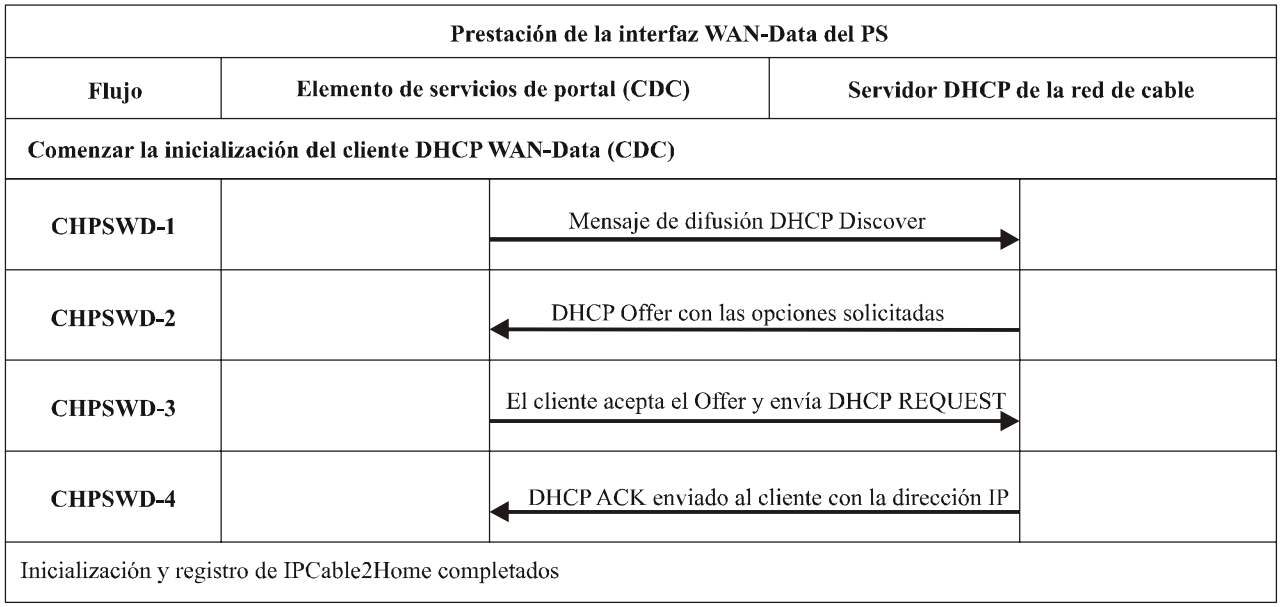


Figura 13-5/J.191 – Proceso de configuración WAN-Data del PS

Cuadro 13-3/J.191 – Descripción del flujo de la configuración WAN-Data del PS

Fase	Configuración de dirección WAN-Data del PS	Secuencia ordinaria	Secuencia de fallo
CHPSWD-1	*Mensaje de difusión DHCP Discover* El PS difunde un mensaje DHCP DISCOVER con las opciones obligatorias que figuran en el cuadro 7-7.	Continuar en CHPSWD-2.	Si falla en virtud del protocolo DHCP repetir CHPSWD-1.
CHPSWD-2	*DHCP OFFER* El servidor DHCP de cabecera recibe el paquete DHCP DISCOVER, asigna una dirección IP del grupo WAN-Data, construye un paquete DHCP OFFER y lo transmite al agente de enlace DHCP del CMTS.	Continuar en CHPSWD-3.	Si falla, el cliente agotará el tiempo en virtud del protocolo DHCP y se repetirá la fase CHPSWD-1.
CHPSWD-3	*DHCP REQUEST* El CDP envía un mensaje DHCP REQUEST al servidor DHCP seleccionado para aceptar el DHCP OFFER.	CHPSWD-3 DEBE tener lugar tras completarse CHPSWD-2.	Si hay fallo en virtud del protocolo DHCP volver a CHPSWD-1.
CHPSWD-4	*DHCP ACK* El servidor DHCP envía al CDP un mensaje DHCP ACK con la dirección IPv4 de la interfaz WAN-Data del PS.	CHPSWD-4 DEBE tener lugar tras completarse CHPSWD-3. La configuración termina al completarse CHPSWD-4.	Si falla en virtud del protocolo DHCP volver a CHPSWD-1.

13.5 Proceso de configuración: Cliente DHCP en el sector LAN-Trans

Los dispositivos IP de LAN solicitan direcciones IP mediante procesos DHCP. El elemento PS maneja estos mensajes de acuerdo con los parámetros de configuración asignados por el NMS de la red de cable (véase 7.2.3.2).

Esta cláusula describe el proceso de configuración correspondiente al caso en que el NMS haya provisto al PS del funcionamiento en el modo de tratamiento de paquetes primario C-NAT o C-NAPT (véase la cláusula 8). No hay diferencia entre el proceso de configuración de los dispositivos IP del sector LAN-Trans en los modos de configuración DHCP y SNMP.

El flujo de mensajes del proceso de configuración para un dispositivo IP de LAN del sector LAN-Trans se describe en la figura 13-6. El cuadro 13-4 proporciona detalles adicionales de dicho proceso.

El proceso de configuración correspondiente a los dispositivos IP de LAN del sector LAN-Trans DEBE tener lugar de acuerdo con la secuencia representada en la figura 13-6 y descrita en más detalle en el cuadro 13-4.

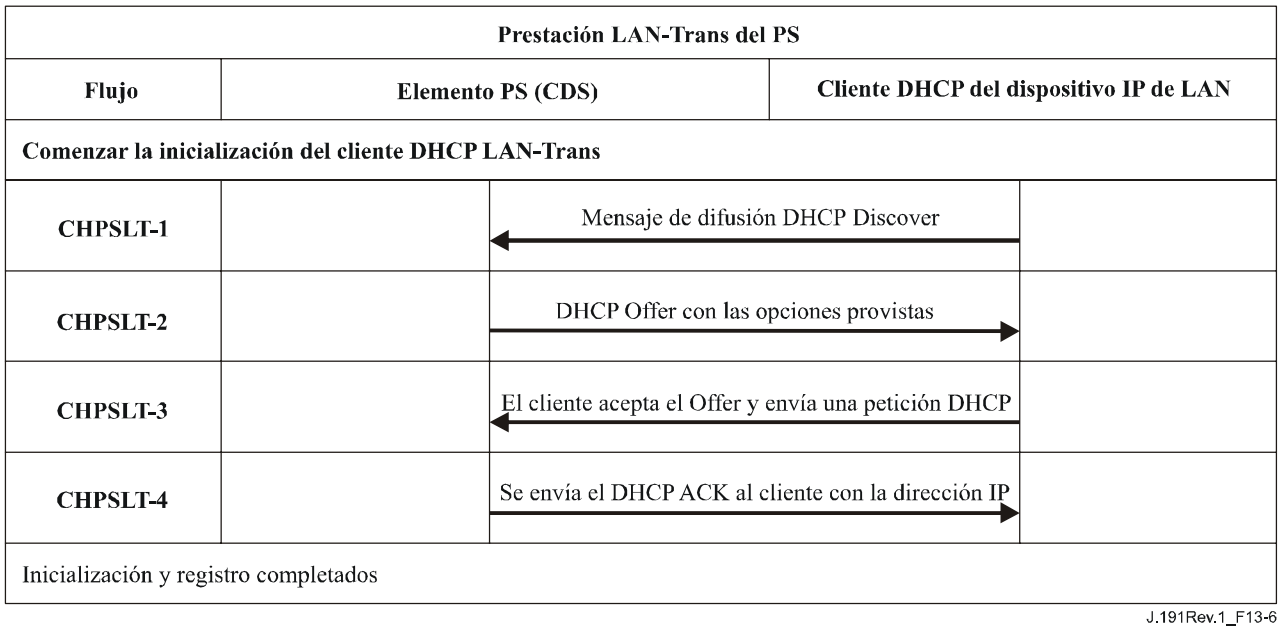


Figura 13-6/J.191 – Proceso de configuración de un dispositivo IP de LAN en el sector LAN-Trans

Cuadro 13-4/J.191 – Descripción del flujo del proceso de configuración LAN-Trans del PS

Fase	Configuración de dirección LAN-Trans del cliente	Secuencia ordinaria	Secuencia de fallo
CHPSLT-1	*Mensaje de difusión DHCP Discover* El Cliente (nota 1) envía un mensaje de difusión DHCP DISCOVER por su LAN (nota 2) local.	Continuar en CHPSLT-2.	Si falla el protocolo DHCP repetir CHPSLT-1.
CHPSLT-2	*DHCP OFFER* El PS recibe el mensaje DHCP DISCOVER en su interfaz LAN y examina el campo chaddr. Si: – hay una dirección disponible LAN-Trans, y – no hay impedimentos administrativos para denegar la dirección LAN-Trans al cliente, entonces el PS DEBE enviar un mensaje DHCP OFFER al cliente para ofrecerle su dirección LAN-Trans ya sea para unidifusión o para multidifusión específica del enlace (dependiendo del bit BROADCAST del campo de banderas del DHCP DISCOVER).	Continuar en CHPSLT-3.	Si falla, el cliente cancelará el temporizador del protocolo DHCP y se repetirá CHPSLT-1.
CHPSLT-3	*DHCP REQUEST* El cliente DHCP del dispositivo IP de LAN recibe el mensaje DHCP OFFER. Cuando un cliente DHCP de un dispositivo IP de LAN desea aceptar un DHCP OFFER, debe formatear y enviar un paquete DHCP REQUEST utilizando una difusión (nota 3) específica del enlace.	Continuar en CHPSLT-4.	Si falla, el cliente cancelará el temporizador del protocolo DHCP y se repetirá CHPSLT-1.
CHPSLT-4	*DHCP ACK* El PS recibe el DHCP REQUEST en su interfaz LAN. Si la dirección LAN-Trans indicada sigue siendo asignable, el PS DEBE enviar un DHCP ACK al cliente ya sea como de unidifusión o de multidifusión específica del enlace (dependiendo del bit BROADCAST del campo de banderas del DHCP REQUEST).	Configuración completada.	Si falla, el cliente cancelará el temporizador del protocolo DHCP y se repetirá CHPSLT-1.
NOTA 1 – Si el cliente conociera la dirección IP anterior (por ejemplo, tras un rearranque), podría omitir el DHCP DISCOVER y continuar en la fase 3. NOTA 2 – Si el cliente se encuentra en una red que no es de difusión se espera que envíe el mensaje al servidor DHCP en unidifusión. NOTA 3 – Si el cliente se encuentra en una red que no es de multidifusión se espera que envíe el mensaje al PS en unidifusión.			

13.5.1 Selección de la dirección LAN-Trans y opciones DHCP

El PS DEBE seleccionar la dirección LAN-Trans que ofrece a partir del intervalo indicado por las variables de la MIB cabhCdpLanPoolStart y cabhCdpLanPoolEnd.

El CDS del PS DEBE incluir en el DHCP OFFER las opciones obligatorias del cuadro 7-3.

13.6 Proceso de configuración: Cliente DHCP en el sector LAN-Pass

Algunas aplicaciones LAN domésticas no funcionan correctamente con una dirección de red traducida. Para poder manejar estas aplicaciones, el PS tiene la posibilidad de funcionar en modo

transferencia (puenteo transparente). Como se describe en 8.2.2.2, el puenteo tiene lugar cuando el NMS de la red de cable establece el modo de tratamiento de paquetes primario (cabhCapPrimaryMode) en transferencia, o escribiendo direcciones MAC de dispositivo IP de LAN individuales en el cuadro transferencia (cabhCapPassthroughTable). La figura 13-7 describe el proceso de la petición y asignación de una dirección de red a dispositivos IP de LAN para lo cual el PS se ha provisto previamente para que puentee el tráfico. Cuando se ha configurado el PS para que puentee el tráfico de un dispositivo IP de LAN, los DHCP DISCOVER y DHCP REQUEST emitidos por dicho dispositivo IP de LAN, serán atendidos por el servidor DHCP de la red de cable y no por el CDS.

El proceso de configuración para el dispositivo IP de LAN del sector LAN-Pass DEBE realizarse de acuerdo con la secuencia descrita en la figura 13-7 y expuesta en detalle en el cuadro 13-5.

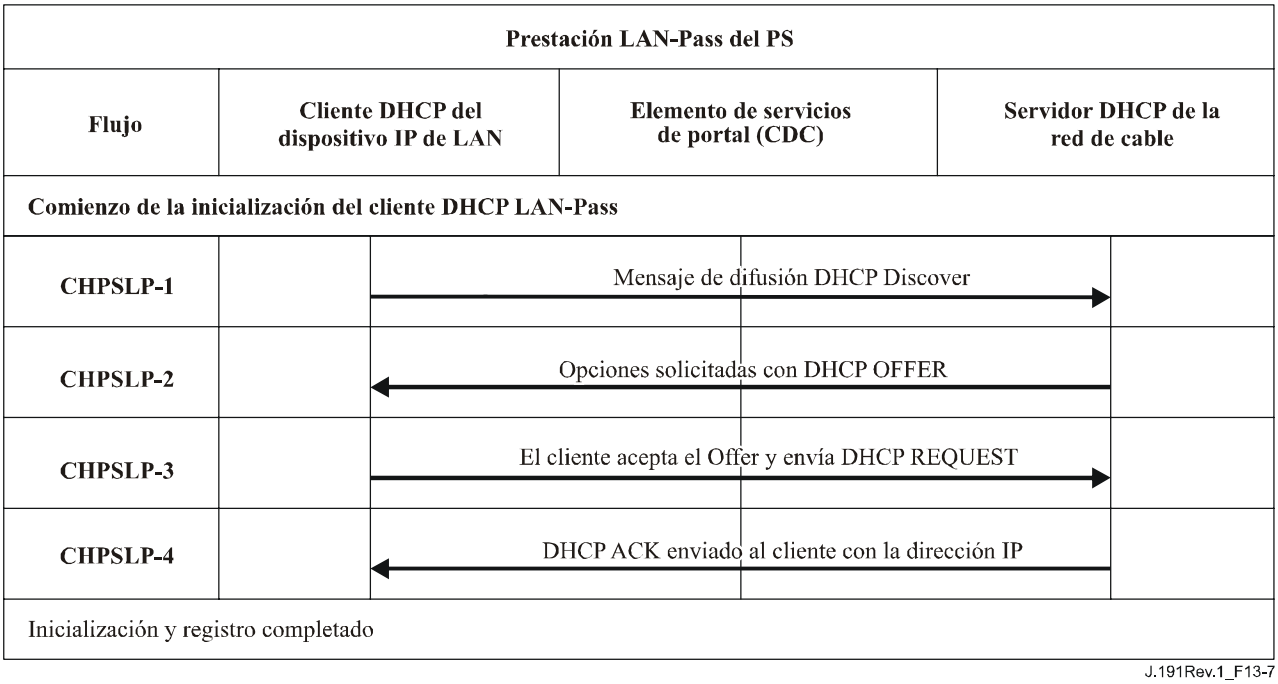


Figura 13-7/J.191 – Proceso de configuración para dispositivo IP de LAN en el sector LAN-Pass

Cuadro 13-5/J.191 – Descripción del flujo del proceso de configuración LAN-Pass

Fase	Configuración de dirección transferencia del cliente	Secuencia ordinaria	Secuencia de fallo
CHPSLP-1	*Mensaje de difusión del DHCP Discover* El dispositivo IP de LAN difunde un mensaje DHCP DISCOVER en su LAN (nota) local. El PS recibe la difusión del paquete DHCP DISCOVER en su interfaz LAN y DEBE puentear transparentemente el paquete a la interfaz WAN sin modificar su contenido.	Continuar en CHPSLP-2.	Si falla el protocolo DHCP repetir CHPSLP-1.
CHPSLP-2	*DHCP OFFER* El servidor DHCP de la cabecera recibe el paquete DHCP DISCOVER y asigna una dirección IP direccionable externamente y otras opciones, construye un paquete DHCP OFFER y transmite el DHCP OFFER al dispositivo IP de LAN. El PS DEBE puentear transparentemente el DHCP OFFER de su interfaz WAN a su interfaz LAN sin modificar el contenido el paquete IP.	Continuar en CHPSLP-3.	Si falla, el dispositivo IP de LAN cancelará el temporizador del protocolo DHCP y repetirá CHPSLP-1.
CHPSLP-3	*DHCP REQUEST* El dispositivo IP de LAN recibe el DHCP OFFER y emite un mensaje DHCP REQUEST. El PS DEBE puentear transparentemente el DHCP REQUEST de su interfaz LAN a su interfaz WAN sin modificar el contenido el paquete IP.	Continuar en CHPSLP-4.	Si falla el protocolo DHCP repetir CHPSLP-1.
CHPSLP-4	*DHCP ACK* El servidor DHCP de cabecera recibe el DHCP REQUEST y envía el DHCP ACK al dispositivo IP de LAN con la dirección IPv4 del dispositivo IP de LAN. El PS DEBE puentear transparentemente el DHCP ACK de su interfaz WAN a su interfaz LAN sin modificar el contenido el paquete IP.	Configuración completada.	Si falla, el dispositivo IP de LAN cancelará el temporizador del protocolo DHCP y se repetirá CHPSLP-1.
NOTA – Si el cliente se encuentra en una red que no es de difusión, debe enviar por unidifusión el mensaje al servidor DHCP o al agente de enlace DHCP de la red del cable.			

Anexo A

Objetos MIB

Este anexo contiene la relación de todos los objetos de la MIB necesarios, indicados en 6.3.7.

