UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T J.191

(07/2002)

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

Varios

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

Recomendación UIT-T J.191

RECOMENDACIONES UIT-T DE LA SERIE J

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

Recomendaciones generales	J.1–J.9
Especificaciones generales para transmisiones radiofónicas analógicas	J.10–J.19
Características de funcionamiento de los circuitos radiofónicos	J.20–J.29
Equipos y líneas utilizados para circuitos radiofónicos analógicos	J.30–J.39
Codificadores digitales para señales radiofónicas analógicas	J.40–J.49
Transmisión digital de señales radiofónicas	J.50–J.59
Circuitos para transmisiones de televisión analógica	J.60–J.69
Transmisiones de televisión analógica por líneas metálicas e interconexión con radioenlaces	J.70–J.79
Transmisión digital de señales de televisión	J.80–J.89
Servicios digitales auxiliares para transmisiones de televisión	J.90–J.99
Requisitos operacionales y métodos para transmisiones de televisión	J.100–J.109
Sistemas interactivos para distribución de televisión digital	J.110–J.129
Transporte de señales MPEG-2 por redes de transmisión de paquetes	J.130–J.139
Mediciones de la calidad de servicio	J.140–J.149
Distribución de televisión digital por redes locales de abonados	J.150–J.159
IPCablecom	J.160–J.179
Varios	**J.180–J.199**
Aplicación para televisión digital interactiva	J.200–J.209

Para más información, véase la Lista de Recomendaciones del UIT-T.

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 de Internet (IP) que pueden añadirse a los módems de cable 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, características adicionales de administración y prestación de los servicios y mejoras en el direccionamiento y en el tratamiento de los paquetes.

Orígenes

La Recomendación UIT-T J.191, preparada por la Comisión de Estudio 9 (2001-2004) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la AMNT el 29 de julio de 2002.

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.

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.

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 de Internet (IP) que pueden añadirse a los módems de cable 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, características adicionales de administración y prestación de los servicios y mejoras en el direccionamiento y en el tratamiento de los paquetes.

2 Referencias

2.1 Referencias normativas

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.

[UIT-T J.112] Recomendación UIT-T J.112 Anexo B (2001), *Especificaciones de interfaces de servicios de datos por cable: Especificación de la interfaz de radiofrecuencia*.

[UIT-T J.161] 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*.

[UIT-T J.163] Recomendación UIT-T J.163 (2001), *Calidad de servicio dinámica para la prestación de servicios en tiempo real por las redes de televisión por cable que utilizan módems de cable*.

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

[UIT-T X.509] 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 de atributos*.

[UIT-T X.690] 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*.

[FIPS 140-2] FIPS PVB 140-2 (2001), *Security Requirements for Cryptographic Modules*, *Department of commerce*, *NIST*.

[ISO/CEI 10038] ISO/CEI 10038 (ANSI/IEEE Std 802.1D):1993, *Information technology – Telecommunications and information exchange between systems – Local area networks – Media access control (MAC) bridges*.

[RFC 768] IETF RFC 768 (1980), *User Datagram Protocol*.

[RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol*.

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

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

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

[RFC 1122] IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication Layers*.

[RFC 1123] IETF RFC 1123 (1989), *Requirements for Internet Hosts – Application and Support*.

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

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

[RFC 1901] IETF RFC 1901 (1996), *Introduction to Community-based SNMPv2*.

[RFC 1905] IETF RFC 1905 (1996), *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*.

[RFC 1907] IETF RFC 1907 (1996), *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*.

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

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

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

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

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

[RFC 2349] IETF RFC 2349 (1998), *TFTP Time-out Interval and Transfer Size Options*.

[RFC 2570] IETF RFC 2570 (1999), *Introduction to Version 3 of the Internet-standard Network Management Framework*.

[RFC 2571] IETF RFC 2571 (1999), *An Architecture for Describing SNMP Management Frameworks*.

[RFC 2572] IETF RFC 2572 (1999), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*.

[RFC 2573] IETF RFC 2573 (1999), *SNMP Applications*.

[RFC 2574] IETF RFC 2574 (1999), *User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)*.

[RFC 2575] IETF RFC 2575 (1999), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

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

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

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

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

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

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

[RFC 2786] IETF RFC 2786 (2000), *USM Key Management Information Base and Textual Convention*.