Nombre/parámetro de la MIB	Acceso máximo	Se conserva	# de anotaciones que se conservan
mib-2			
system			
sysDescr	sólo lectura	N/A	N/A
sysObjectID	sólo lectura	N/A	N/A
sysUpTime	sólo lectura	N/A	N/A
sysContact	lectura-escritura	Sí	1
sysName	lectura-escritura	Sí	1
sysLocation	lectura-escritura	Sí	1
sysServices	sólo lectura	N/A	N/A
interfaces [RFC 2863]			
ifNumber	sólo lectura	N/A	N/A
ifTable/ifEntry			
ifIndex	sólo lectura	N/A	N/A
ifDescr	sólo lectura	N/A	N/A
ifType	sólo lectura	N/A	N/A
ifMtu	sólo lectura	N/A	N/A
ifSpeed	sólo lectura	N/A	N/A
ifPhysAddress	sólo lectura	N/A	N/A
ifAdminStatus	lectura-escritura	N/A	N/A
ifOperStatus	sólo lectura	N/A	N/A
ifLastChange	sólo lectura	N/A	N/A
ifInOctets	sólo lectura	N/A	N/A
ifInUcastPkts	sólo lectura	N/A	N/A
ifInDiscards	sólo lectura	N/A	N/A
ifInErrors	sólo lectura	N/A	N/A
ifInUnknownProtos	sólo lectura	N/A	N/A
ifOutOctets	sólo lectura	N/A	N/A
ifOutUcastPkts	sólo lectura	N/A	N/A
ifOutDiscards	sólo lectura	N/A	N/A
ifOutErrors	sólo lectura	N/A	N/A

ip [RFC 2011]			
ipForwarding	lectura-escritura	No	N/A
ipDefaultTTL	lectura-escritura	No	N/A
ipInReceives	sólo lectura	N/A	N/A
ipInHdrErrors	sólo lectura	N/A	N/A
ipInAddrErrors	sólo lectura	N/A	N/A
ipForwDatagrams	sólo lectura	N/A	N/A
ipInUnknownProtos	sólo lectura	N/A	N/A
ipInDiscards	sólo lectura	N/A	N/A
ipInDelivers	sólo lectura	N/A	N/A
ipOutRequests	sólo lectura	N/A	N/A
ipOutDiscards	sólo lectura	N/A	N/A
ipOutNoRoutes	sólo lectura	N/A	N/A
ipReasmTimeout	sólo lectura	N/A	N/A
ipReasmReqds	sólo lectura	N/A	N/A
ipReasmOKs	sólo lectura	N/A	N/A
ipReasmFails	sólo lectura	N/A	N/A
ipFragOKs	sólo lectura	N/A	N/A
ipFragFails	sólo lectura	N/A	N/A
ipFragCreates	sólo lectura	N/A	N/A
ipNetToMediaTable/ipNetToMediaEntry			
ipNetToMediaIfIndex	lectura-creación	No	N/A
ipNetToMediaPhyAddress	lectura-creación	No	N/A
ipNetToMediaNetAddress	lectura-creación	No	N/A
ipNetToMediaType	lectura-creación	No	N/A
icmp			
icmpInMsgs	sólo lectura	N/A	N/A
icmpInErrors	sólo lectura	N/A	N/A
icmpInDestUnreachs	sólo lectura	N/A	N/A
icmpInTimeExcds	sólo lectura	N/A	N/A
icmpInParmProbs	sólo lectura	N/A	N/A
icmpInSrcQuenchs	sólo lectura	N/A	N/A
icmpInRedirects	sólo lectura	N/A	N/A
icmpInEchos	sólo lectura	N/A	N/A
icmpInEchosReps	sólo lectura	N/A	N/A
icmpInTimestamps	sólo lectura	N/A	N/A
icmpInTimestampsReps	sólo lectura	N/A	N/A
icmpInAddrMasks	sólo lectura	N/A	N/A

icmpInAddrMaskReps	sólo lectura	N/A	N/A
icmpOutMsgs	sólo lectura	N/A	N/A
icmpOutErrors	sólo lectura	N/A	N/A
icmpOutDestUnreachs	sólo lectura	N/A	N/A
icmpOutTimeExcds	sólo lectura	N/A	N/A
icmpOutParmProbs	sólo lectura	N/A	N/A
icmpOutSrcQuenchs	sólo lectura	N/A	N/A
icmpOutRedirects	sólo lectura	N/A	N/A
icmpOutEchos	sólo lectura	N/A	N/A
icmpOutEchosReps	sólo lectura	N/A	N/A
icmpOutTimestamps	sólo lectura	N/A	N/A
icmpOutTimestampReps	sólo lectura	N/A	N/A
icmpOutAddrMasks	sólo lectura	N/A	N/A
icmpOutAddrMaskReps	sólo lectura	N/A	N/A
udp [RFC 2013]			
udpInDatagrams	sólo lectura	N/A	N/A
udpNoPorts	sólo lectura	N/A	N/A
udpInErrors	sólo lectura	N/A	N/A
udpOutDatagrams	sólo lectura	N/A	N/A
udpTable/udpEntry			
udpLocalAddress	sólo lectura	N/A	N/A
udpLocalPort	sólo lectura	N/A	N/A
transmission [draft-ietf-ipcdn-bpiplus-mib-12]			
docsIfMib			
docsBpi2MIB			
docsBpi2MIBObjects			
docsBpi2CmObjects			
docsBpi2CmCertObjects			
docsBpi2CmDeviceCertTable/docsBpi2CmDeviceCertEntry			
docsBpi2CmDeviceCmCert	lectura-escritura	Sí	5
docsBpi2CmDeviceManufCert	sólo lectura	N/A	N/A
docsBpi2CodeDownloadGroup			
docsBpi2CodeDownloadStatusCode	sólo lectura	N/A	N/A
docsBpi2CodeDownloadStatusString	sólo lectura	N/A	N/A
docsBpi2CodeMfgOrgName	sólo lectura	N/A	N/A
docsBpi2CodeMfgCodeAccessStart	sólo lectura	N/A	N/A
docsBpi2CodeMfgCvcAccessStart	sólo lectura	N/A	N/A
docsBpi2CodeCoSignerOrgName	sólo lectura	N/A	N/A
docsBpi2CodeCoSignerCodeAccessStart	sólo lectura	N/A	N/A
docsBpi2CodeCoSignerCvcAccessStart	sólo lectura	N/A	N/A

docsBpi2CodeCvcUpdate	lectura-escritura	Sí	1
snmp [RFC 3416]			
snmpInPkts	sólo lectura	N/A	N/A
snmpInBadVersions	sólo lectura	N/A	N/A
snmpInBadCommunityNames	sólo lectura	N/A	N/A
snmpInBadCommunityUses	sólo lectura	N/A	N/A
snmpInASNParseErrs	sólo lectura	N/A	N/A
snmpEnableAuthenTraps	lectura-escritura	No	N/A
snmpSilentDrops	sólo lectura	N/A	N/A
ifMIB [RFC 2863]			
ifMIBOjects			
ifXTable/ifXEntry			
ifName	sólo lectura	N/A	N/A
ifInMulticastPkts	sólo lectura	N/A	N/A
ifInBroadcastPkts	sólo lectura	N/A	N/A
ifOutMulticastPkts	sólo lectura	N/A	N/A
ifOutBroadcastPkts	sólo lectura	N/A	N/A
ifLinkUpDownTrapEnable	lectura-escritura	No	N/A
ifHighSpeed	sólo lectura	N/A	N/A
ifPromiscuousMode	lectura-escritura	N/A	N/A
ifConnectorPresent	sólo lectura	N/A	N/A
ifAlias	lectura-escritura	No	N/A
ifCounterDiscontinuityTime	sólo lectura	N/A	N/A
ifStackTable/ifStackEntry			
ifStackHigherLayer		N/A	N/A
IfStackLowerLayer	sólo lectura	N/A	N/A
ifStackStatus	sólo lectura	N/A	N/A
ifName	sólo lectura	N/A	N/A
docsDev [RFC 2669]			
docsDevMIBObjects			
docsDevNmAccessTable/docsDevNmAccessEntry			
docsDevNmAccessIndex	inaccesible	N/A	N/A
docsDevNmAccessIp	lectura-creación	No	N/A
docsDevNmAccessIpMask	lectura-creación	No	N/A
docsDevNmAccessCommunity	lectura-creación	No	N/A

docsDevNmAccessControl	lectura-creación	No	N/A
docsDevNmAccessInterfaces	lectura-creación	No	N/A
docsDevNmAccessStatus	lectura-creación	No	N/A
docsDevNmAccessTrapVersion	lectura-creación	No	N/A
docsDevSoftware			
docsDevSwServer	lectura-escritura	Sí	1
docsDevSwFilename	lectura-escritura	Sí	1
docsDevSwAdminStatus	lectura-escritura	No	1
docsDevSwOperStatus	sólo lectura	N/A	N/A
docsDevSwCurrentVers	sólo lectura	N/A	N/A
docsDevEvent			
docsDevEvControl	lectura-escritura	No	N/A
docsDevEvSyslog	lectura-escritura	No	N/A
docsDevEvThrottleAdminStatus	lectura-escritura	No	N/A
docsDevEvThrottleInhibited	sólo lectura	N/A	N/A
docsDevEvThrottleThreshold	lectura-escritura	No	N/A
docsDevEvThrottleInterval	lectura-escritura	No	N/A
docsDevEvControlTable/docsDevEvControlEntry			
docsDevEvPriority	inaccesible	N/A	N/A
docsDevEvReporting	lectura-escritura	No	N/A
docsDevEventTable/docsDevEventEntry			
docsDevEvIndex	inaccesible	N/A	N/A
docsDevEvFirstTime	sólo lectura	Sí	1
docsDevEvLastTime	sólo lectura	Sí	1
docsDevEvCounts	sólo lectura	Sí	1
docsDevEvLevel	sólo lectura	Sí	1
docsDevEvId	sólo lectura	Sí	1
docsDevEvText	sólo lectura	Sí	1

private			
enterprises			
cableLabs			
clabProject			
clabProjCableHome			
cabhPsDevMib			
cabhPsDevBase			
cabhPsDevDateTime	lectura-escritura	No	N/A
cabhPsDevResetNow	lectura-escritura	No	N/A
cabhPsDevSerialNumber	sólo lectura	N/A	N/A
cabhPsDevHardwareVersion	sólo lectura	N/A	N/A
cabhPsDevWanManMacAddress	sólo lectura	N/A	N/A
cabhPsDevWanDataMacAddress	sólo lectura	N/A	N/A
cabhPsDevTypeIdentifier	sólo lectura	N/A	N/A
cabhPsDevSetToFactory	lectura-escritura	No	N/A
cabhPsDevTodSyncStatus	sólo lectura	N/A	N/A
cabhPsDevProvMode	sólo lectura	N/A	N/A
cabhPsDevLastSetToFactory	sólo lectura	–	N/A
cabhPsDevProv			
cabhPsDevProvisioningTimer	lectura-escritura	No	N/A
cabhPsDevProvConfigFile	lectura-escritura	No	N/A
cabhPsDevProvConfigHash	lectura-escritura	No	N/A
cabhPsDevProvConfigFileSize	sólo lectura	N/A	N/A
cabhPsDevProvConfigFileStatus	sólo lectura	N/A	N/A
cabhPsDevProvConfigTLVProcessed	sólo lectura	N/A	N/A
cabhPsDevProvConfigTLVRejected	sólo lectura	N/A	N/A
cabhPsDevProvSolicitedKeyTimeout	lectura-escritura	Sí	1
cabhPsDevProvState	sólo lectura	N/A	N/A
cabhPsDevProvAuthState	sólo lectura	N/A	N/A
cabhPsDevTimeServerAddrType	sólo lectura	N/A	N/A
cabhPsDevTimeServerAddr	sólo lectura	N/A	N/A
cabhSecMib			
cabhSecFwObjects			
cabhSecFwBase			
cabhSecFwPolicyFileEnable	lectura-escritura	No	N/A
cabhSecFwPolicyFileURL	lectura-escritura	no	N/A

cabhSecFwPolicyFileHash	lectura-escritura	No	N/A
cabhSecFwPolicyFileOperStatus	sólo lectura	N/A	N/A
cabhSecFwPolicyFileCurrentVersion	sólo lectura	N/A	N/A
cabhSecFwPolicySuccessfulFileURL, Max-Access	sólo lectura	Sí	1
cabhSecFwLogCtl			
cabhSecFwEventType1Enable	lectura-escritura	No	N/A
cabhSecFwEventType2Enable	lectura-escritura	No	N/A
cabhSecFwEventType3Enable	lectura-escritura	No	N/A
cabhSecFwEventAttackAlertThreshold	lectura-escritura	No	N/A
cabhSecFwEventAttackAlertPeriod	lectura-escritura	No	N/A
cabhSecCertObjects			
cabhSecCertPsCert	sólo lectura	Sí	1
cabhCapMib			
cabhCapObjects			
cabhCapBase			
cabhCapTcpTimeWait	lectura-escritura	Sí	1
cabhCapUdpTimeWait	lectura-escritura	Sí	1
cabhCapIcmpTimeWait	lectura-escritura	Sí	1
cabhCapPrimaryMode	lectura-escritura	No	N/A
cabhCapSetToFactory	lectura-escritura	No	N/A
cabhCapLastSetToFactory	sólo lectura	–	N/A
cabhCapMap			
cabhCapMappingTable/cabhCapMappingEntry			
cabhCapMappingIndex	inaccesible	Sí (nota)	16
cabhCapMappingWanAddrType	lectura-creación	Sí (nota)	16
cabhCapMappingWanAddr	lectura-creación	Sí (nota)	16
cabhCapMappingWanPort	lectura-creación	Sí (nota)	16
cabhCapMappingLanAddrType	lectura-creación	Sí (nota)	16
cabhCapMappingLanAddr	lectura-creación	Sí (nota)	16

cabhCapMappingLanPort	lectura-creación	Sí (nota)	16
cabhCapMappingMethod	sólo lectura	N/A	16
cabhCapMappingProtocol	lectura-creación	Sí (nota)	16
cabhCapMappingRowStatus	lectura-creación	Sí	16
cabhCapPass-throughTable/cabhCapPass-throughEntry			
cabhCapPass-throughIndex	inaccesible	Sí	16
cabhCapPass-throughMACAddr	lectura-creación	Sí	16
cabhCapPass-throughRowStatus	lectura-creación	Sí	16

NOTA – Los objetos cabhCapMappingEntry se conservan si son suministrados por el NMS y no se conservan si se crearon dinámicamente basándose en el tráfico saliente. Véase 8.3.2.2.

cabhCdpMib

cabhCdpObjects

cabhCdpBase

cabhCdpSetToFactory	lectura-escritura	No	N/A
cabhCdpLanTransCurCount	sólo lectura	N/A	N/A
cabhCdpLanTransThreshold	lectura-escritura	No	N/A
cabhCdpLanTransAction	lectura-escritura	No	N/A
cabhCdpWanDataIpAddrCount	lectura-escritura	No	N/A
cabhCdpLastSetToFactory	sólo lectura	–	N/A

cabhCdpAddr

cabhCdpLanAddrTable/cabhCdpLanAddrEntry			
cabhCdpLanAddrIpType	inaccesible	Sí	16
cabhCdpLanAddrIp	inaccesible	Sí	16
cabhCdpLanAddrClientID	lectura-creación	Sí	16
cabhCdpLanAddrLeaseCreateTime	sólo lectura	Sí	16
cabhCdpLanAddrLeaseExpireTime	sólo lectura	Sí	16
cabhCdpLanAddrMethod	sólo lectura	Sí	16
cabhCdpLanAddrHostName	sólo lectura	Sí	16
cabhCdpLanAddrRowStatus	lectura-creación	Sí	16
cabhCdpWanDataAddrTable/cabhCdpWanDataAddrEntry			
cabhCdpWanDataAddrIndex	inaccesible	N/A	N/A
cabhCdpWanDataAddrClientId	lectura-creación	No	N/A
cabhCdpWanDataAddrIpType	sólo lectura	N/A	N/A
cabhCdpWanDataAddrIp	sólo lectura	N/A	N/A

cabhCdpWanDataAddrRenewalTime	sólo lectura	N/A	N/A
cabhCdpWanDataAddrRowStatus	lectura-creación	No	N/A
cabhCdpWanDataAddrServerTable/cabhCdpWanDataAddrServerEntry			
cabhCdpWanDataAddrDnsIpType	inaccesible	N/A	N/A
cabhCdpWanDataAddrDnsIp	inaccesible	N/A	N/A
cabhCdpWanDataAddrDnsRowStatus	lectura-creación	No	N/A
cabhCdpServer			
cabhCdpLanPoolStartType	lectura-escritura	Sí	1
cabhCdpLanPoolStart	lectura-escritura	Sí	1
cabhCdpLanPoolEndType	lectura-escritura	Sí	1
cabhCdpLanPoolEnd	lectura-escritura	Sí	1
cabhCdpServerNetworkNumberType	lectura-escritura	Sí	1
cabhCdpServerNetworkNumber	lectura-escritura	Sí	1
cabhCdpServerSubnetMaskType	lectura-escritura	Sí	1
cabhCdpServerSubnetMask	lectura-escritura	Sí	1
cabhCdpServerTimeOffset	lectura-escritura	Sí	1
cabhCdpServerRouterType	lectura-escritura	Sí	1
cabhCdpServerRouter	lectura-escritura	Sí	1
cabhCdpServerDnsAddressType	lectura-escritura	Sí	1
cabhCdpServerDnsAddress	lectura-escritura	Sí	1
cabhCdpServerSyslogAddressType	lectura-escritura	Sí	1
cabhCdpServerSyslogAddress	lectura-escritura	Sí	1
cabhCdpServerDomainName	lectura-escritura	Sí	1
cabhCdpServerTTL	lectura-escritura	Sí	1
cabhCdpServerInterfaceMTU	lectura-escritura	Sí	1
cabhCdpServerVendorSpecific	lectura-escritura	Sí	1
cabhCdpServerLeaseTime	lectura-escritura	Sí	1

cabhCdpServerDhcpAddressType	lectura-escritura	Sí	1
cabhCdpServerDhcpAddress	lectura-escritura	Sí	1
cabhCdpServerControl	lectura-escritura	No	N/A
cabhCdpServerCommitStatus	sólo lectura	–	N/A
cabhCtpMib			
cabhCtpObjects			
cabhCtpBase			
cabhCtpSetToFactory	lectura-escritura	No	N/A
cabhCtpLastSetToFactory	sólo lectura	–	N/A
cabhCtpConnSpeed			
cabhCtpConnSrcIpType	lectura-escritura	No	N/A
cabhCtpConnSrcIp	lectura-escritura	No	N/A
cabhCtpConnDestIpType	lectura-escritura	No	N/A
cabhCtpConnDestIp	lectura-escritura	No	N/A
cabhCtpConnProto	lectura-escritura	No	N/A
cabhCtpConnNumPkts	lectura-escritura	No	N/A
cabhCtpConnPktSize	lectura-escritura	No	N/A
cabhCtpConnTimeOut	lectura-escritura	No	N/A
cabhCtpConnControl	lectura-escritura	No	N/A
cabhCtpConnStatus	sólo lectura	N/A	N/A
cabhCtpConnPktsSent	sólo lectura	N/A	N/A
cabhCtpConnPktsRecv	sólo lectura	N/A	N/A
cabhCtpConnRTT	sólo lectura	N/A	N/A
cabhCtpConnThroughput	sólo lectura	N/A	N/A
cabhCtpPing			
cabhCtpPingSrcIpType	lectura-escritura	No	N/A
cabhCtpPingSrcIp	lectura-escritura	No	N/A
cabhCtpPingDestIpType	lectura-escritura	No	N/A
cabhCtpPingDestIp	lectura-escritura	No	N/A
cabhCtpPingNumPkts	lectura-escritura	No	N/A