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

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

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

2.2 Referencias informativas

[FIPS 186-2] FIPS PUB 186-2 (2000), *Digital Signature Standard*, *Department of commerce*, *NIST*.

[RFC 347] IETF RFC 347 (1972), *Echo Process*.

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

[DOCSIS2] *Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus*, draft-ietf-ipcdn-bpiplus-mib-01.txt (trabajo en curso).

draft-ietf-ipcdn-bpiplus-mib-06 INTERNET DRAFT – DOCSIS Baseline Privacy Plus MIB – *Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus*, Noviembre de 2001.

[ID-IGMP] FENNER (W.) et al., *IGMP-based Multicast Forwarding ("IGMP Proxying")*, IETF Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-magma-igmp-proxy-00.txt.

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 típico para instalarse 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, acrónimos y convenios

4.1 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes siglas.

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*)
CDS	Servidor DHCP del cable (*cable DHCP server*)
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 port 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 (*cableHome testing portal*)
CVC	Certificado de verificación de código
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*)
HA	Acceso a la vivienda (*home access*)
HEX	Hexadecimal
HFC	Híbrido fibra coaxial (*hybrid fiber 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 center*)
LAN-Pass	Dirección de transferencia de la LAN (*pass-through LAN address*)
LAN-Trans	Dirección traducida de la 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*)
MPLS	Conmutación por etiquetas multiprotocolo (*multiprotocol label switching*)
MSO	Operador de servicios múltiples (*multiple service operator*)
MTA	Adaptador de terminal multimedios (*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 Servicio de portal (*portal service*)

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*)

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

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 coordinadao (*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 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 Requisitos, arquitectura y presentación del lote de características basadas en el protocolo Internet

La presente Recomendación proporciona un conjunto de características basadas en el protocolo Internet que pueden añadirse a un módem de cable, 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 módems de cable dotados de estas características mejoradas reciben el nombre de módems de cable mejorados con IP (IPCM, *IP-enhanced cable modem),* y son implementaciones de la clase de dispositivo HA de J.190. Como explica la Rec. UIT-T J.190, la clase de dispositivos HA incluye tanto la funcionalidad de módem de cable como la funcionabilidad de servicios de portal.

Sus principales aspectos y características son los siguientes:

– *Gestión y prestación*
  - Gestión y configuración remotas del PS.
  - Apoderado de gestión sencilla para dispositivos IP con base en el hogar (por ejemplo, los PC).
  - Prestación sin intervención para el PS.

– *Direccionamiento y tratamiento de paquetes*
  - Traducción biunívoca de direcciones para los dispositivos del hogar.
  - Traducción de direcciones de uno a varios para los dispositivos del hogar.
  - Direccionamiento no traducido para los dispositivos del hogar.
  - Servidor DNS sencillo en el PS.

– *Calidad de servicio*
  - Funcionalidad de puenteo transparente para la mensajería de QoS IPCablecom enviada a las aplicaciones homologados con IPCablecom o recibidor de éstas.

– *Seguridad*
  - Autenticación del dispositivo PS.
  - Mensajes de gestión segura.
  - Descarga segura de ficheros de configuración y de soporte lógico.
  - QoS segura en el enlace HFC.

- Gestión remota de la barrera contra fuegos del PS.

5.1 Arquitectura

Véase la figura 1.

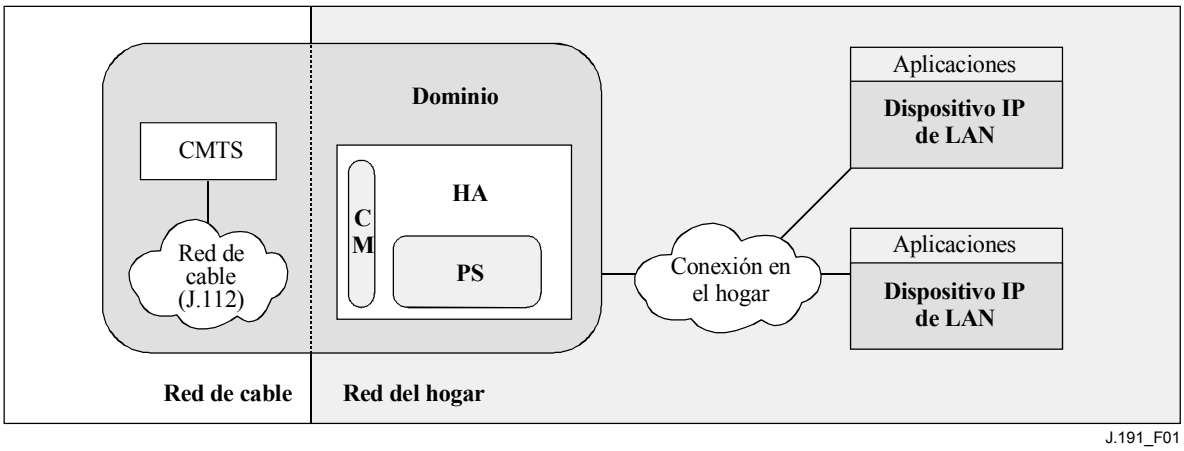


Figura 1/J.191 – Conceptos clave

5.1.1 Servicio de portal

El servicio de portal es el elemento lógico que proporciona al mismo tiempo la seguridad, la gestión, la prestación y los servicios de direccionamiento locales. Se definen tres conjuntos de funciones del servicio 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.

5.1.2 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 2).

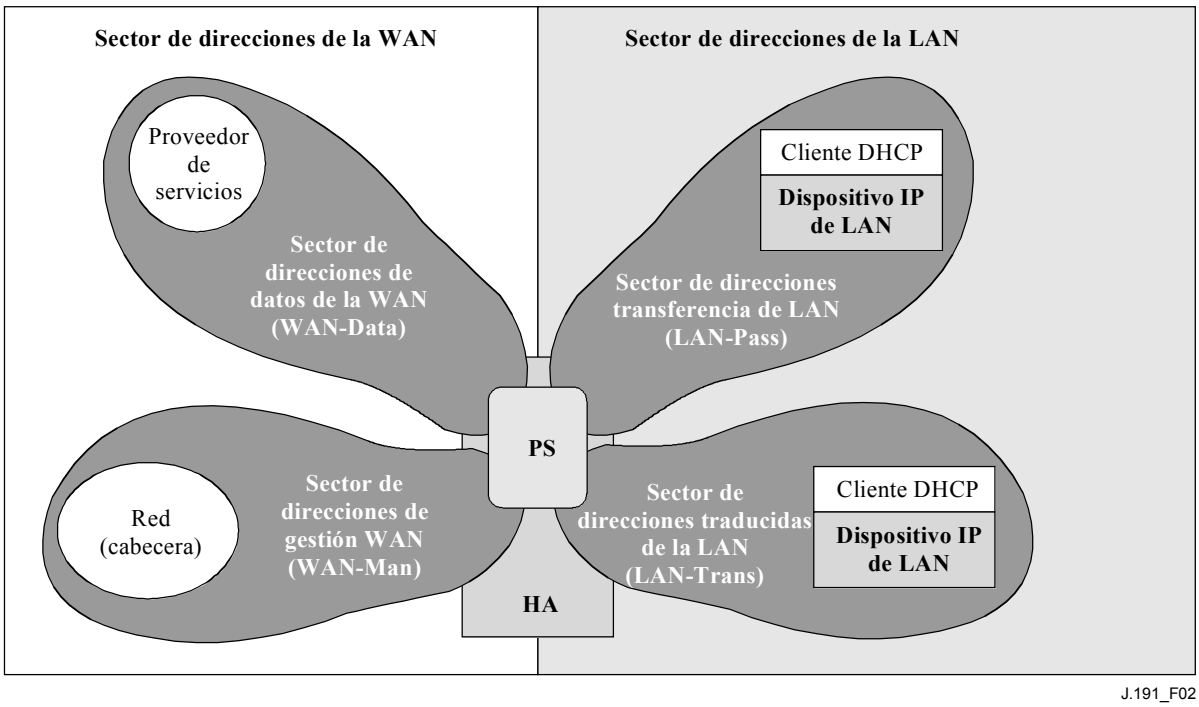


Figura 2/J.191 – Sector de direcciones

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 del hogar entre los dispositivos IP de LAN y el 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 el enlace del hogar, 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).