cabhCtpPingPktSize	lectura-escritura	No	N/A
cabhCtpPingTimeBetween	lectura-escritura	No	N/A
cabhCtpPingTimeOut	lectura-escritura	No	N/A
cabhCtpPingControl	lectura-escritura	No	N/A
cabhCtpPingStatus	sólo lectura	N/A	N/A
cabhCtpPingNumSent	sólo lectura	N/A	N/A
cabhCtpPingNumRecv	sólo lectura	N/A	N/A
cabhCtpPingAvgRTT	sólo lectura	N/A	N/A
cabhCtpPingMinRTT	sólo lectura	N/A	N/A
cabhCtpPingMaxRTT	sólo lectura	N/A	N/A
cabhCtpPingNumIcmpError	sólo lectura	N/A	N/A
cabhCtpPingIcmpError	sólo lectura	N/A	N/A
experimental			
snmpUSMDHObjectsMIB [RFC 2786]			
usmDHKeyObjects			
usmDHPublicObjects			
usmDHPParamaters	lectura-escritura	No	N/A
usmDHUserKeyTable/usmDHUserKeyEntry			
usmDHUserAuthKeyChange	lectura-creación	No	N/A
usmDHUserOwnAuthKeyChange	lectura-creación	No	N/A
usmDHUserPrivKeyChange	lectura-creación	No	N/A
usmDHUserOwnPrivKeyChange	lectura-creación	No	N/A
usmDHKickstartGroup			
usmDHKickstartTable/usmDHKickstartEntry			
usmDHKickstartIndex	inaccesible	No	N/A
usmDHKickstartMyPublic	sólo lectura	N/A	N/A
usmDHKickstartMgrPublic	sólo lectura	N/A	N/A
usmDHKickstartSecurityName	sólo lectura	N/A	N/A
snmpV2			
snmpModules			
snmpMIB			
snmpMIBObjects			
snmpSet			
snmpSetSerialNo	lectura-escritura	No	N/A

snmpFrameworkMIB [RFC 2576]			
snmpEngine			
snmpEngineID	sólo lectura	N/A	N/A
snmpEngineBoots	sólo lectura	Sí	1
snmpEngineTime	sólo lectura	N/A	N/A
snmpEngineMaxMessageSize	sólo lectura	N/A	N/A
snmpMPDMIB [RFC 3412]			
snmpMPDObjects			
snmpMPDStats			
snmpUnknownSecurityModels	sólo lectura	N/A	N/A
snmpInvalidMsgs	sólo lectura	N/A	N/A
snmpUnknownPDUHandlers	sólo lectura	N/A	N/A
snmpTargetMIB [RFC 3413]			
snmpTargetObjects			
snmpTargetSpinLock	lectura-escritura	No	N/A
snmpTargetAddrTable/snmpTargetAddrEntry			
snmpTargetAddrName	inaccesible	No	N/A
snmpTargetAddrTDomain	lectura-creación	No	N/A
snmpTargetAddrTAddress	lectura-creación	No	N/A
snmpTargetAddrTimeout	lectura-creación	No	N/A
snmpTargetAddrRetryCount	lectura-creación	No	N/A
snmpTargetAddrTagList	lectura-creación	No	N/A
snmpTargetAddrParams	lectura-creación	No	N/A
snmpTargetAddrStorageType	lectura-creación	No	N/A
snmpTargetAddrRowStatus	lectura-creación	No	N/A
snmpTargetParamsTable/snmpTargetParamsEntry			
snmpTargetParamsName	inaccesible	No	N/A
snmpTargetParamsMPModel	lectura-creación	No	N/A
snmpTargetParamsSecurityModel	lectura-creación	No	N/A
snmpTargetParamsSecurityName	lectura-creación	No	N/A
snmpTargetParamsSecurityLevel	lectura-creación	No	N/A
snmpTargetParamsStorageType	lectura-creación	No	N/A

snmpTargetParamsRowStatus	lectura-creación	No	N/A
snmpUnavailableContexts	sólo lectura	N/A	N/A
snmpUnknownContexts	sólo lectura	N/A	N/A
snmpNotificationMIB [RFC 3413]			
snmpNotifyObjects			
snmpNotifyTable/snmpNotifyEntry			
snmpNotifyName	inaccesible	No	N/A
snmpNotifyTag	lectura-creación	No	N/A
snmpNotifyType	lectura-creación	No	N/A
snmpNotifyStorageType	lectura-creación	No	N/A
snmpNotifyRowStatus	lectura-creación	No	N/A
snmpNotifyFilterProfileTable/snmpNotifyFilterProfileEntry			
snmpNotifyFilterProfileName	lectura-creación	No	N/A
snmpNotifyFilterProfileStorType	lectura-creación	No	N/A
snmpNotifyFilterProfileRowStatus	lectura-creación	No	N/A
snmpNotifyFilterTable/snmpNotifyFilterEntry			
snmpNotifyFilterSubtree	inaccesible	No	N/A
snmpNotifyFilterMask	lectura-creación	No	N/A
snmpNotifyFilterType	lectura-creación	No	N/A
snmpNotifyFilterStorageType	lectura-creación	No	N/A
snmpNotifyFilterRowStatus	lectura-creación	No	N/A
snmpUsmMIB [RFC 3414]			
usmStats			
usmStatsUnsupportedSecLevels	sólo lectura	N/A	N/A
usmStatsNotInTimeWindows	sólo lectura	N/A	N/A
usmStatsUnknownUserNames	sólo lectura	N/A	N/A
usmStatsUnknownEngineIDs	sólo lectura	N/A	N/A
usmStatsWrongDigests	sólo lectura	N/A	N/A
usmStatsDecryptionErrors	sólo lectura	N/A	N/A
usmUser			
usmUserSpinLock	lectura-escritura	No	N/A
usmUserTable/usmUserEntry			
usmUserEngineID	inaccesible	N/A	N/A

usmUserName	inaccesible	N/A	N/A
usmUserSecurityName	sólo lectura	N/A	N/A
usmUserCloneFrom	lectura-creación	No	N/A
usmUserAuthProtocol	lectura-creación	No	N/A
usmUserAuthKeyChange	lectura-creación	No	N/A
usmUserOwnAuthKeyChange	lectura-creación	No	N/A
usmUserPrivProtocol	lectura-creación	No	N/A
usmUserPrivKeyChange	lectura-creación	No	N/A
usmUserOwnPrivKeyChange	lectura-creación	No	N/A
usmUserPublic	lectura-creación	No	N/A
usmUserStorageType	lectura-creación	No	N/A
usmUserStatus	lectura-creación	No	N/A

SNMP-VIEW-BASED-ACM-MIB [RFC 3415]

snmpVacmMIB

vacmMIBObjects

vacmContextTable/vacmContextEntry			
vacmContextName	sólo lectura	No	N/A
vacmSecurityToGroupTable/vacmSecurityToGroupEntry			
vacmSecurityModel	inaccesible	No	N/A
vacmSecurityName	inaccesible	No	N/A
vacmGroupName	lectura-creación	No	N/A
vacmSecurityToGroupStorageType	lectura-creación	No	N/A
vacmSecurityToGroupStatus	lectura-creación	No	N/A
vacmAccessTable/vacmAccessEntry			
vacmAccessContextPrefix	inaccesible	No	N/A
vacmAccessSecurityModel	inaccesible	No	N/A
vacmAccessSecurityLevel	inaccesible	No	N/A
vacmAccessContextMatch	lectura-creación	No	N/A
vacmAccessReadViewName	lectura-creación	No	N/A
vacmAccessWriteViewName	lectura-creación	No	N/A

vacmAccessNotifyViewName	lectura-creación	No	N/A
vacmAccessStorageType	lectura-creación	No	N/A
vacmAccessStatus	lectura-creación	No	N/A
vacmMIBViews			
vacmViewSpinLock	lectura-escritura	No	N/A
vacmViewTreeFamilyTable/vacmViewTreeFamilyEntry			
vacmViewTreeFamilyViewName	inaccesible	No	N/A
vacmViewTreeFamilySubtree	inaccesible	No	N/A
vacmViewTreeFamilyMask	lectura-creación	No	N/A
vacmViewTreeFamilyType	lectura-creación	No	N/A
vacmViewTreeFamilyStorageType	lectura-creación	No	N/A
vacmViewTreeFamilyStatus	lectura-creación	No	N/A
snmpCommunityMIB [RFC 2576]			
snmpCommunityMIBObjects			
snmpCommunityTable/snmpCommunityEntry			
snmpCommunityIndex	inaccesible	No	N/A
snmpCommunityName	lectura-creación	No	N/A
snmpCommunitySecurityName	lectura-creación	No	N/A
snmpCommunityContextEngineID	lectura-creación	No	N/A
snmpCommunityContextName	lectura-creación	No	N/A
snmpCommunityTransportTag	lectura-creación	No	N/A
snmpCommunityStorageType	lectura-creación	No	N/A
snmpCommunityStatus	lectura-creación	No	N/A
snmpTargetAddrExtTable/snmpTargetAddrExtEntry			
snmpTargetAddrTMask	lectura-creación	No	N/A
snmpTargetAddrMMS	lectura-creación	No	N/A

clabSecCertObject			
clabSrvcPrvdrRootCACert	sólo lectura	N/A	N/A
clabCVCRootCACert	sólo lectura	N/A	N/A
clabCVCCACert	sólo lectura	N/A	N/A
clabMfgCVCCert	sólo lectura	N/A	N/A

Anexo B

Formato y contenido de los eventos, SYSLOG y trampa SNMP

El cuadro B.1 resume el formato y el contenido de las anotaciones históricas de eventos, de los mensajes syslog y trampa SNMP.

Las filas del cuadro B.1 especifican los eventos que el PS puede generar. Estos eventos ha de comunicarlos el PS por cualquier medio de los tres siguientes o por todos ellos: anotación histórica local de los eventos implementada por el cuadro local de eventos de RFC 2669, SYSLOG, y SNMP trap. El formato SYSLOG se especifica en 6.5.1.3 y el formato de la trampa SNMP se define en el presente anexo a continuación del cuadro.

En la primera y segunda columna se indican la fase en que se produce el evento. La tercera columna indica la prioridad asignada al evento. Estas prioridades coinciden con las comunicadas en el objeto docsDevEvLevel de RFC 2669 y en el campo LEVEL del mensaje syslog.

La cuarta columna especifica el texto del evento, que se comunica en el objeto docsDevEvText de RFC 2669 y el campo de texto del mensaje syslog. La quinta columna proporciona información adicional sobre el texto del evento de la cuarta columna. Por ejemplo, algunos de los campos de texto del evento son constantes mientras que otros campos de texto del evento contienen información variable. Algunas de las variables sólo son necesarias en el SYSLOG como se describe en la quinta columna. La sexta columna especifica el conjunto de códigos de error.

La séptima columna indica un número único de identificación para el evento, que se asigna al objeto docsDevEvId y al campo <eventId> del mensaje syslog. La octava columna especifica la trampa SNMP, que notifica este evento al receptor de eventos SNMP.

Las reglas para generar un ID único de evento partiendo del código de error se describen en 6.5.1.3. Los ID de eventos del cuadro se expresan en formato decimal.

Para ilustrar más adecuadamente el cuadro, se presenta a continuación un ejemplo que utiliza la primera fila de la sección de eventos de actualización de soporte lógico.

La primera y segunda columnas son "Actualización del SW" e "INICIALIZACIÓN DE ACTUALIZACIÓN DE SOPORTE LÓGICO". La prioridad del evento es "Notificación". El texto del evento es "INIT de descarga de soporte lógico – Mediante NMS". La quinta columna contiene "Únicamente para SYSLOG, añadir: dirección MAC: <P1> P1 = dirección MAC del PS". Esto es una nota sobre SYSLOG. Es decir, el cuerpo del texto del SYSLOG sería "INIT de descarga del soporte lógico – Mediante NMS – dirección MAC: x1 x2 x3 x4 x5 x6".

La última columna "TRAP NAME" es cabhPsDevSwUpgradeInitTrap, cuyo formato se proporciona al final del presente anexo.

Cuadro B.1/J.191 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de errores	ID del evento	Nombre de la trampa
Errores DHCP antes de completar la configuración							
Inicialización	DHCP	Crítica	FALLÓ DHCP – Enviado Discover, no se recibe offer		D01.0	68000100	
Inicialización	DHCP	Crítica	FALLÓ DHCP – Enviado Request, no hay respuesta		D02.0	68000200	
Inicialización	DHCP	Crítica	FALLÓ DHCP – Información solicitada no soportada		D03.0	68000300	
Inicialización	DHCP	Crítica	ERROR DE DHCP – La respuesta no contiene todos los campos válidos o el PS no puede determinar el modo de configuración		D03.1	68000301	
Errores de ToD antes de completar la configuración							
Inicialización	ToD	Alarma	Enviada petición ToD – no se recibe respuesta		D04.1	68000401	
Inicialización	ToD	Alarma	Recibida respuesta ToD – Formato de datos no válido		D04.2	68000402	
Errores TFTP antes de completar la configuración							
Inicialización	TFTP	Crítica	Falló TFTP – Enviada petición – No hay respuesta		D05.0	68000500	
Inicialización	TFTP	Crítica	Falló TFTP – NO ENCONTRADO el fichero de configuración	Únicamente para SYSLOG: añadir: nombre del fichero = <P1> P1 = nombre del fichero solicitado	D06.0	68000600	
Inicialización	TFTP	Crítica	Falló TFTP – paquetes DESORDENADOS		D07.0	68000700	
Inicialización	TFTP	Crítica	Fichero TFTP completo – pero falló la verificación del troceo SHA-1	Únicamente para SYSLOG: añadir: nombre del fichero = <P1> P1 = nombre del fichero TFTP	D08.0	68000800	
Inicialización	TFTP	Crítica	Falló TFTP – Sobrepasado el máximo número de reintentos	Únicamente para SYSLOG: añadir: límite de reintentos = <P1> P1 = número máximo de reintentos	D09.0	68000900	
TFTP conseguido							

Cuadro B.1/J.191 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de errores	ID del evento	Nombre de la trampa
Inicialización	TFTP	Notificación	TFTP conseguido		D10.0	68001000	
Análisis sintáctico TLV							
Inicialización	Análisis sintáctico TLV	Notificación	TLV-28 – OID no reconocida		I401.0	73040100	cabhPsDev InitTLV Unknown Trap
Inicialización	Análisis sintáctico TLV	Notificación	TLV desconocida <P1>	Únicamente para SYSLOG: <P1> = el TLV completo en hexadecimal	I401.1	73040101	cabhPsDev InitTLV Unknown Trap
Inicialización	Análisis sintáctico TLV	Notificación	Formato o contenido TLV no válido <P1>	Únicamente para SYSLOG: <P1> = el TLV completo en hexadecimal	I401.2	73040102	
Configuración							
Inicialización	SNMP Inform	Notificación	SNMP Inform enviado para indicar que se ha completado la configuración (pass/fail)	Únicamente para SYSLOG, añadir dirección MAC: <P1>. P1 = dirección MAC del PS	I11.0	73001100	cabhPsDev InitTrap
Inicialización	Retransmisión de SNMP Inform	Crítica	SNMP Inform enviado para indicar que se ha completado la configuración (pass/fail), sin respuesta. Se vuelve a enviar SNMP Inform	Únicamente para SYSLOG, añadir dirección MAC: <P1>. P1 = dirección MAC del PS	I11.1	73001101	cabhPsDev InitRetry Trap
Inicialización de actualización del SW (nota)							
Actualización del SW	Inicialización de actualización del SW	Notificación	INIT de descarga de soporte lógico – mediante NMS	Únicamente para SYSLOG, añadir: fichero de soporte lógico: <P1> – servidor de soporte lógico: <P2>. P1 = nombre del fichero de soporte lógico y P2 = dirección IP del servidor TFTP	E101.0	69010100	cabhPsDev SwUpgrade InitTrap

Cuadro B.1/J.191 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de errores	ID del evento	Nombre de la trampa
Actualización del SW	Inicialización de actualización del SW	Notificación	INIT de descarga de soporte lógico – mediante fichero de configuración <P1>	P1 = nombre del fichero de configuración CM. Únicamente para SYSLOG, añadir: fichero de soporte lógico: <P2> − servidor de soporte lógico: <P3>. P2 = nombre del fichero de soporte lógico y P3 = dirección IP del servidor TFTP	E102.0	69010200	cabhPsDev SwUpgrade InitTrap
Fallo general de la actualización del SW (nota)							
Actualización del SW	Fallo general de la actualización del SW	Error	Actualización de soporte lógico fallida durante descarga – superado máximo de reintentos (3)	Únicamente para SYSLOG, añadir: fichero de soporte lógico: <P1> − servidor de soporte lógico: <P2>. P1 = nombre del fichero de soporte lógico y P2 = dirección IP del servidor TFTP	E103.0	69010300	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización del SW	Error	Actualización de soporte lógico fallida antes de la descarga – servidor ausente	Únicamente para SYSLOG, añadir: fichero de soporte lógico: <P1> − servidor de soporte lógico: <P2>. P1 = nombre del fichero de soporte lógico y P2 = dirección IP del servidor TFTP	E104.0	69010400	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización del SW	Error	Actualización de soporte lógico fallida antes de la descarga – fichero ausente	Únicamente para SYSLOG, añadir: fichero de soporte lógico: <P1> – servidor de soporte lógico: <P2>. P1 = nombre del fichero de soporte lógico y P2 = dirección IP del servidor TFTP	E105.0	69010500	cabhPsDev SwUpgrade FailTrap