5.2 Funciones de gestión

Para dar soporte a la prestación 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 de servicio.

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 de servicio se encuentran en el elemento lógico PS del módem de cable, 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 3 muestra ejemplos de las funciones de gestión cliente, servidor y PS de los cuadros 1, 2 y 3.

Cuadro 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 DNS de cabecera	El servidor DNS de cabecera es un componente interno destinado a traducir los nombres de dominio ASCII a direcciones IP.
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 2/J.191 – Descripción de las funciones PS de gestión y prestación

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 la cabecera 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 para iniciar en remoto pings y bucles dentro de la LAN.

Cuadro 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 prestación 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.

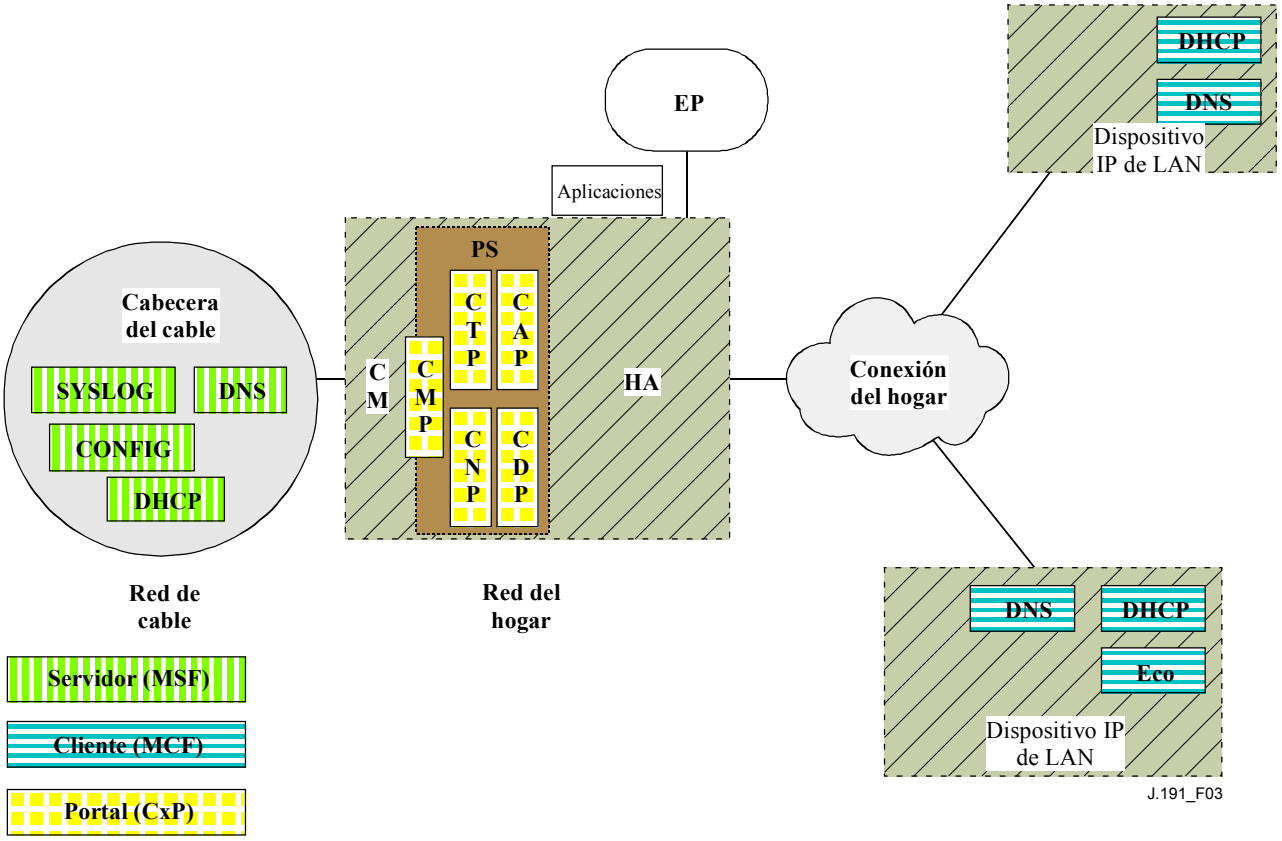


Figura 3/J.191 – Relaciones de gestión cliente-servidor

5.3 Funciones de seguridad

Las funciones de seguridad se clasifican en funciones de seguridad del portal y funciones de seguridad del servidor. La relación entre los distintos elementos de seguridad y su clasificación como funciones de servidor o de portal se muestra en la figura 4 y se describe en los cuadros 4 y 5.