Cuadro B.1/J.191 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de errores	ID del evento	Nombre de la trampa
Actualización del SW	Fallo general de la actualización del SW	Error	Actualización de soporte lógico fallida antes de la descarga – sobrepasado el número máximo de reintentos TFTP	Únicamente para SYSLOG, añadir: fichero de soporte lógico: <P1> – servidor de soporte lógico: <P2>. P1 = nombre del fichero de soporte lógico y P2 = dirección IP del servidor TFTP	E106.0	69010600	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización del SW	Error	Actualización de soporte lógico fallida tras descarga – fichero de soporte lógico incompatible	Únicamente para SYSLOG, añadir: fichero de soporte lógico: <P1> – servidor de soporte lógico: <P2>. P1 = nombre del fichero de soporte lógico y P2 = dirección IP del servidor TFTP	E107.0	69010700	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización del SW	Error	Actualización de soporte lógico fallida tras descarga –fichero de soporte lógico corrompido	Únicamente para SYSLOG, añadir: fichero de soporte lógico: <P1> – servidor de soporte lógico: <P2>. P1 = nombre del fichero de soporte lógico y P2 = dirección IP del servidor TFTP	E108.0	69010800	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización del SW	Error	Interrupción de la descarga de soporte lógico – fallo de la alimentación	Únicamente para SYSLOG, añadir: fichero de soporte lógico: <P1> – servidor de soporte lógico: <P2>. P1 = nombre del fichero de soporte lógico y P2 = dirección IP del servidor TFTP	E109.0	69010900	cabhPsDev SwUpgrade FailTrap

Cuadro B.1/J.191 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de errores	ID del evento	Nombre de la trampa
Actualización del SW	Fallo general de la actualización del SW	Error	Interrupción de la descarga de soporte lógico – supresión de RF	Únicamente para SYSLOG, añadir: fichero de soporte lógico: <P1> – servidor de soporte lógico: <P2>. P1 = nombre del fichero de soporte lógico y P2 = dirección IP del servidor TFTP	E110.0	69011000	cabhPsDev SwUpgrade FailTrap
Éxito de la actualización del SW (nota)							
Actualización del SW	Éxito de la actualización del SW	Notificación	Éxito del soporte lógico descargado mediante NMS	Únicamente para SYSLOG, añadir: fichero de soporte lógico: <P1> – servidor de soporte lógico: <P2>. P1 = nombre del fichero de soporte lógico y P2 = dirección IP del servidor TFTP	E111.0	69011100	cabhPsDev SwUpgrade SuccessTrap
Actualización del SW	Éxito de la actualización del SW	Notificación	Éxito del soporte lógico descargado mediante fichero de configuración	Únicamente para SYSLOG, añadir: fichero de soporte lógico: <P1> – servidor de soporte lógico: <P2>. P1 = nombre del fichero de soporte lógico y P2 = dirección IP del servidor TFTP	E112.0	69011200	cabhPsDev SwUpgrade SuccessTrap
Fallo del DHCP tras completarse la configuración							
DHCP		Error	Enviado RENEW DHCP – sin respuesta		D101.0	68010100	cabhPsDev DHCPFail Trap
DHCP		Error	Enviado REBIND DHCP – sin respuesta		D102.0	68010200	cabhPsDev DHCPFail Trap
DHCP		Error	Enviado RENEW DHCP – opción DHCP no válida		D103.0	68010300	cabhPsDev DHCPFail Trap
DHCP		Error	Enviado REBIND DHCP – opción DHCP no válida		D104.0	68010400	cabhPsDev DHCPFail Trap
Fallo de ToD tras completarse la configuración							
ToD	ToD	Alarma	Petición ToD enviada – no se recibe respuesta		D04.3	68000403	cabhPsDev ToDFailTrap

Cuadro B.1/J.191 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de errores	ID del evento	Nombre de la trampa
ToD	ToD	Alarma	Respuesta ToD recibida – formato de datos no válido		D04.4	68000404	cabhPsDev ToDFailTrap
Verificación del fichero de código							
Actualización del SW	Fallo general de la actualización del SW	Error	Controles del fichero de código inadecuados	Únicamente para SYSLOG, añadir: fichero de código: <P1> – servidor del fichero de código: <P2>. P1= nombre del fichero de código, P2 = dirección IP del servidor del fichero de código	E201.0	69020100	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización del SW	Error	Fallo en la validación CVC del fabricante del fichero de código	Únicamente para SYSLOG, añadir: fichero de código: <P1> – servidor del fichero de código: <P2>. P1= nombre del fichero de código, P2 = dirección IP del servidor del fichero de código	E202.0	69020200	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización del SW	Error	Fallo en la validación CVS del fabricante del fichero de código	Únicamente para SYSLOG, añadir: fichero de código: <P1> – servidor del fichero de código: <P2>. P1= nombre del fichero de código, P2 = dirección IP del servidor del fichero de código	E203.0	69020300	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización del SW	Error	Fallo en la validación CVC del cofirmante del fichero de código	Únicamente para SYSLOG, añadir: fichero de código: <P1> – servidor del fichero de código: <P2>. P1= nombre del fichero de código, P2 = dirección IP del servidor del fichero de código	E204.0	69020400	cabhPsDev SwUpgrade FailTrap

Cuadro B.1/J.191 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de errores	ID del evento	Nombre de la trampa
Actualización del SW	Fallo general de la actualización del SW	Error	Fallo en la validación CVS del cofirmante del fichero de código	Únicamente para SYSLOG, añadir: fichero de código: <P1> – servidor del fichero de código: <P2>. P1= nombre del fichero de código, P2 = dirección IP del servidor del fichero de código	E205.0	69020500	cabhPsDev SwUpgrade FailTrap
Verificación del CVC							
Actualización del SW	Verificación del CVC	Error	Formato CVC del fichero de configuración inadecuado – servidor TFTP: <P1> – fichero de configuración: <P2>	P1 = dirección IP del servidor TFTP, P2 = nombre del fichero de configuración	E206.0	69020600	cabhPsDev SwUpgrade CVCFailTrap
Actualización del SW	Verificación del CVC	Error	Fallo en la validación CVC del fichero de configuración – servidor TFTP: <P1> – fichero de configuración: <P2>	P1 = dirección IP del servidor TFTP, P2 = nombre del fichero de configuración	E207.0	69020700	cabhPsDev SwUpgrade CVCFailTrap
Actualización del SW	Verificación del CVC	Error	Formato SNMP CVC inadecuado – gestor SNMP: <P1>	P1 = dirección IP del gestor SNMP	E208.0	69020800	cabhPsDev SwUpgrade CVCFailTrap
Actualización del SW	Verificación del CVC	Error	Fallo en la validación CVC de SNMP – gestor de SNMP: <P1>	P1 = dirección IP del gestor SNMP	E209.0	69020900	cabhPsDev SwUpgrade CVCFailTrap
Eventos CDP							
CDP	CDS	Notificación	Intento de asignar más direcciones IP LAN-Trans de las permitidas		P01.0	80000100	cabhPsDev CDP Threshold Trap
CDP	CDS	Notificación	No pudo obtener todas las direcciones IP de WAN-Data para las que se configuró el PS		P02.0	80000200	cabhPsDev CdpWanData IpTrap
CDP	CDS	Notificación	No pudo suministrar la dirección IP de cliente de LAN DHCP por agotamiento del grupo de direcciones		P03.0	80000300	cabhPsDev CdpLanIp PoolTrap

Cuadro B.1/J.191 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de errores	ID del evento	Nombre de la trampa
Eventos CSP							
CSP	Barrera contra fuegos	Notificación	Sobrepasado el umbral de piratería de la barrera contra fuegos tipo 1 y tipo 2		P101.0	80010100	cabhPsDev CSPTrap
CSP	Barrera contra fuegos	Notificación	Detectado evento tipo 1 de la barrera contra fuegos	P1 = dirección IP del origen, P2 = dirección IP de destino, P3 = tipo de protocolo, P4 = nombre del fichero del conjunto de reglas activas, P5 = descripción de evento	P102.0	80010200	cabhPsDev CSPTrap
CSP	Barrera contra fuegos	Notificación	Detectado evento tipo 2 de la barrera contra fuegos	P1 = dirección IP del origen, P2 = dirección IP de destino, P3 = tipo de protocolo, P4 = nombre del fichero del conjunto de reglas activas, P5 = descripción de evento	P103.0	80010300	cabhPsDev CSPTrap
CSP	Barrera contra fuegos	Notificación	Modificada la configuración de la barrera contra fuegos	P1 = descripción de la modificación de los parámetros de configuración de la barrera contra fuegos	P120.0	80012000	cabhPsDev CSPTrap
CSP	TFTP de la barrera contra fuegos	Crítica	Fracaso de la descarga TFTP del fichero de política de la barrera contra fuegos: se envió la solicitud y no hubo respuesta	P1 = URL del fichero de la política de la barrera contra fuegos solicitado	P130.0	80013000	cabhPsDev CSPTrap
CSP	TFTP de la barrera contra fuegos	Crítica	Fracaso de TFTP – no se encontró el fichero de la política de la barrea contra fuegos	P1 = URL del fichero de la política de la barrera contra fuegos solicitado	P131.0	80013100	cabhPsDev CSPTrap
CSP	TFTP de la barrera contra fuegos	Crítica	Fracaso de TFTP – fichero de política de la barrera contra fuegos inválido	P1 = URL del fichero de la política de la barrera contra fuegos solicitado	P132.0	80013200	cabhPsDev CSPTrap

Cuadro B.1/J.191 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de errores	ID del evento	Nombre de la trampa
CSP	TFTP de la barrera contra fuegos	Crítica	Descarga completa del fichero de la política de la barrera contra fuegos pero con fracaso de la verificación del troceo SHA-1	P1 = URL del fichero de la política de la barrera contra fuegos solicitado, P2 = valor del troceo del fichero de la política de la barrera contra fuegos	P133.0	80013300	cabhPsDev CSPTrap
CSP	TFTP de la barrera contra fuegos	Crítica	La descarga del fichero de la política de la barrera contra fuegos rebasó el número máximo permisible de reintentos TFTP	P1 = URL del fichero de la política de la barrera contra fuegos solicitado	P134.0	80013400	cabhPsDev CSPTrap
CSP	TFTP de la barrera contra fuegos	Notificación	Éxito de la descarga TFTP del fichero de la política de la barrera contra fuegos	P1 = URL del fichero de la política de la barrera contra fuegos solicitado Únicamente para SYSLOG: añadir: límite de reintentos = <P2> P2 = número máximo permitido de reintentos	P135.0	80013500	cabhPsDev CSPTrap
Eventos CAP							
CAP	C-NAT	Notificación	CAP incapaz de establecer la correspondencia C-NAT. No hay direcciones IP WAN-Data disponibles		P201.0	80020100	cabhPsDev CAPTrap
CAP	C-NAPT	Notificación	CAP incapaz de establecer la correspondencia C-NAPT. No hay direcciones IP WAN disponibles		P250.0	80025000	cabhPsDev CAPTrap
Eventos CTP							
CTP	Herramienta de velocidad de la conexión	Notificación	Se completó satisfactoriamente la prueba de la herramienta de velocidad de la conexión	P1 = dirección IP del origen P2 = dirección IP del destino P3 = protocolo P4 = caudal	P301.0	80030100	cabhPsDev CtpTrap

Cuadro B.1/J.191 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de errores	ID del evento	Nombre de la trampa
CTP	Herramienta de velocidad de la conexión	Notificación	Fin de temporización de la prueba de la herramienta de velocidad de la conexión	P1 = dirección IP del origen P2 = dirección IP del destino P3 = protocolo P4 = valor del temporizador (ms)	P302.0	80030200	cabhPsDev CtpTrap
CTP	Herramienta de velocidad de la conexión	Notificación	Anulación de la prueba de la herramienta de velocidad de la conexión	P1 = dirección IP del origen P2 = dirección IP del destino P3 = protocolo P4 = valor del temporizador (ms)	P303.0	80030300	cabhPsDev CtpTrap
CTP	Herramienta Ping	Notificación	Se completó satisfactoriamente la prueba de la herramienta Ping	P1 = dirección IP del origen P2 = dirección IP del destino P3 = Tiempo de ida y vuelta promedio	P320.0	80032000	cabhPsDev CtpTrap
CTP	Herramienta Ping	Notificación	Fin de temporización de la prueba de la herramienta Ping	P1 = dirección IP del origen P2 = dirección IP del destino P3 = número de peticiones enviadas P4 = número de respuestas recibidas	P321.0	80032100	cabhPsDev CtpTrap
CTP	Herramienta Ping	Notificación	Anulación de la prueba de la herramienta Ping	P1 = dirección IP del origen P2 = dirección IP del destino P3 = número de peticiones enviadas P4 = número de respuestas recibidas	P322.0	80032200	cabhPsDev CtpTrap

NOTA – Los eventos de actualización del soporte lógico (descarga segura de soporte lógico) se aplican únicamente a los servicios de portal autónomos. En el caso de un PS integrado el módem de cable se encarga del control de la actualización del soporte lógico así como de la gestión de los informes de los eventos correspondientes. Si se desea obtener mayor información, véase 11.3.7.1.

B.1 Descripción de las trampas

Todas las trampas determinadas para IPCable2Home se definen en la especificación de la MIB DEV del PS, [véase E.1].

Anexo C

Amenazas de seguridad y medidas preventivas

C.1 Amenazas de seguridad

Cuando se diseña una tecnología de seguridad es importante tener una idea precisa de las principales amenazas para una determinada aplicación o entorno. Esta información puede utilizarse para seleccionar las herramientas de seguridad y las tecnología más eficaces destinadas a proteger y prevenir los ataques maliciosos.

Las principales amenazas de seguridad de la red doméstica para abonados y operadores que se han advertido son las siguientes:

C.1.1 robo del servicio: El robo de servicios se presenta en dos formas, acceso no autorizado a los servicios de cable y reproducción no autorizada del contenido del servicio.

El acceso no autorizado supone que un abonado o un tercero (tal como un negocio) tenga acceso a los servicios del cable que no ha pagado. Los dispositivos pueden "clonarse" o modificarse para que parezcan dispositivos calificados de la red doméstica del abonado. Esto puede provocar asimismo la degradación de la calidad de funcionamiento del servicio ya que estos dispositivos consumen recursos adicionales de transporte de la HFC y de los enlaces en la red doméstica.

La reproducción no autorizada supone que un abonado o tercero (tal como un vecino) copie ilegalmente el contenido del servicio. En ciertos casos estas copias se distribuyen a otros consumidores sin la aprobación del operador ni del proveedor de contenidos.

C.1.2 ataques de denegación del servicio (DoS, *denial of service)*: Los ataques de denegación del servicio pueden tener lugar cuando un tercero (atacante, abonado hostil, etc.) perturba la comunicación y prestación de servicio normales entre operadores y abonados. Se puede insertar en el enlace del hogar transmisiones de datos ofensivas procedentes de fuentes o dispositivos aparentemente válidos, degradando gravemente el funcionamiento ordinario. Estas transmisiones de datos ofensivas podrían ampliarse asimismo a la red HFC del operador provocando en ella problemas de calidad de funcionamiento.

C.1.3 confidencialidad del servicio: La amenaza a la confidencialidad del servicio supone la supervisión o recepción de información acerca de un abonado o de los servicios utilizados por éste, por parte de un tercero (vecino, atacante, etc.). Esto podría provocar el robo de la información de las contraseñas o de la configuración de los dispositivos permitiendo a los atacantes ampliar su acceso a los recursos de la red del abonado y a los ficheros o datos confidenciales.

C.2 Medidas preventivas

Hay varios métodos que pueden utilizarse para evitar las amenazas de seguridad antedichas. Desgraciadamente, no hay un solo método que permita evitarlas todas, no obstante lo cual, una combinación de métodos podría constituir el mejor sistema de defensa. Se pueden utilizar las siguientes medidas preventivas:

C.2.1 autenticación: La autenticación supone la verificación de que las entidades emisora y receptora son quienes pretenden ser. Entre éstas se encuentran la fuente del servicio, el dispositivo receptor y el abonado.

La autenticación contribuye a evitar el robo del servicio al validar los dispositivos y usuarios finales, aunque no evita la copia ilegal de contenidos ni el acceso no autorizado por parte de terceros que supervisen el enlace. Evita razonablemente bien los ataques DoS porque se puede rechazar el tráfico cuando no proviene de un origen válido. En sí misma la autenticación no proporciona ningún soporte de confidencialidad de servicios, para lo que habría que usar la criptación.

C.2.2 protección de copias: Los métodos de protección de copias limitan la posibilidad de que un dispositivo receptor haga copias no autorizadas de los contenidos del servicio.

La protección de copia contribuye a evitar el robo del servicio limitando el número máximo de copias que puede realizarse, pero no evita el acceso no autorizado a los servicios. No evita la DoS ni protege la confidencialidad del servicio. En general, esta medida preventiva se implementa en las capas superiores de la aplicación.

C.2.3 criptación de datos: La criptación de datos evita la divulgación o acceso no autorizado a los datos.

La criptación de datos es un excelente modo de proporcionar confidencialidad sobre los datos y protección frente al robo del servicio. La criptación funciona impidiendo la lectura de los datos sin la clave de descriptación adecuada, no obstante lo cual no valida las entidades de origen y recepción y no proporciona protección contra copias una vez descriptados los datos. Tampoco evita los ataques DoS.

C.2.4 Barrera contra fuegos: Las aplicaciones de barrera contra fuegos evitan que el tráfico de la red pase de un dominio a otro sin satisfacer determinados criterios establecidos por el abonado o el operador. En las redes domésticas, las barreras contra fuegos se suelen ubicar en los dispositivos domésticos de pasarela que conectan la red HFC a la red doméstica.

Una aplicación barrera contra fuegos contribuye a evitar los ataques DoS y los de confidencialidad procedentes del lado de red de área extensa (WAN) de la barrera contra fuegos, aunque no evita el tipo de ataques procedente del lado del hogar de la barrera contra fuegos. Tampoco protege del robo del servicio.

C.2.5 seguridad de los mensajes de gestión: Este método de prevención implica la autenticación y criptación únicamente de los mensajes de gestión de la red. Los mensajes de gestión de la red se utilizan para la configuración de dispositivos, supervisión y control de la red, prestación de servicios y reservas de la calidad de servicio (QoS).

La seguridad de los mensajes de gestión constituye un buen mecanismo para evitar los ataques DoS mediante la autenticación y criptación de los mensajes de gestión. La información personal del abonado y de la configuración de la red queda asimismo protegida de los ataques de confidencialidad, aunque no ocurre lo mismo con el contenido de los servicios. Asimismo, la seguridad de mensajes de gestión no evita el robo del contenido de los servicios por parte de entidades no autorizadas.

Anexo D

Aplicaciones a través de CAT y barreras contra fuegos

Se sabe que la presencia del NAT y de la funcionalidad de barreras contra fuegos perturban determinados protocolos de aplicaciones. Los siguientes protocolos de aplicaciones DEBEN trabajar a través de implementaciones CAT y barreras contra fuegos de IPCable2Home. Esta lista NO supone ninguna prioridad específica.

1) FTP.
2) Aplicaciones par-a-par (es decir, Gnutella, LimeWire, BearShare, Morpheus, etc.).
3) IPSec.
4) Multidifusión IGMP e IP.
5) H.323 (Utilizado en diversas aplicaciones sobre Windows).
6) Aplicaciones de mensajería instantánea (es decir, AOL, Microsoft, Yahoo, etc.).
7) Correo electrónico (SMTP y POP).
8) Aplicaciones de transmisión de multimedia (por ejemplo, Real, MediaPlayer, etc.).

Además, los fabricantes DEBERÍAN intentar soportar, en la medida de lo posible, las aplicaciones de juegos a través de implementaciones CAT y barreras contra fuegos.

La norma RFC 3235 expone en términos generales varias directrices útiles para la creación de aplicaciones de modo que no se vean afectadas cuando se apliquen durante la utilización de la funcionalidad de la traducción de la dirección de red. Se recomienda definitivamente a los desarrolladores de las aplicaciones que funcionarán dentro del entorno de IPCable2Home que se apeguen a dichas directrices.

Anexo E

Las MIB

E.1 MIB del servicio de portal (PS)

La MIB Dev del PS DEBE implementarse como se define a continuación.

```
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,
   InetAddressIPv4,
   InetAddressIPv6                    FROM INET-ADDRESS-MIB

   docsDevSwCurrentVers,
   docsDevEvLevel,
   docsDevEvId,
   docsDevEvText,
   docsDevSwFilename,
   docsDevSwServer                    FROM DOCS-CABLE-DEVICE-MIB -- RFC 2669

   cabhCdpServerDhcpAddress,
   cabhCdpWanDataAddrClientId,
   cabhCdpLanTransThreshold           FROM CABH-CDP-MIB

   clabProjCableHome                  FROM CLAB-DEF-MIB;

--============================================================================
--
--   History:
--
--
--============================================================================


cabhPsDevMib MODULE-IDENTITY
    LAST-UPDATED    "0209200000Z"-- September 20, 2002
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
                    400 Centennial Parkway
                    Louisville, Colorado 80027-1266
                    U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
```

```
    DESCRIPTION
            "This MIB module supplies the basic management objects
             for the PS Device.  The PS device parameter describes
             general PS Device attributes and behaviour characteristics.
             Most of the PS Device MIB is needed for configuration download."


    ::=  { clabProjCableHome 1 }

-- Textual conventions
     X509Certificate ::= TEXTUAL-CONVENTION
       STATUS current
       DESCRIPTION
          "An X509 digital certificate encoded as an ASN.1 DER object."
       SYNTAX OCTET STRING (SIZE (0..4096))


cabhPsDevMibObjects    OBJECT IDENTIFIER ::= { cabhPsDevMib 1 }
cabhPsDevBase        OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 1 }
cabhPsDevProv     OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 2 }

--
-- The following group describes the base objects in the PS.
-- These are device based parameters.
--

cabhPsDevDateTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "The date and time, with optional timezone
             information."
    ::= { cabhPsDevBase 1 }

cabhPsDevResetNow       OBJECT-TYPE
SYNTAX                  TruthValue
MAX-ACCESS    read-write
STATUS                  current
DESCRIPTION
"Setting this object to true(1) causes the stand-alone or embedded PS device to
reboot. Device code initializes as if starting from a power-on reset. The CMP
ensures that MIB object values persist as specified. Reading this object always
returns false(2)."
::= { cabhPsDevBase 2 }

cabhPsDevSerialNumber OBJECT-TYPE
SYNTAX      SnmpAdminString (SIZE (0..128))
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "The manufacturer's serial number for this PS. This parameter
    is manufacturer provided and is stored in non-volatile memory."
::= { cabhPsDevBase 3 }

cabhPsDevHardwareVersion OBJECT-TYPE
SYNTAX      SnmpAdminString (SIZE (0..48))
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "The manufacturer's hardware version for this PS.  This
    parameter is manufacturer provided and is stored in non-volatile
    memory."
::= { cabhPsDevBase 4 }
```

```
cabhPsDevWanManMacAddress OBJECT-TYPE
SYNTAX      PhysAddress
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
"The PS WAN-MAN MAC address. This is the PS hardware address
to be used by the CDC to uniquely identify the PS to the cable data network DHCP
server for the acquisition of an IP address to be used for
management messaging between the cable network NMS and the CMP."


::= { cabhPsDevBase 5 }

cabhPsDevWanDataMacAddress OBJECT-TYPE
     SYNTAX      PhysAddress
     MAX-ACCESS  read-only
     STATUS      current
     DESCRIPTION
       "The PS WAN-Data MAC address. The PS could have multiple WAN-Data
       Interfaces, which share the same hardware address. The client
       identifiers will be unique so that each may be assigned
       a different, unique IP address."


    ::= { cabhPsDevBase 6 }

cabhPsDevTypeIdentifier    OBJECT-TYPE
     SYNTAX      SnmpAdminString
     MAX-ACCESS  read-only
     STATUS      current
     DESCRIPTION
       "This is a copy of the device type identifier used in the
       DHCP option 60 exchanged between the PS and the
       DHCP server."
     ::= { cabhPsDevBase 7 }

cabhPsDevSetToFactory    OBJECT-TYPE
     SYNTAX      TruthValue
     MAX-ACCESS  read-write
     STATUS      current
     DESCRIPTION
       "Setting this object to true(1) sets all PsDev MIB objects
       to the factory default values. Reading this object always
       returns false(2)."

    ::= { cabhPsDevBase 8 }

cabhPsDevWanManClientId    OBJECT-TYPE
     SYNTAX      OCTET STRING (SIZE (1..80))
     MAX-ACCESS  read-write
     STATUS      current
     DESCRIPTION
       "This is the client ID used for WAN-MAN DHCP requests.
       The default value is the 6 byte MAC address."
::= { cabhPsDevBase 9 }

cabhPsDevTodSyncStatus OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
          "This object indicates whether the PS was able to
          successfully synchronize with the Time of Day (ToD)
```

```
          Server in the cable network. The PS sets this object
          to true(1) if the PS successfully synchronizes its time
          with the ToD server. The PS sets this object to
          false(2) if the PS does not successfully synchronize
          with the ToD server."
    DEFVAL { false }
::= { cabhPsDevBase 10 }

cabhPsDevProvMode  OBJECT-TYPE
     SYNTAX    INTEGER
     {
       dhcpmode(1),
       snmpmode(2)
     }
     MAX-ACCESS  read-only
     STATUS    current
     DESCRIPTION
       "This object indicates the provisioning mode in which the
       PS is operating. If the PS is operating in DHCP Provisioning
       Mode, the PS sets this object to dhcpmode(1). If the PS is operating in
       SNMP Provisioning Mode, the PS sets this object to snmpmode(2)."
::={ cabhPsDevBase 11 }



--
--   The following group defines Provisioning Specific parameters
--

cabhPsDevProvisioningTimer OBJECT-TYPE
     SYNTAX      INTEGER (0..16383)
     UNITS    "minutes"
     MAX-ACCESS  read-write
     STATUS      current
     DESCRIPTION
       "This object enables the user to set the duration of the provisioning
       timeout timer. The value is in minutes. Setting the timer
       to 0 disables it. The default value for the timer is 5."
     DEFVAL {5}
     ::=  {cabhPsDevProv 1}

cabhPsDevProvConfigFile OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..128))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The URL of the TFTP host for downloading provisioning
             and configuration parameters to this device. Returns NULL if the
             server address is unknown."
    ::= { cabhPsDevProv 2 }

cabhPsDevProvConfigHash OBJECT-TYPE
     SYNTAX OCTET STRING (SIZE(20))
     MAX-ACCESS read-write
     STATUS current
     DESCRIPTION
       "Hash of the contents of the config file, calculated and
       sent to the PS prior to sending the config file. For the
       SHA-1 authentication algorithm the hash length is 160 bits."
     ::= { cabhPsDevProv 3 }

cabhPsDevProvConfigFileSize OBJECT-TYPE
     SYNTAX    Integer32
     UNITS    "bytes"
```

```
     MAX-ACCESS  read-only
     STATUS    current
     DESCRIPTION
       "Size of the configuration file."
     ::={ cabhPsDevProv 4 }

cabhPsDevProvConfigFileStatus OBJECT-TYPE
     SYNTAX    INTEGER
     {
            idle      (1),
            busy    (2)
     }
     MAX-ACCESS  read-only
     STATUS    current
     DESCRIPTION
       "This object indicates the current status
       of the configuration file download process. It is
       provided to indicate to the management entity
       that the PS will reject PS Configuration File triggers
       (set request to cabhPsDevProvConfigFile) when busy."
     ::={ cabhPsDevProv 5 }

cabhPsDevProvConfigTLVProcessed OBJECT-TYPE
     SYNTAX    INTEGER (0..16383)
     MAX-ACCESS  read-only
     STATUS    current
     DESCRIPTION
       "Number of TLVs processed in config file."
     ::={ cabhPsDevProv 6 }

cabhPsDevProvConfigTLVRejected OBJECT-TYPE
     SYNTAX    INTEGER (0..16383)
     MAX-ACCESS  read-only
     STATUS    current
     DESCRIPTION
       "Number of TLVs rejected in config file."
     ::={ cabhPsDevProv 7 }

cabhPsDevProvSolicitedKeyTimeout OBJECT-TYPE
   SYNTAX      Integer32 (15..600)
   UNITS  "seconds"
   MAX-ACCESS  read-write
   STATUS      current
     DESCRIPTION
       "This timeout applies only when the Provisioning Server initiated
       key management (with a Wake Up message) for SNMPv3.  It is the
       period during which the PS will save a number (inside the
       sequence number field) from the sent out AP Request and wait for the
       matching AP Reply from the Provisioning Server."
     DEFVAL { 120 }
     ::= { cabhPsDevProv 8 }


cabhPsDevProvState    OBJECT-TYPE
    SYNTAX      INTEGER
    {
            pass        (1),
            inProgress  (2),
            fail        (3)
    }
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "This object indicates the completion state of the
     initialization process. Pass or Fail states occur after
     completion of the initialization flow. InProgress occurs
     from PS initialization start to PS initialization end."
    ::= { cabhPsDevProv 9 }

cabhPsDevProvAuthState    OBJECT-TYPE
    SYNTAX      INTEGER
    {
            accepted    (1),
            rejected    (2)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object indicates the authentication state
            of the configuration file."
    ::= { cabhPsDevProv 10 }

cabhPsDevProvCorrelationId OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
             "Random value generated by the PS for use in registration
              authorization. It is for use only in the PS initialization
              messages and for PS configuration file download. This value
              appears in both cabhPsDevProvisioningStatus and
              cabhPsDevProvisioningEnrollmentReport informs to verify the
              instance of loading the configuration file."
    ::= { cabhPsDevProv 11 }

cabhPsDevTimeServerAddrType OBJECT-TYPE
        SYNTAX      InetAddressType
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The IP address type of the Time server (RFC-868).  IP version 4
            is typically used."
    ::= { cabhPsDevProv 12 }

cabhPsDevTimeServerAddr OBJECT-TYPE
        SYNTAX      InetAddress
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The IP address of the Time server (RFC-868). Returns
             0.0.0.0 if the time server IP address is unknown."
    ::= { cabhPsDevProv 13 }

--
-- Notification group is for future extension.
--

cabhPsNotification OBJECT IDENTIFIER ::= { cabhPsDevMib 2 0 }
cabhPsConformance  OBJECT IDENTIFIER ::= { cabhPsDevMib 3 }
cabhPsCompliances  OBJECT IDENTIFIER ::= { cabhPsConformance 1 }
cabhPsGroups       OBJECT IDENTIFIER ::= { cabhPsConformance 2 }

--
--    Notification Group
--
```

```
cabhPsDevInitTLVUnknownTrap     NOTIFICATION-TYPE
   OBJECTS   {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
      cabhPsDevWanManMacAddress
   }
   STATUS  current
   DESCRIPTION
           "Event due to detection of unknown TLV during
           the TLV parsing process.
           The values of docsDevEvLevel, docsDevEvId, and docsDevEvText are from
           the entry which logs this event in the docsDevEventTable. The value
           of cabhPsDevWanManMacAddress indicates the
           Wan-Man MAC address of the PS.
           This part of the information is uniform across all PS Traps."
   ::= { cabhPsNotification 1 }

cabhPsDevInitTrap  NOTIFICATION-TYPE
   OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
      cabhPsDevWanManMacAddress,
        cabhPsDevProvConfigFile,
        cabhPsDevProvConfigTLVProcessed,
        cabhPsDevProvConfigTLVRejected
   }
   STATUS      current
   DESCRIPTION
           "This inform is issued to confirm the successful completion
           of the provisioning process."
   ::= { cabhPsNotification 2 }

cabhPsDevInitRetryTrap  NOTIFICATION-TYPE
   OBJECTS  {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
      cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
           "An event to report a failure happened during the initialization
           process and detected in the PS."
   ::= { cabhPsNotification 3 }

cabhPsDevDHCPFailTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       cabhCdpServerDhcpAddress
   }
   STATUS  current
   DESCRIPTION
           "An event to report the failure of a DHCP server.
           The value of  cabhCdpServerDhcpAddress is the IP address
           of the DHCP server."
   ::= { cabhPsNotification 4 }
```

```
cabhPsDevSwUpgradeInitTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       docsDevSwFilename,
       docsDevSwServer
   }
   STATUS  current
   DESCRIPTION
           "An event to report a software upgrade initiated
           event. The values of docsDevSwFilename, and
           docsDevSwServer indicate the software image name
           and the server IP address the image is from."
   ::= { cabhPsNotification 5 }


cabhPsDevSwUpgradeFailTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       docsDevSwFilename,
       docsDevSwServer
   }
   STATUS  current
   DESCRIPTION
           "An event to report the failure of a software upgrade
           attempt. The values of docsDevSwFilename, and
           docsDevSwServer indicate the software image name
           and the server IP address the image is from."
   ::= { cabhPsNotification 6 }


cabhPsDevSwUpgradeSuccessTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       docsDevSwFilename,
       docsDevSwServer
   }
   STATUS  current
   DESCRIPTION
           "An event to report the Software upgrade success event.
           The values of docsDevSwFilename, and
           docsDevSwServer indicate the software image name
           and the server IP address the image is from."
   ::= { cabhPsNotification 7 }


cabhPsDevSwUpgradeCVCFailTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress
   }
```

```
    STATUS  current
    DESCRIPTION
            "An event to report the failure of the verification
            of code file happened during a secure software upgrade
            attempt."
    ::= { cabhPsNotification 8 }


cabhPsDevTODFailTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevTimeServerAddr,
        cabhPsDevWanManMacAddress
    }
    STATUS  current
    DESCRIPTION
            "An event to report the failure of a time of day server.
            The value of cabhPsDevTimeServerAddr indicates the server IP
            address."
    ::= { cabhPsNotification 9 }

cabhPsDevCdpWanDataIpTrap  NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhCdpWanDataAddrClientId,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "An event to report the failure of PS to obtain all needed WAN-Data
            Ip Addresses. cabhCdpWanDataAddrClientId indicates the ClientId for
            which the failure occured."
    ::= { cabhPsNotification 10 }


cabhPsDevCdpThresholdTrap  NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        cabhCdpLanTransThreshold
    }
    STATUS      current
    DESCRIPTION
            "An event to report that the Lan-Trans threshold has been exceeded."
    ::= { cabhPsNotification 11 }

cabhPsDevCspTrap  NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "To report an event with the Cable Security Portal."
    ::= { cabhPsNotification 12 }
```

```
cabhPsDevCapTrap  NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
           "To report an event with the Cable Address Portal."
   ::= { cabhPsNotification 13 }

cabhPsDevCtpTrap  NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
           "To report an event with the CableHome Test Portal."
   ::= { cabhPsNotification 14 }

cabhPsDevProvEnrollTrap  NOTIFICATION-TYPE
   OBJECTS {
       cabhPsDevHardwareVersion,
       docsDevSwCurrentVers,
       cabhPsDevTypeIdentifier,
       cabhPsDevWanManMacAddress,
       cabhPsDevProvCorrelationId
   }
   STATUS      current
   DESCRIPTION
           "This inform is issued to initiate the CableHome
            process provisioning."
   REFERENCE
        "Inform as defined in RFC 1902"
   ::= { cabhPsNotification 15 }

cabhPsDevCdpLanIpPoolTrap NOTIFICATION-TYPE
     OBJECTS {
     docsDevEvLevel, docsDevEvId, docsDevEvText, cabhPsDevWanManMacAddress,
     cabhCdpLanTransCurCount
     }
     STATUS current
     DESCRIPTION
"An event to report that the pool of IP addresses for LAN clients, as
defined by cabhCdpLanPoolStart and cabhCdpLanPoolEnd, is exhausted."

     ::= { cabhPsNotification 16}

-- compliance statements

cabhPsBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
             "The compliance statement for devices that implement
              PS feature."
    MODULE   --cabhPsMib
```

```
-- unconditionally mandatory groups

    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
        "Group of objects for PS MIB."
    ::= { cabhPsGroups 1 }

cabhPsNotificationGroup     NOTIFICATION-GROUP
     NOTIFICATIONS { cabhPsDevInitTLVUnknownTrap, cabhPsDevInitTrap,
cabhPsDevInitRetryTrap,
                     cabhPsDevDHCPFailTrap, cabhPsDevSwUpgradeInitTrap,
cabhPsDevSwUpgradeFailTrap,
                     cabhPsDevSwUpgradeSuccessTrap, cabhPsDevSwUpgradeCVCFailTrap,
cabhPsDevTODFailTrap,
                     cabhPsDevCdpWanDataIpTrap, cabhPsDevCdpThresholdTrap,
cabhPsDevCspTrap,
                     cabhPsDevCapTrap, cabhPsDevCtpTrap, cabhPsDevProvEnrollTrap }
     STATUS   current
     DESCRIPTION
       "These notifications deal with change in status of
       PS Device."
     ::= { cabhPsGroups 2 }

END
```