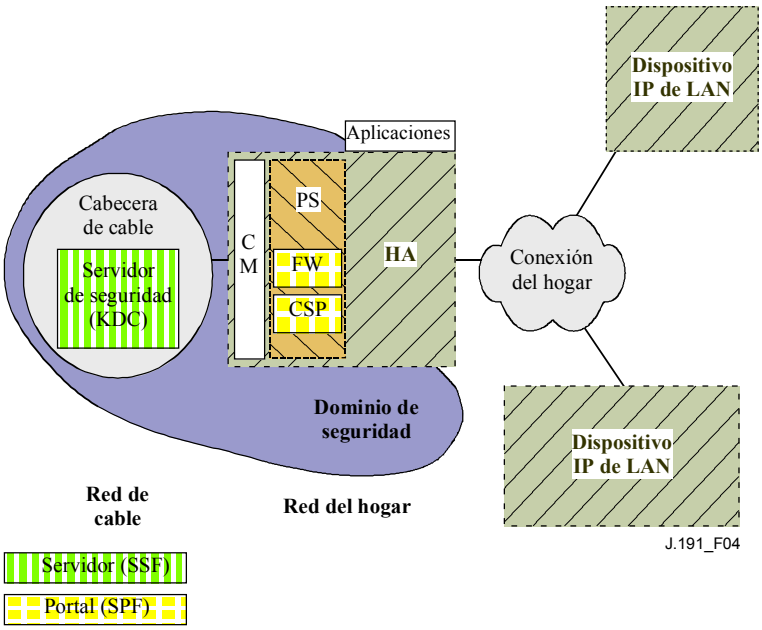


Figura 4/J.191 – Elementos de seguridad

Cuadro 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 comporta como un portal en lo relativo al material de seguridad para todas las demás funciones de seguridad del PS. El CSP se comunica en el lado WAN con un servidor de seguridad (centro de distribución de claves (KDC, *key distribution center*)).
Barrera contra fuegos (FW, *firewall*)	La barrera contra fuegos proporciona la protección del entorno IP del hogar contra ataques malintencionados.

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

Función servidor de seguridad	Descripción
KDC	Los servidores KDC de la cabecera proporcionan los servicios de autenticación y la distribución de claves para el hogar, comunicándose con la función CSP para establecer estos servicios.

5.4 Funciones QoS

La arquitectura QoS se compone de una sola entidad funcional basada en el PS denominada portal QoS del cable (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.

5.5 Modelo de la interfaz de mensajería

La comunicación entre las funciones de los elementos de red 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.