E.2 MIB del portal de prueba del cable

La MIB del CPT DEBE implementarse como se define a continuación.

```
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;

--============================================================================
--
--   History:
--
--   Date        Modified by          Reason
--
--============================================================================

cabhCtpMib MODULE-IDENTITY
    LAST-UPDATED  "0209200000Z" -- September 20, 2002
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
                            400 Centennial Parkway
                            Louisville, Colorado 80027-1266
                            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
            "This MIB module defines the diagnostic controls
            offered by the Cable Test Portal (CTP)."

    ::=  { clabProjCableHome 5 }

-- Textual conventions


cabhCtpObjects          OBJECT IDENTIFIER ::= { cabhCtpMib 1 }
cabhCtpBase             OBJECT IDENTIFIER ::= { cabhCtpObjects 1 }
cabhCtpConnSpeed                OBJECT IDENTIFIER ::= { cabhCtpObjects 2 }
cabhCtpPing                     OBJECT IDENTIFIER ::= { cabhCtpObjects 3 }

--
--   The following group describes the base objects in the Cable
--   Management Portal.
--
```

```
cabhCtpSetToFactory     OBJECT-TYPE
SYNTAX                  TruthValue
MAX-ACCESS   read-write
STATUS                  current
DESCRIPTION
"Setting this object to true(1) causes all the tables in the CTP MIB to
be cleared, and all CTP MIB objects with default values set back to those
default values. Reading this object always returns false(2)."
::={cabhCtpBase 1}

--
--   Parameter and results from Connection Speed Command
--

cabhCtpConnSrcIpType    OBJECT-TYPE
     SYNTAX    InetAddressType
     MAX-ACCESS  read-write
   STATUS      current
   DESCRIPTION
"The IP Address type used as the source address for the Connection
Speed Test."
     DEFVAL { ipv4 }
::= { cabhCtpConnSpeed 1 }

cabhCtpConnSrcIp OBJECT-TYPE
     SYNTAX    InetAddress
     MAX-ACCESS  read-write
   STATUS      current
   DESCRIPTION
"The IP Address used as the source address for the Connection
Speed Test. The default value is the value of cabhCdpServerRouter
(192.168.0.1)."
     REFERENCE
       " Specification 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
     "The IP Address Type for the CTP Connection Speed Tool destination
address."
     DEFVAL { ipv4 }
::={ cabhCtpConnSpeed 3 }




cabhCtpConnDestIp  OBJECT-TYPE
     SYNTAX         InetAddress
     MAX-ACCESS     read-write
    STATUS          current
    DESCRIPTION
            "The IP Address used as the destination address for the Connection
             Speed Test."
     ::= { cabhCtpConnSpeed 4 }
```

```
cabhCtpConnProto OBJECT-TYPE
     SYNTAX    INTEGER {
               udp        (1),
               tcp        (2)
               }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "The protocol used in the Connection Speed Test.  TCP
        testing is optional."
    DEFVAL { udp }
     ::= { cabhCtpConnSpeed 5 }


cabhCtpConnNumPkts OBJECT-TYPE
    SYNTAX    INTEGER (1..65535)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "The number of packets the CTP is to send when triggered to
 execute the Connection Speed Tool."
     DEFVAL { 100 }
     ::= { cabhCtpConnSpeed 6 }

cabhCtpConnPktSize OBJECT-TYPE
     SYNTAX    INTEGER (64..1518)
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The size of the test frames."
     REFERENCE
       ""
     DEFVAL { 1518 }
     ::= { cabhCtpConnSpeed 7 }

cabhCtpConnTimeOut OBJECT-TYPE
     SYNTAX    INTEGER (0..600000)            -- Max 10 minutes
     UNITS    "milliseconds"
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The timeout value for the response.  A value of zero indicates
             no time out and can be used for TCP only."
     DEFVAL {30000}   -- 30 seconds
    ::= { cabhCtpConnSpeed 8 }

cabhCtpConnControl OBJECT-TYPE
SYNTAX    INTEGER {
     start(1),
     abort(2)
     }
MAX-ACCESS   read-write
STATUS    current
DESCRIPTION
  "The control for the Connection Speed Tool. Setting this object to start(1)
causes the Connection Speed Tool to execute. Setting this object to abort(2)
causes the Connection Speed Tool to stop running. This parameter should only be
set via SNMP."
DEFVAL  {abort }
::={ cabhCtpConnSpeed 9 }
```

```
cabhCtpConnStatus  OBJECT-TYPE
SYNTAX    INTEGER {
     notRun(1),
     running(2),
complete(3),
aborted(4),
timedOut(5)
     }
MAX-ACCESS   read-only
STATUS    current
DESCRIPTION
   "The status of the Connection Speed Tool."
DEFVAL   { notRun }
::={ cabhCtpConnSpeed 10 }


cabhCtpConnPktsSent     OBJECT-TYPE
     SYNTAX    INTEGER (0..65535)
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of packets the CTP sent after it was triggered to
            execute the Connection Speed Tool."
     ::= { cabhCtpConnSpeed 11 }

cabhCtpConnPktsRecv     OBJECT-TYPE
     SYNTAX    INTEGER (0..65535)
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of packets the CTP received after it executed the
            Connection Speed Tool."
     ::= { cabhCtpConnSpeed 12 }

cabhCtpConnRTTOBJECT-TYPE
     SYNTAX   INTEGER (0..600000)
     UNITS    "millisec"
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The resulting round trip time for the set of
            packets sent to and received from the target LAN IP Device."
     ::= { cabhCtpConnSpeed 13 }

cabhCtpConnThroughput   OBJECT-TYPE
     SYNTAX    INTEGER (0..65535)
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The average round-trip throughput measured in
            kilobits per second."
     ::= { cabhCtpConnSpeed 14 }



--
--   Parameters and Results for Ping Command
--

cabhCtpPingSrcIpType    OBJECT-TYPE
SYNTAX    InetAddressType
MAX-ACCESS    read-write
STATUS    current
```

```
DESCRIPTION
  "The IP Address Type for CTP Ping Tool source address."
DEFVAL { ipv4 }
::={ cabhCtpPing 1 }

cabhCtpPingSrcIp OBJECT-TYPE
     SYNTAX    InetAddress
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP Address used as the source address for the Ping
            Test. The default value is the value of
             CabhCdpServerRouter (192.168.0.1)."
    REFERENCE
             " Specification Section 6.4.4"
    DEFVAL { 'c0a80001'h }
     ::= { cabhCtpPing 2 }

cabhCtpPingDestIpType   OBJECT-TYPE
SYNTAX    InetAddressType
MAX-ACCESS    read-write
STATUS    current
DESCRIPTION
  "The IP Address Type for the CTP Ping Tool destination address."
DEFVAL { ipv4 }
::={ cabhCtpPing 3 }

cabhCtpPingDestIp  OBJECT-TYPE
     SYNTAX    InetAddress
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Destination IP Address used as the destination address for
            the Ping Test."
     ::= { cabhCtpPing 4 }

cabhCtpPingNumPkts OBJECT-TYPE
     SYNTAX    INTEGER (1..4)
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The number of packets to send to each host."
     DEFVAL {1}
     ::= { cabhCtpPing 5 }

cabhCtpPingPktSize OBJECT-TYPE
     SYNTAX    INTEGER (64..1518)
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The size of the test frames."
     DEFVAL {64}
     ::= { cabhCtpPing 6 }

cabhCtpPingTimeBetween  OBJECT-TYPE
     SYNTAX    INTEGER (0..600000)
     UNITS    "milliseconds"
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The time between sending one ping and the next."
     DEFVAL { 1000 }
    ::= { cabhCtpPing 7 }
```

```
cabhCtpPingTimeOut      OBJECT-TYPE
SYNTAX    INTEGER (1..600000)
UNITS     "milliseconds"
MAX-ACCESS    read-write
STATUS    current
DESCRIPTION
  "The time out for ping response (ICMP reply) for a single transmitted ping
message (ICMP request)."
DEFVAL  { 5000 } -- 5 seconds
::={ cabhCtpPing 8 }



cabhCtpPingControl OBJECT-TYPE
SYNTAX    INTEGER {
     start(1),
     abort(2)
     }
MAX-ACCESS    read-write
STATUS    current
DESCRIPTION
  "The control for the Ping Tool. Setting this object to start(1) causes the
Ping Tool to execute. Setting this object to abort(2) causes the Ping Tool to
stop running. This parameter should only be set via SNMP."
DEFVAL  {abort }
::={ cabhCtpPing 9 }


cabhCtpPingStatus  OBJECT-TYPE
SYNTAX    INTEGER {
     notRun(1),
     running(2),
complete(3),
aborted(4),
timedOut(5)
     }
MAX-ACCESS    read-only
STATUS    current
DESCRIPTION
   "The status of the Ping Tool."
DEFVAL   { notRun }
::={ cabhCtpPing 10 }


cabhCtpPingNumSent      OBJECT-TYPE
SYNTAX    INTEGER (0..4)
MAX-ACCESS    read-only
STATUS    current
DESCRIPTION
  "The number of Pings sent"
::={ cabhCtpPing 11 }

cabhCtpPingNumRecv OBJECT-TYPE
     SYNTAX    INTEGER (0..255)
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of pings received."
     ::= { cabhCtpPing 12 }

cabhCtpPingAvgRTT  OBJECT-TYPE
     SYNTAX    INTEGER (0..600000)
     UNITS     "millisec"
     MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
            "The resulting average of round trip times for acknowledged
            packets."
     ::= { cabhCtpPing 13 }

cabhCtpPingMaxRTT  OBJECT-TYPE
     SYNTAX    INTEGER (0..600000)
     UNITS     "millisec"
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The resulting maximum of round trip times for acknowledged
            packets."
     ::= { cabhCtpPing 14 }

cabhCtpPingMinRTT  OBJECT-TYPE
     SYNTAX    INTEGER (0..600000)
     UNITS     "millisec"
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The resulting minimum of round trip times for acknowledged
            packets."
     ::= { cabhCtpPing 15 }

cabhCtpPingNumIcmpError OBJECT-TYPE
     SYNTAX    INTEGER (0..255)
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Number of ICMP errors."
     ::= { cabhCtpPing 16 }

cabhCtpPingIcmpError    OBJECT-TYPE
     SYNTAX    INTEGER (0..255)
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The last ICMP error."
     ::= { cabhCtpPing 17 }

--============================================================================

--
-- Notification group is for future extension.
--

cabhCtpNotification OBJECT IDENTIFIER ::= { cabhCtpMib 2 0 }
cabhCtpConformance  OBJECT IDENTIFIER ::= { cabhCtpMib 3 }
cabhCtpCompliances  OBJECT IDENTIFIER ::= { cabhCtpConformance 1 }
cabhCtpGroups       OBJECT IDENTIFIER ::= { cabhCtpConformance 2 }

--
--    Notification Group
--

-- compliance statements

cabhCtpBasicCompliance MODULE-COMPLIANCE
    STATUS     current
```

```
    DESCRIPTION
            "The compliance statement for devices that implement
             Portal Service feature."
    MODULE   --cabhCtpMib



-- unconditionally mandatory groups

    MANDATORY-GROUPS {
            cabhCtpGroup
    }

::= { cabhCtpCompliances 3 }


cabhCtpGroup OBJECT-GROUP
    OBJECTS {

        cabhCtpSetToFactory,
        cabhCtpConnSrcIpType,
        cabhCtpConnSrcIp,
        cabhCtpConnDestIpType,
        cabhCtpConnDestIp,
        cabhCtpConnProto,
        cabhCtpConnNumPkts,
        cabhCtpConnPktSize,
        cabhCtpConnTimeOut,
        cabhCtpConnControl,
        cabhCtpConnStatus,
        cabhCtpConnPktsSent,
        cabhCtpConnPktsRecv,
        cabhCtpConnRTT,
        cabhCtpConnThroughput,

        cabhCtpPingSrcIpType,
        cabhCtpPingSrcIp,
        cabhCtpPingDestIpType,
        cabhCtpPingDestIp,
        cabhCtpPingNumPkts,
        cabhCtpPingPktSize,
        cabhCtpPingTimeBetween,
        cabhCtpPingTimeOut,
        cabhCtpPingControl,
        cabhCtpPingStatus,
        cabhCtpPingNumSent,
        cabhCtpPingNumRecv,
        cabhCtpPingAvgRTT,
        cabhCtpPingMinRTT,
        cabhCtpPingMaxRTT,
        cabhCtpPingNumIcmpError,
        cabhCtpPingIcmpError
     }
    STATUS    current
    DESCRIPTION
        "Group of objects for CTP MIB."
    ::= { cabhCtpGroups 1 }

END
```

E.3 MIB de seguridad

La MIB de seguridad DEBE implementarse como se define a continuación.

```
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 -- RFC 2571
     X509Certificate         FROM DOCS-BPI2-MIB
     clabProjCableHome  FROM CLAB-DEF-MIB;

--=========================================================================
--
--   History:
--
--   Date     Modified by         Reason
--
--
--=========================================================================

cabhSecMib MODULE-IDENTITY
    LAST-UPDATED    "0209200000Z" --September 20, 2002
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal:     Cable Television Laboratories, Inc.
                        400 Centennial Parkway
                        Louisville, Colorado 80027-1266
                        U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
            "This MIB module supplies the basic management objects
            for the Security Portal Services."


    ::=  { clabProjCableHome 2 }

-- Textual conventions


cabhSecFwObjects   OBJECT IDENTIFIER ::= { cabhSecMib 1 }
cabhSecFwBase           OBJECT IDENTIFIER ::= { cabhSecFwObjects 1 }
cabhSecFwLogCtl    OBJECT IDENTIFIER ::= { cabhSecFwObjects 2 }
cabhSecCertObjects      OBJECT IDENTIFIER ::= { cabhSecMib 2 }
--
--   The following group describes the base objects in the Cable Home
--   Firewall.
--
```

```
cabhSecFwPolicyFileEnable OBJECT-TYPE
     SYNTAX      INTEGER {
              enable          (1),
              disable    (2)
              }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
         "This parameter indicates whether or not to enable the firewall
         functionality."
     DEFVAL {enable}
    ::= { cabhSecFwBase 1 }

cabhSecFwPolicyFileURL OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
"This object contains the name and IP address of the policy rule set
file in a TFTP URL format. Once this object has been updated, it will
trigger the file download."

::= { cabhSecFwBase 2 }



cabhSecFwPolicyFileHash OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(20))
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
"Hash of the contents of the rules set file, calculated and sent to the
PS prior to sending the rules set file.  For the SHA-1 authentication
algorithm the length of the hash is 160 bits. This hash value is
encoded in binary format."

::= { cabhSecFwBase 3 }


cabhSecFwPolicyFileOperStatus OBJECT-TYPE
     SYNTAX   INTEGER    {
               inProgress(1),
               completeFromProvisioning(2),
               completeFromMgt(3),
               failed(4)
     }
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION
        "InProgress(1) indicates that a TFTP download is under way,
         either as a result of a version mismatch at provisioning
         or as a result of a upgradeFromMgt request.
         CompleteFromProvisioning(2) indicates that the last
         software upgrade was a result of version mismatch at
         provisioning. CompleteFromMgt(3) indicates that the last
         software upgrade was a result of setting
         docsDevSwAdminStatus to upgradeFromMgt.
         Failed(4) indicates that the last attempted download
         failed, ordinarily due to TFTP timeout."

     ::= { cabhSecFwBase 4 }
```

```
cabhSecFwPolicyFileCurrentVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The rule set version currently operating in the PS device.
             This object should be in the syntax used by the individual
             vendor to identify software versions.  Any PS element MUST
             return a string descriptive of the current rule set file load.
             If this is not applicable, this object MUST contain an empty
             string."
     ::= { cabhSecFwBase 5 }

--
--   Firewall log parameters
--



cabhSecFwEventType1Enable OBJECT-TYPE
SYNTAX INTEGER {
       enable (1), -- log event
       disable (2) -- do not log event
       }
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"This object enables or disables logging of type 1 firewall event
messages. Type 1 event messages report attempts from both private and public
clients to traverse the firewall that violate the Security Policy."

DEFVAL { disable }
::= { cabhSecFwLogCtl 1 }

cabhSecFwEventType2Enable OBJECT-TYPE
SYNTAX INTEGER {
       enable (1), -- log event
       disable (2) -- do not log event
       }
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"This object enables or disables logging of type 2 firewall event
messages. Type 2 event messages report identified Denial of Service attack
attempts."

DEFVAL { disable }
::= { cabhSecFwLogCtl 2 }

cabhSecFwEventType3Enable OBJECT-TYPE
SYNTAX INTEGER {
enable (1), -- log event
disable (2) -- do not log event
}
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"Enables or disables logging of type 3 firewall event messages. Type 3 event
messages report changes made to the following firewall management
parameters: cabhSecFwPolicyFileURL, cabhSecFwPolicyFileCurrentVersion,
cabhSecFwPolicyFileEnable."
```

```
DEFVAL { disable }
::= { cabhSecFwLogCtl 3 }

cabhSecFwEventAttackAlertThreshold  OBJECT-TYPE
     SYNTAX   INTEGER    (0..65535)
     MAX-ACCESS read-write
     STATUS current
     DESCRIPTION
       "If the number of type 1 or 2 hacker attacks exceeds this
       threshold in the period defined by cabhSecFwEventAttackAlertPeriod, a
       firewall message event MUST be logged with priority level 4."
DEFVAL { 65535 }
     ::= { cabhSecFwLogCtl 4 }


cabhSecFwEventAttackAlertPeriod OBJECT-TYPE
SYNTAX INTEGER (0..65535)
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"Indicates the period to be used (in hours) for the
cabhSecFwEventAttackAlertThreshold. This MIB variable should always keep
track of the last x hours of events meaning that if the variable is set
to track events for 10 hours then when the 11th hour is reached, the 1st
hour of events is deleted from the tracking log. A default value is set
to zero, meaning zero time, so that this MIB variable will not track any
events unless configured."
DEFVAL {0}

::= { cabhSecFwLogCtl 5 }



cabhSecCertPsCert OBJECT-TYPE
SYNTAX    X509Certificate
MAX-ACCESS   read-only
STATUS    current
DESCRIPTION
"The X509 DER-encoded PS certificate."
REFERENCE
" Specification
 Section 11.3 Requirements (security requirements)"
::= { cabhSecCertObjects 1 }


--
-- Notification group is for future extension.
--

cabhSecNotification OBJECT IDENTIFIER ::= { cabhSecMib 3 0 }
cabhSecConformance  OBJECT IDENTIFIER ::= { cabhSecMib 4 }
cabhSecCompliances  OBJECT IDENTIFIER ::= { cabhSecConformance 1 }
cabhSecGroups       OBJECT IDENTIFIER ::= { cabhSecConformance 2 }

--
--    Notification Group
--



-- compliance statements

cabhSecBasicCompliance MODULE-COMPLIANCE
    STATUS     current
```

```
    DESCRIPTION
            "The compliance statement for Cable Firewall feature."
    MODULE   --cabhSecMib




-- unconditionally mandatory groups

    MANDATORY-GROUPS {
            cabhSecGroup
    }

::= { cabhSecCompliances 3 }


cabhSecGroup OBJECT-GROUP
    OBJECTS {
       cabhSecFwPolicyFileEnable,
       cabhSecFwPolicyFileURL,
       cabhSecFwPolicyFileHash,
       cabhSecFwPolicyFileOperStatus,
       cabhSecFwPolicyFileCurrentVersion,

       cabhSecFwEventType1Enable,
       cabhSecFwEventType2Enable,
       cabhSecFwEventType3Enable,
       cabhSecFwEventAttackAlertThreshold,
       cabhSecFwEventAttackAlertPeriod,
       cabhSecCertPsCert
    }
    STATUS    current
    DESCRIPTION
     "Group of object in Cable Firewall MIB"
    ::= { cabhSecGroups 1 }

END
```

E.4 Definición

La MIB de definición DEBE implementarse como se define a continuación.

```
CLAB-DEF-MIB DEFINITIONS ::= BEGIN
IMPORTS
     MODULE-IDENTITY,
     X509Certificate         FROM DOCS-BPI2-MIB
     enterprises        FROM SNMPv2-SMI;

cableLabs MODULE-IDENTITY
     LAST-UPDATED    "0209200000Z" -- September 20, 2002
    ORGANIZATION    "CableLabs"
    CONTACT-INFO
            "Ralph Brown
            Postal: Cable Television Laboratories, Inc.
                    400 Centennial Parkway
                    Louisville, Colorado 80027-1266
                    U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: r.brown@cablelabs.com"
```

```
    DESCRIPTION
            "This MIB module supplies the basic management object categories for
            Cable Labs."

    ::= { 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 }
clabProjOpenCable  OBJECT IDENTIFIER ::= { clabProject 3}
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
            "The X509 DER-encoded Service Provider Root CA Certificate."
    REFERENCE
    " Specification Section 11"
    ::= { clabSecCertObject 1 }

clabCVCRootCACert       OBJECT-TYPE
    SYNTAX    X509Certificate
    MAX-ACCESS   read-only
    STATUS    current
    DESCRIPTION
            "The X509 DER-encoded CVC Root CA Certificate."
    REFERENCE
    " Specification Section 11 for Standalone PS Elements only"
    ::= { clabSecCertObject 2 }

clabCVCCACert    OBJECT-TYPE
    SYNTAX    X509Certificate
    MAX-ACCESS   read-only
    STATUS    current
    DESCRIPTION
            "The X509 DER-encoded CableLabs CVC CA Certificate."
    REFERENCE
    " Specification Section 11 for Standalone PS Elements only"
    ::= { clabSecCertObject 3 }

clabMfgCVCCert     OBJECT-TYPE
    SYNTAX    X509Certificate
    MAX-ACCESS   read-only
    STATUS    current
    DESCRIPTION
            "The X509 DER-encoded Manufacturer CVC Certificate."
    REFERENCE
    " Specification Section 11 for Standalone PS Elements only"
    ::= { clabSecCertObject 4 }

END
```

E.5 MIB del portal DHCP del cable (CDP)

La MIB del CDP DEBE implementarse como se define a continuación.

```
CABH-CDP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
     Integer32,
     Unsigned32
                    FROM SNMPv2-SMI
     TruthValue,
     TimeStamp,
     RowStatus,
    TEXTUAL-CONVENTION
                    FROM SNMPv2-TC
    OBJECT-GROUP,
    MODULE-COMPLIANCE
                    FROM SNMPv2-CONF
    InetAddressType,
    InetAddress,
    InetAddressIPv4,
    InetAddressIPv6
                       FROM INET-ADDRESS-MIB
     SnmpAdminString         FROM SNMP-FRAMEWORK-MIB -- RFC 2571
    clabProjCableHome
                    FROM CLAB-DEF-MIB;

--============================================================================
--
--   History:
--
--   Date Modified by       Reason
--
--============================================================================

cabhCdpMib MODULE-IDENTITY
    LAST-UPDATED    "0209200000Z" -- September 20, 2002
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
                   400 Centennial Parkway
                    Louisville, Colorado 80027-1266
                    U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
     "This MIB module supplies the basic management objects
for the Cable DHCP Portal (CDP) portion of the PS database."



    ::=  { clabProjCableHome 4 }

-- Textual conventions
CabhCdpLanTransDhcpClientId ::= TEXTUAL-CONVENTION
     STATUS   current
     DESCRIPTION
       "LAN-Trans DHCP option61 information."
     SYNTAX OCTET STRING (SIZE (1..80))
```

```
cabhCdpObjects   OBJECT IDENTIFIER ::= { cabhCdpMib 1 }
cabhCdpBase      OBJECT IDENTIFIER ::= { cabhCdpObjects 1 }
cabhCdpAddr      OBJECT IDENTIFIER ::= { cabhCdpObjects 2 }
cabhCdpServer    OBJECT IDENTIFIER ::= { cabhCdpObjects 3 }
--
--   The following group describes the base objects in the Cable
--   DHCP Portal. The rest of this group deals with addresses defined on
--   the LAN side.
--

cabhCdpSetToFactory     OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Setting this object to true(1) causes the DHCP default options to
be returned back to factory defaults. Reading this object always returns
false(2). When cabhCdpSetToFactory is set to true, the following actions occur:
1. Clear all cabhCdpLanAddrEntries in the CDP LAN Address Table.
2. Reset all default CDS DHCP options to the factory defaults.
3. The CDS will offer the factory default DHCP options at the next lease renewal
time.
            The objects set to factory defaults are:
       cabhCdpLanTransThreshold,
       cabhCdpLanTransAction,
       cabhCdpWanDataIpAddrCount,
       cabhCdpLanStartType,
       cabhCdpLanPoolStart,
       cabhCdpLanPoolEndType,
       cabhCdpLanPoolEnd,
       cabhCdpNetworkNumber,
       cabhCdpServerSubnetMaskType,
       cabhCdpServerSubnetMask,
       cabhCdpServerTimeOffset,
       cabhCdpServerRouterType,
       cabhCdpServerRouter,
       cabhCdpServerDnsAddressType,
       cabhCdpServerDnsAddress,
       cabhCdpServerSyslogAddressType,
       cabhCdpServerSyslogAddress,
       cabhCdpServerDomainName,
       cabhCdpServerTTL,
       cabhCdpServerInterfaceMTU,
       cabhCdpServerVendorSpecific,
       cabhCdpServerLeaseTime,
       cabhCdpServerDhcpAddressType,
       cabhCdpServerDhcpAddress"
REFERENCE
""
::= { cabhCdpBase 1 }



cabhCdpLanTransCurCount OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The current number of LAN-Trans IP addresses for
            Translated addresses (NAT and NAPT Interconnects).
            This is a count of LAN side addresses."
     REFERENCE
       ""
    ::= { cabhCdpBase 2 }
```

```
cabhCdpLanTransThreshold OBJECT-TYPE
    SYNTAX      INTEGER (0..65533)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
     "The threshold number of LAN-Trans IP addresses allocated or assigned above
which the PS generates an alarm condition. Whenever an attempt is made to
allocate a LAN-Trans IP address when cabhCdpLanTransCurCount is greater than or
equal to cabhCdpLanTransThreshold, an event is generated. A value of 0 indicates
that the CDP sets the threshold at the highest number of addresses in the LAN
address pool."

     DEFVAL { 0 }
    ::= { cabhCdpBase 3 }

cabhCdpLanTransAction OBJECT-TYPE
    SYNTAX      INTEGER {
     normal    (1),
     noAssignment  (2)
     }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The action taken when the CDS assigns a LAN-Trans address
            and the number of LAN-Trans addresses assigned
            (cabhCdpLanTransCurCount) is greater than the threshold
            (cabhCdpLanTransThreshold). The actions are as follows:

          normal -  assign a LAN-Trans IP address and treat the
               interconnection between the LAN and WAN as
               would normally occur if the threshold was not
               exceeded.


          noAssignment - do not assign a LAN-Trans IP address and do
               not create an interconnection"
     REFERENCE
       ""
     DEFVAL { normal }
    ::= { cabhCdpBase 4 }

cabhCdpWanDataIpAddrCount OBJECT-TYPE
    SYNTAX      INTEGER ( 0..63 )
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This is the number of WAN-Data IP addresses that the CDC needs to
acquire via DHCP."

     REFERENCE
       ""
     DEFVAL { 0 }
    ::= { cabhCdpBase 5 }

--
--   CDP Address Management Tables
--
```

```
--=========================================================================
--
--   cabhCdpLanAddrTable (CDP LAN Address Table)
--
--   The cabhCdpLanAddrTable contains the DHCP parameters
--   for each IP address served to the LAN-Trans realm.
--
--   This table contains a list of entries for the LAN side CDP parameters.
--   These parameters can be set either by the CDP or by the cable operator
--   through the CMP.
--
--=========================================================================

cabhCdpLanAddrTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCdpLanAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table is a list of LAN-Trans realm parameters. This
            list has one entry for each allocated LAN-Trans IP
            address."
    ::= {  cabhCdpAddr 1 }

cabhCdpLanAddrEntry OBJECT-TYPE
    SYNTAX      CabhCdpLanAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "List of general parameter for CDP mappings."
    INDEX { cabhCdpLanAddrIpType, cabhCdpLanAddrIp }
    ::= { cabhCdpLanAddrTable 1 }

CabhCdpLanAddrEntry ::= SEQUENCE {
cabhCdpLanAddrIpType             InetAddressType,
     cabhCdpLanAddrIp            InetAddress,
     cabhCdpLanAddrClientID           CabhCdpLanTransDhcpClientId,
     cabhCdpLanAddrLeaseCreateTime        TimeStamp,
     cabhCdpLanAddrLeaseExpireTime        TimeStamp,
     cabhCdpLanAddrMethod             INTEGER,
     cabhCdpLanAddrHostName       SnmpAdminString,
     cabhCdpLanAddrRowStatus      RowStatus
    }

cabhCdpLanAddrIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The address type assigned on the LAN side for the CDP Address
Table."
    DEFVAL  { ipv4 }
    ::= { cabhCdpLanAddrEntry 1 }



cabhCdpLanAddrIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
"The address assigned on the LAN side for the CDP Address Table. This parameter
is entered by the CDP when the CDS grants a lease to a LAN IP Device in the
LAN-Trans realm and creates a row in this table. Alternatively, this parameter
can be created by the NMS through the CMP, when the NMS creates a new DHCP
```

```
address reservation by accessing the cabhCdpLanAddrRowStatus object with an
index comprised of a new cabhCdpLanAddrIp and its Type."

    ::= { cabhCdpLanAddrEntry 2 }

cabhCdpLanAddrClientID OBJECT-TYPE
    SYNTAX      CabhCdpLanTransDhcpClientId
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
     "The client ID as indicated in Option 61 of the DHCP Discover. There is a
     one-to-one relationship between the Client ID and the assigned LAN address.
     This parameter is entered by the CDP when the CDS grants a lease to a LAN
     IP Device in the LAN Trans realm and creates a row in this table.
     Alternatively, this parameter can be created by the NMS through the CMP,
     when the NMS creates a new DHCP address reservation by accessing the
     cabhCdpLanDataAddrRowStatus object with an index comprised of a new
     cabhCdpLanAddrIp and a new cabhCdpLanAddrClientID."

    ::= { cabhCdpLanAddrEntry 3 }

cabhCdpLanAddrLeaseCreateTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The time the LAN side of the CDP LAN Table was created.
       This entry is only set when the cabhCdpLanAddrTable
       entry is created and the entry does not already exist. In
       other words, this value is not overwritten at lease renewal
       time."
    ::= { cabhCdpLanAddrEntry 4 }

cabhCdpLanAddrLeaseExpireTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "This is the time that the LAN side lease expires.  When
       the lease expires this entry will be deleted from the table."
    ::= { cabhCdpLanAddrEntry 5 }

cabhCdpLanAddrMethod OBJECT-TYPE
    SYNTAX      INTEGER {
     cmp (1),
     cdp (2)
     }
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The method that created this Address Entry. cmp
       indicates that configuration through the CMP established this
       row (entry). cdp indicates that a DHCP discover established
       this row (entry)."
    ::= { cabhCdpLanAddrEntry 6 }

cabhCdpLanAddrHostName OBJECT-TYPE
    SYNTAX      SnmpAdminString(SIZE(0..80))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "This is the Host Name of the LAN IP address, based on DCHP Option 12."
    ::= { cabhCdpLanAddrEntry 7 }
```

```
cabhCdpLanAddrRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The RowStatus interlock for creation and deletion."
    ::= { cabhCdpLanAddrEntry 8 }


--------------------------------------------------------------------------
--
--   cabhCdpWanDataAddrTable (CDP WAN-Data Address Table)
--
--   The cabhCdpWanDataAddrTable contains the configuration or DHCP parameters
--   for each IP address mapping per WAN-Data IP Address.
--
--------------------------------------------------------------------------

cabhCdpWanDataAddrTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCdpWanDataAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains WAN-Data address realm information."
    ::= {  cabhCdpAddr 2 }

cabhCdpWanDataAddrEntry OBJECT-TYPE
    SYNTAX      CabhCdpWanDataAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "List of general parameter for CDP WAN-Data address realm."
    INDEX { cabhCdpWanDataAddrIndex }
    ::= { cabhCdpWanDataAddrTable 1 }

CabhCdpWanDataAddrEntry ::= SEQUENCE {
     cabhCdpWanDataAddrIndex     INTEGER,
     cabhCdpWanDataAddrClientId       OCTET STRING,
     cabhCdpWanDataAddrIpType         InetAddressType,
     cabhCdpWanDataAddrIp             InetAddress,
     cabhCdpWanDataAddrRenewalTime    Integer32,
     cabhCdpWanDataAddrRowStatus      RowStatus
    }


cabhCdpWanDataAddrIndex OBJECT-TYPE
    SYNTAX      INTEGER (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "Index into table."
    ::= { cabhCdpWanDataAddrEntry 1 }

cabhCdpWanDataAddrClientId OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE (1..80))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "A unique WAN-Data ClientID used when attempting to acquire a WAN-Data IP
Address via DHCP."
    ::= { cabhCdpWanDataAddrEntry 2 }
```

```
cabhCdpWanDataAddrIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The address type assigned on the WAN-Data side."
    DEFVAL { ipv4 }
    ::= { cabhCdpWanDataAddrEntry 3 }

cabhCdpWanDataAddrIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The address assigned on the WAN-Data side."
    ::= { cabhCdpWanDataAddrEntry 4 }

cabhCdpWanDataAddrRenewalTime OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "This is the time remaining before the lease expires.
       This is based on DHCP Option 51."
    ::= { cabhCdpWanDataAddrEntry 5 }

cabhCdpWanDataAddrRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The RowStatus interlock for creation and deletion."
    ::= { cabhCdpWanDataAddrEntry 6 }

--------------------------------------------------------------------------
--
--   cabhCdpWanDataAddrServerTable (CDP WAN-Data DNS Server Table)
--
--   The cabhCdpWanDataAddrServerTable contains a table of referral DNS Servers.

--
--------------------------------------------------------------------------

cabhCdpWanDataAddrServerTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCdpWanDataAddrServerEntry
     MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains the IP addresses used for the WAN-Data DNS
            hosts obtained via the DHCP option 6 during the WAN-Data process."
    ::= {  cabhCdpAddr 3 }

cabhCdpWanDataAddrServerEntry OBJECT-TYPE
    SYNTAX      CabhCdpWanDataAddrServerEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "List of WAN-Data DNS Hosts."
    INDEX { cabhCdpWanDataAddrDnsIpType, cabhCdpWanDataAddrDnsIp }
    ::= { cabhCdpWanDataAddrServerTable 1 }
```

```
CabhCdpWanDataAddrServerEntry ::= SEQUENCE {
    cabhCdpWanDataAddrDnsIpType  InetAddressType,
    cabhCdpWanDataAddrDnsIp      InetAddress,
    cabhCdpWanDataAddrDnsRowStatus    RowStatus
    }


cabhCdpWanDataAddrDnsIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This parameter indicates the IP address type of a DNS server."
     DEFVAL  { ipv4 }
     ::= { cabhCdpWanDataAddrServerEntry 1 }


cabhCdpWanDataAddrDnsIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This parameter indicates the IP address of a DNS server."
     ::= { cabhCdpWanDataAddrServerEntry 2 }

cabhCdpWanDataAddrDnsRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The RowStatus interlock for creation and deletion."
     ::= { cabhCdpWanDataAddrServerEntry 3 }


--
--   DHCP Server Side (CDS) Option Values for the LAN-Trans realm
--
cabhCdpLanPoolStartType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "The Address type of the start of range LAN Trans IP Addresses."
     DEFVAL { ipv4 }
    ::= { cabhCdpServer 1 }

cabhCdpLanPoolStart OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "The start of range LAN Trans IP Addresses."
     DEFVAL { 'c0a8000a'h }  -- 192.168.0.10
     -- 192.168.0.0 is the network number
     -- 192.168.0.255 is broadcast
     -- address and 192.168.0.1
     -- is reserved for the router
    ::= { cabhCdpServer 2 }

cabhCdpLanPoolEndType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
```

```
    DESCRIPTION
       "The Address type of the end of range LAN Trans IP Addresses."
     DEFVAL { ipv4 }
    ::= { cabhCdpServer 3 }

cabhCdpLanPoolEnd OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "The end of range for LAN-Trans IP Addresses."
     DEFVAL { 'c0a800fe'h }  -- 192.168.0.254
    ::= { cabhCdpServer 4 }

cabhCdpServerNetworkNumberType   OBJECT-TYPE
     SYNTAX    InetAddressType
MAX-ACCESS   read-write
STATUS    current
DESCRIPTION
  "The IP address type of the LAN-Trans network number."
DEFVAL  { ipv4 }
::= { cabhCdpServer 5 }

cabhCdpServerNetworkNumber       OBJECT-TYPE
SYNTAX    InetAddress
MAX-ACCESS   read-write
STATUS    current
DESCRIPTION
     "The LAN-Trans network number."
DEFVAL  { 'c0a80000'h }
::= { cabhCdpServer 6 }



cabhCdpServerSubnetMaskType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Type of LAN-Trans Subnet Mask."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 7 }

cabhCdpServerSubnetMask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
         "Option value 1 - Value of LAN-Trans Subnet Mask."
     DEFVAL { 'ffffff00'h }  -- 255.255.255.0
    ::= { cabhCdpServer 8 }

cabhCdpServerTimeOffset OBJECT-TYPE
    SYNTAX      Integer32 (-86400..86400)  -- 0 to 24 hours (in seconds)
    UNITS "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Option value 2 - Value of LAN-Trans Time Offset from
        Coordinated Universal Time (UTC)."
     DEFVAL { 0 }  -- UTC
    ::= { cabhCdpServer 9 }
```

```
cabhCdpServerRouterType OBJECT-TYPE
     SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Type of Address, Router for the LAN-Trans
            address realm."
     DEFVAL { ipv4 }
    ::= { cabhCdpServer 10 }

cabhCdpServerRouter     OBJECT-TYPE
     SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Option value 3 - Router for the LAN-Trans
            address realm."
     DEFVAL { 'c0a80001'h }  -- 192.168.0.1
    ::= { cabhCdpServer 11 }

cabhCdpServerDnsAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "The Type of IP Addresses of the LAN-Trans address realm
       DNS servers."
     DEFVAL { ipv4 }
    ::= { cabhCdpServer 12 }

cabhCdpServerDnsAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "The IP Addresses of the LAN-Trans address realm
       DNS servers. As a default there is only one DNS
       server and it is the address specified in Option
       Value 3 - cabhCdpServerRouter.  Only one address
       is specified."
     DEFVAL { 'c0a80001'h }  -- 192.168.0.1
    ::= { cabhCdpServer 13 }

cabhCdpServerSyslogAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "The Type of IP Address of the LAN-Trans SYSLOG servers."
     DEFVAL { ipv4 }
    ::= { cabhCdpServer 14 }

cabhCdpServerSyslogAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "The IP Addresses of the LAN-Trans SYSLOG servers.
       As a default there are no SYSLOG Servers.
       The factory defaults contains the indication of
       no Syslog Server value equals (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
            "Option value 15 - Domain name of LAN-Trans address realm."
     DEFVAL {""}
     ::= { cabhCdpServer 16 }

cabhCdpServerTTL OBJECT-TYPE
     SYNTAX      INTEGER (0..255)
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Option value 23 - LAN-Trans Time to Live."
     DEFVAL  { 64 }
     ::= { cabhCdpServer 17 }

cabhCdpServerInterfaceMTU   OBJECT-TYPE
     SYNTAX      INTEGER (68..4096)
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Option value 26 - LAN-Trans Interface MTU."
     ::= { cabhCdpServer 18 }

cabhCdpServerVendorSpecific  OBJECT-TYPE
     SYNTAX      OCTET STRING (SIZE(0..255))
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Option value 43 - Vendor Specific Options."
     DEFVAL  { ''h }
     ::= { cabhCdpServer 19 }

cabhCdpServerLeaseTime  OBJECT-TYPE
     SYNTAX      Unsigned32
     UNITS    "seconds"
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
      "Option value 51 – Lease Time for LAN IP Devices in the LAN-Trans realm
(seconds)."
DEFVAL  { 3600 }

     ::= { cabhCdpServer 20 }

cabhCdpServerDhcpAddressType OBJECT-TYPE
     SYNTAX      InetAddressType
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Option value 54 - Type of LAN-Trans DHCP server IP address."
     DEFVAL { ipv4 }
     ::= { cabhCdpServer 21 }

cabhCdpServerDhcpAddress    OBJECT-TYPE
     SYNTAX      InetAddress
     MAX-ACCESS  read-write
    STATUS      current
```

```
    DESCRIPTION
            "Option value 54 - LAN-Trans DHCP server IP
            address. It defaults to the router address as
            specified in cabhCdpServerRouter.  Alternatively
            a vendor may want to separate CDS address from
            router address."
     DEFVAL { 'c0a80001'h }       --   192.168.0.1
     ::= { cabhCdpServer 22 }


--
-- Notification group is for future extension.
--

cabhCdpNotification OBJECT IDENTIFIER ::= { cabhCdpMib 2 0 }
cabhCdpConformance  OBJECT IDENTIFIER ::= { cabhCdpMib 3 }
cabhCdpCompliances  OBJECT IDENTIFIER ::= { cabhCdpConformance 1 }
cabhCdpGroups       OBJECT IDENTIFIER ::= { cabhCdpConformance 2 }

--
--    Notification Group
--


-- compliance statements

cabhCdpBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
            "The compliance statement for devices that implement
             MTA feature."
    MODULE   --cabhCdpMib




-- unconditionally mandatory groups

    MANDATORY-GROUPS {
            cabhCdpGroup
    }

::= { cabhCdpCompliances 3 }


cabhCdpGroup  OBJECT-GROUP

  OBJECTS {

cabhCdpSetToFactory,
cabhCdpLanTransCurCount,
cabhCdpLanTransThreshold,
cabhCdpLanTransAction,
cabhCdpWanDataIpAddrCount,

cabhCdpLanAddrClientID,
cabhCdpLanAddrLeaseCreateTime,
cabhCdpLanAddrLeaseExpireTime,
cabhCdpLanAddrMethod,
cabhCdpLanAddrHostName,
cabhCdpLanAddrRowStatus,
```

```
cabhCdpWanDataAddrClientId,
cabhCdpWanDataAddrIp,
cabhCdpWanDataAddrRenewalTime,
cabhCdpWanDataAddrRowStatus,

cabhCdpWanDataAddrDnsRowStatus,

cabhCdpLanPoolStartType,
cabhCdpLanPoolStart,
cabhCdpLanPoolEndType,
cabhCdpLanPoolEnd,
cabhCdpServerNetworkNumberType,
cabhCdpServerNetworkNumber,
cabhCdpServerSubnetMaskType,
cabhCdpServerSubnetMask,
cabhCdpServerTimeOffset,


cabhCdpServerRouterType,
cabhCdpServerRouter,
cabhCdpServerDnsAddressType,
cabhCdpServerDnsAddress,
cabhCdpServerSyslogAddressType,
cabhCdpServerSyslogAddress,
cabhCdpServerDomainName,
cabhCdpServerTTL,
cabhCdpServerInterfaceMTU,
cabhCdpServerVendorSpecific,
cabhCdpServerLeaseTime,
cabhCdpServerDhcpAddressType,
cabhCdpServerDhcpAddress
       }
    STATUS    current
    DESCRIPTION
        "Group of objects for Cable CDP MIB."
    ::= { cabhCdpGroups 1 }



END
```