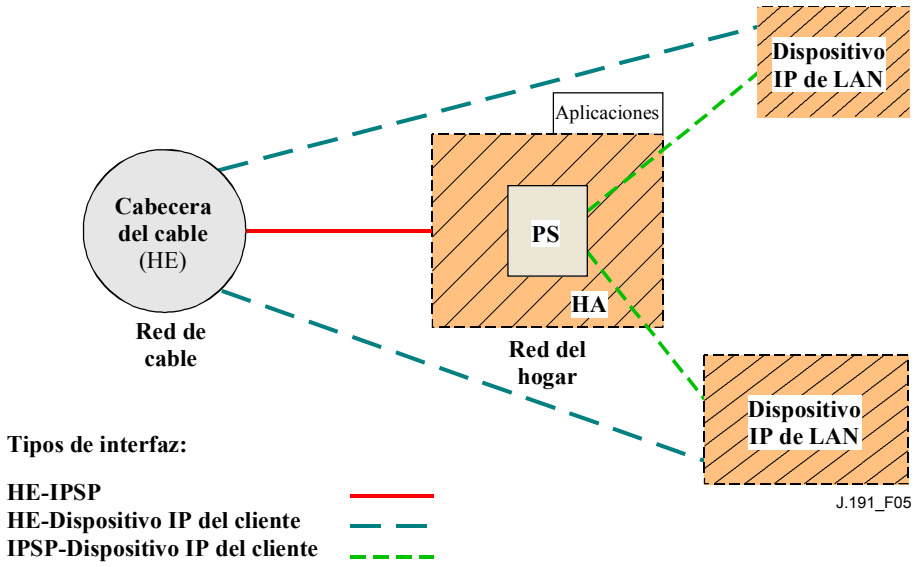


Figura 5/J.191 – Interfaces de referencia

Las interfaces de mensajería se resumen en el cuadro 6.

Cuadro 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	Sin especificar
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

5.6 Modelo de referencia de información

El funcionamiento del modelo de gestión se basa en la información almacenada en el portal por las diversas funciones del portal (CAP, CDP, CMP, etc.). Dichas funciones deben poder interactuar a través del intercambio de información, representando la base de datos del portal una entidad conceptual que almacena esta información. La base de datos del portal 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 6 muestra la relación entre la base de datos y las funciones del portal, el cuadro 7 describe la información que suele asociarse a cada una de estas funciones. La figura 7 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.

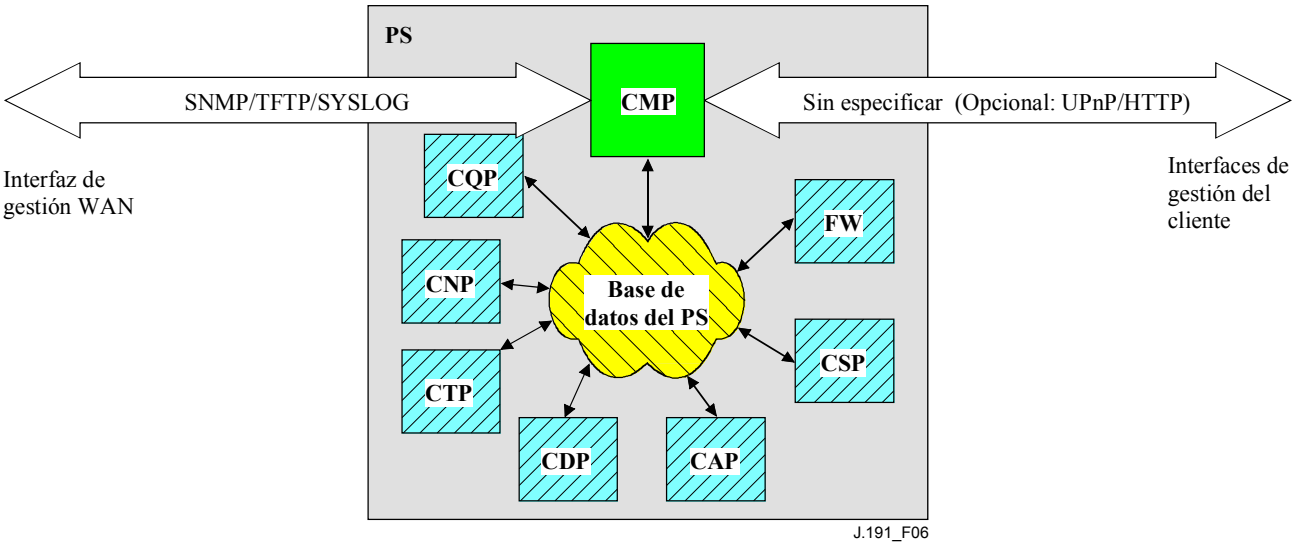


Figura 6/J.191 – Relación entre las funciones del portal y la base de datos del portal

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

Cuadro 7/J.191 – Ejemplos característicos de la información de la base de datos del portal

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
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

Cuadro 7/J.191 – Ejemplos característicos de la información de la base de datos del portal

Nombre	Utilización (en general)
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

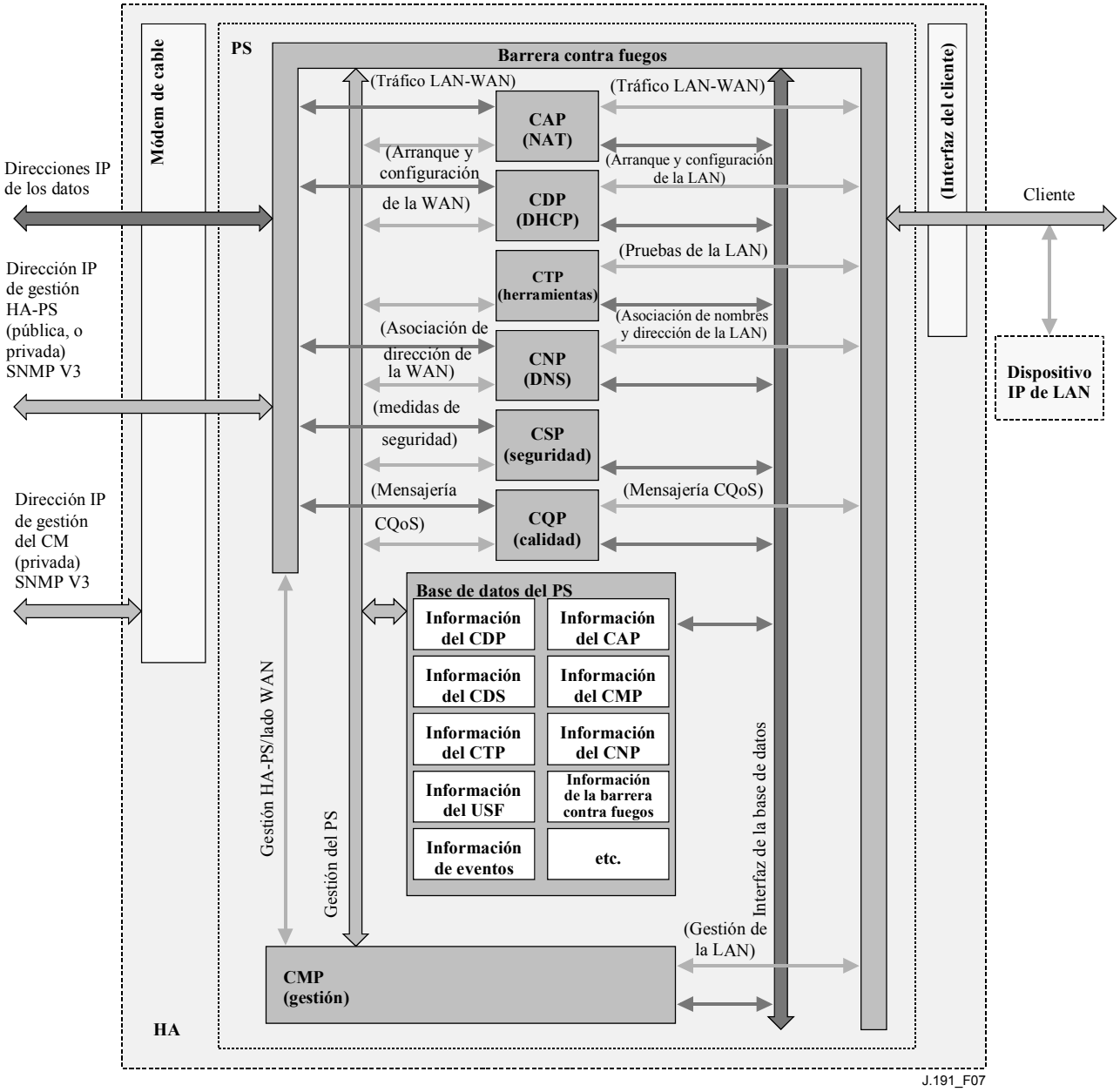


Figura 7/J.191 – Ejemplo detallado de implementación de la base de datos del portal

El portal 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 portal. La gestión tiene por objeto la inicialización y prestación de los elementos de la red del lado WAN por una parte, y de los diagnósticos y estado del lado 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 CNP sólo responde a las consultas de DNS en el sector LAN-Trans.

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 PORTAL 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 portal. 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.

La barrera contra fuegos es específica de la implementación pero la presente Recomendación no expone en detalle la implementación de la barrera contra fuegos.