E.6 Portal de dirección del cable

La MIB de CAP DEBE implementarse como se define a continuación.

```
CABH-CAP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
      Unsigned32
          FROM SNMPv2-SMI
      TimeStamp,
      TruthValue,
      RowStatus,
      PhysAddress
          FROM SNMPv2-TC
    OBJECT-GROUP,
    MODULE-COMPLIANCE   FROM SNMPv2-CONF
    InetAddressType,
    InetAddress,
    InetAddressIPv4,
    InetAddressIPv6          FROM INET-ADDRESS-MIB
    clabProjCableHome
          FROM CLAB-DEF-MIB;
```

```
--============================================================================
--
--   History:
--
--   Date Modified by   Reason
--
--============================================================================

cabhCapMib MODULE-IDENTITY
    LAST-UPDATED    "0209200000Z" --September 20, 2002
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
          400 Centennial Parkway
          Louisville, Colorado 80027-1266
                U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
           "This MIB module supplies the basic management objects for the Cable
           Address Portal (CAP) portion of the PS database."


    ::=  { clabProjCableHome 3 }

-- Textual conventions

CabhCapPacketMode ::= TEXTUAL-CONVENTION
     STATUS   current
     DESCRIPTION
       "The data type established when
       a binding/mapping is established."
     SYNTAX   INTEGER {
          napt   (1),    -- NAT with port translation
          nat  (2), -- Basic NAT
          passthrough   (3)  -- Pass Through External Address
          }


cabhCapObjects      OBJECT IDENTIFIER ::= { cabhCapMib 1 }
cabhCapBase         OBJECT IDENTIFIER ::= { cabhCapObjects 1 }
cabhCapMap           OBJECT IDENTIFIER ::= { cabhCapObjects 2 }


--============================================================================
--
--   General CAP Parameters
--
--============================================================================

cabhCapTcpTimeWait OBJECT-TYPE
    SYNTAX Unsigned32
    UNITS "seconds"
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
            "This object is the maximum inactivity time to wait before assuming
            TCP session is terminated. It has no relation to the TCP session
            TIME_WAIT state referred to in [RFC 793]."
    DEFVAL { 300 }
    ::= { cabhCapBase 1 }
```

```
cabhCapUdpTimeWait OBJECT-TYPE
     SYNTAX      Unsigned32
     UNITS    "seconds"
     MAX-ACCESS  read-write
     STATUS      current
     DESCRIPTION
            "The inactivity time to wait before destroying
            CAP mappings for UDP."
     DEFVAL { 300 }  -- 5 minutes
     ::={ cabhCapBase 2 }

cabhCapIcmpTimeWait OBJECT-TYPE
     SYNTAX      Unsigned32
     UNITS "seconds"
     MAX-ACCESS read-write
     STATUS current
     DESCRIPTION
            "The inactivty time to wait before destroying
            CAP mappings for ICMP."
     DEFVAL { 300 }  --  5 minutes
     ::= { cabhCapBase 3 }


cabhCapPrimaryMode OBJECT-TYPE
    SYNTAX   CabhCapPacketMode
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Primary Packet Handling Mode to be used."
    DEFVAL { napt }
    ::= { cabhCapBase 4 }

cabhCapSetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Setting this object to true(1) causes all the tables in the CAP
            to be cleared, and all CAP objects with defaults to be reset back to
            their default values.

         The objects to set to factory default values when this object is set to
'true' are listed below:
         cabhCapTcpTimeWait,
         cabhCapUdpTimeWait,
         cabhCapIcmpTimeWait,
         cabhCapPrimaryMode,
         cabhCapMappingWanAddrType,
         cabhCapMappingWanPort,
         cabhCapMappingLanAddrType,
         cabhCapMappingLanPort"
    ::= { cabhCapBase 5 }


--================================================================================
--
--   cabhCapMappingTable (CAP Mapping Table)
--
--   The cabhCapMappingTable contains the mappings for all CAP mappings.
--
--================================================================================
```

```
cabhCapMappingTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCapMappingEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains IP address mapping for all CAP mappings."
    ::= {  cabhCapMap 1 }

cabhCapMappingEntry OBJECT-TYPE
    SYNTAX      CabhCapMappingEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "List of CAP IP mappings."
    INDEX { cabhCapMappingIndex }
    ::= { cabhCapMappingTable 1 }

     CabhCapMappingEntry ::= SEQUENCE {
     cabhCapMappingWanAddrType        InetAddressType,
     cabhCapMappingIndex              INTEGER,
     cabhCapMappingWanAddr            InetAddress,
     cabhCapMappingWanPort            INTEGER,
     cabhCapMappingLanAddrType        InetAddressType,
     cabhCapMappingLanAddr            InetAddress,
     cabhCapMappingLanPort            INTEGER,
     cabhCapMappingMethod             INTEGER,
     cabhCapMappingProtocol           INTEGER,
     cabhCapMappingRowStatus          RowStatus
     }


cabhCapMappingIndex    OBJECT-TYPE
    SYNTAX              INTEGER   (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "The Index into the CAP Mapping Table."
    ::= { cabhCapMappingEntry 1 }

cabhCapMappingWanAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The IP address type assigned on the WAN side. IP version 4 is
       typically used."
    DEFVAL { ipv4 }
    ::= { cabhCapMappingEntry 2 }

cabhCapMappingWanAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The IP address assigned on the WAN side.  IP version 4
       is typically used."
    ::= { cabhCapMappingEntry 3 }

cabhCapMappingWanPort OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The TCP/UDP port number on the WAN side."
```

```
        DEFVAL { 0 }
    ::= { cabhCapMappingEntry 4 }

cabhCapMappingLanAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The IP address type assigned on the LAN side.  IP version
        4 is typically used."
    DEFVAL { ipv4 }
    ::= { cabhCapMappingEntry 5 }

cabhCapMappingLanAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The IP address assigned on the LAN side.  IP version 4
       is typically used."
    ::= { cabhCapMappingEntry 6 }

cabhCapMappingLanPort OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The TCP/UDP port number on the LAN side."
    DEFVAL { 0 }
    ::= { cabhCapMappingEntry 7 }

cabhCapMappingMethod OBJECT-TYPE
    SYNTAX      INTEGER {
       static   (1),
       dynamic (2)
       }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Indicates how this mapping was created. Static means that it was
       provisioned, and dynamic means that it was handled by the PS itself."
    ::= { cabhCapMappingEntry 8 }

cabhCapMappingProtocol OBJECT-TYPE
    SYNTAX      INTEGER {
       other   (1), -- not specified
       icmp    (2),
       udp    (3),
       tcp    (4)
          }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The protocol for this mapping."
    ::= { cabhCapMappingEntry 9 }

cabhCapMappingRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
"The RowStatus interlock for the creation and deletion of a cabhCapMappingTable
entry. Changing the value of the IP address or port number columns of the CAP
Mapping Table may have an effect on active traffic, so the CMP will prevent
```

```
modification of this table's columns when the cabhCapMappingRowStatus object is
in the active state."
    ::={ cabhCapMappingEntry 10 }


--=========================================================================
--
--   cabhCapPassthroughTable (CAP Passthrough Table)
--
--   The cabhCapPassthroughTable contains the MAC Addresses for all LAN-IP
--   Devices which will be configured as passthrough.
--
--=========================================================================

cabhCapPassthroughTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCapPassthroughEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This table contains MAC addresses for LAN-IP Devices which are
        configured as passthrough mode."
    ::= {  cabhCapMap 2 }

cabhCapPassthroughEntry OBJECT-TYPE
    SYNTAX   CabhCapPassthroughEntry
    MAX-ACCESSnot-accessible
    STATUS   current
    DESCRIPTION
            "List of hardware addresses of LAN IP Devices which are configured
            for passthrough mode."
    INDEX {cabhCapPassthroughIndex}
::= {cabhCapPassthroughTable 1}

CabhCapPassthroughEntry::=SEQUENCE {
     cabhCapPassthroughIndex     INTEGER,
     cabhCapPassthroughMacAddr   PhysAddress,
     cabhCapPassthroughRowStatus RowStatus
     }

cabhCapPassthroughIndex     OBJECT-TYPE
    SYNTAX   INTEGER (1..65535)
    MAX-ACCESSnot-accessible
    STATUS   current
    DESCRIPTION
            "The index into the CAP Passthrough Table."
    ::= { cabhCapPassthroughEntry 1 }

cabhCapPassthroughMacAddr        OBJECT-TYPE
    SYNTAX   PhysAddress
    MAX-ACCESSread-create
    STATUS   current
    DESCRIPTION
            "Hardware address of the LAN-IP Device to be configured as
            passthrough mode."
    ::={cabhCapPassthroughEntry 2}

cabhCapPassthroughRowStatus OBJECT-TYPE
    SYNTAX   RowStatus
    MAX-ACCESSread-create
    STATUS    current
    DESCRIPTION
            "The RowStatus interlock for the creation and deletion of a
             cabhCapPassthroughTable entry.
             There are no restrictions on setting the read-create column of this
```

```
            table (i.e., cabhCapPassthroughMacAddr) when the status of
            cabhCapPassthroughRowStatus is active."
    ::= { cabhCapPassthroughEntry 3 }

--
-- Notification group is for future extension.
--

cabhCapNotification     OBJECT IDENTIFIER ::= { cabhCapMib 2 0 }
cabhCapConformance OBJECT IDENTIFIER ::= { cabhCapMib 3 }
cabhCapCompliances OBJECT IDENTIFIER ::= { cabhCapConformance 1 }
cabhCapGroups OBJECT IDENTIFIER ::= { cabhCapConformance 2 }

--
--    Notification Group
--


-- compliance statements

cabhCapBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
            "The compliance statement for devices that implement
             MTA feature."
    MODULE   --cabhCapMib




-- unconditionally mandatory groups

MANDATORY-GROUPS {
    cabhCapGroup
    }

::= { cabhCapCompliances 1 }


cabhCapGroup OBJECT-GROUP
    OBJECTS {
       cabhCapTcpTimeWait,
       cabhCapUdpTimeWait,
       cabhCapIcmpTimeWait,
       cabhCapPrimaryMode,
       cabhCapMappingWanAddrType,
       cabhCapMappingWanAddr,
       cabhCapMappingWanPort,
       cabhCapMappingLanAddrType,
       cabhCapMappingLanAddr,
       cabhCapMappingLanPort,
       cabhCapMappingMethod,
       cabhCapMappingProtocol,
       cabhCapMappingRowStatus,
       cabhCapPassthroughMacAddr,
       cabhCapPassthroughRowStatus
       }
    STATUS    current
    DESCRIPTION
        "Group of objects for CAP MIB."
    ::= { cabhCapGroups 1 }



END
```

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	**Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios**
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2005