5.7 Modelos operacionales

Esta infraestructura mejorada se construye sobre una infraestructura de módem de cable proporcionando servicios adicionales e incorporando capacidades semejantes a las de los sistemas de prestación IPCablecom.

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

- El modo de prestación DHCP.
- El modo de prestación SNMP.

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

- Modo NmAccess.
- Modo de coexistencia.

La figura 8 muestra los diversos modos operacionales del PS junto con los activadores asociados a cada de uno de ellos.

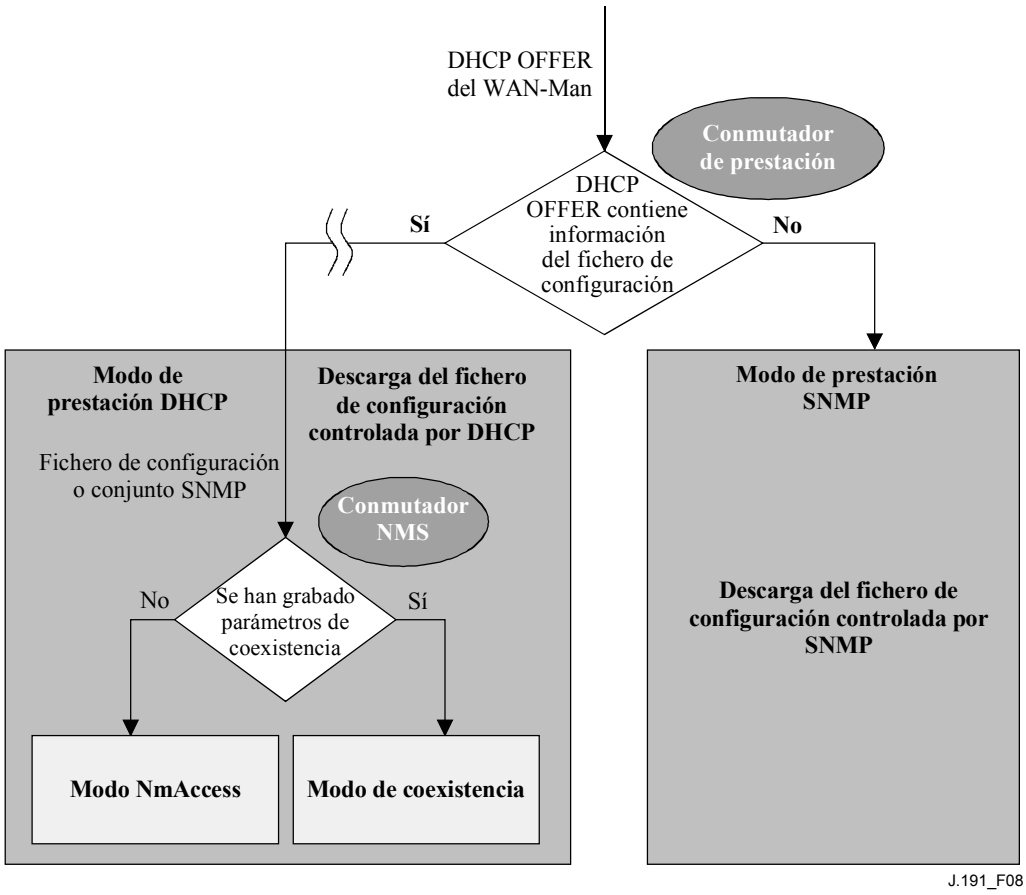


Figura 8/J.191 – Modos operacionales del portal

Si la información del fichero de configuración del portal (ubicación del servidor y nombre del fichero) se suministra al portal en el DHCP OFFER emitido por el servidor DHCP de la red de cable, el portal funcionará en el modo de prestación DHCP. Cuando se encuentre en el modo de prestación DHCP, el portal podrá funcionar en uno de los dos modos de gestión de red (el NmAccess y la coexistencia). En el modo de prestación DHCP, el portal 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 la información del fichero de configuración del portal no se suministra a éste en el DHCP OFFER emitido por el servidor DHCP de la red de cable, el portal funcionará en el modo de prestación SNMP. Cuando funcione en dicho modo, la información y los activadores de descarga del fichero de configuración del portal los suministrará el NMS por medio de mensaje SNMP. A diferencia del modo de prestación DHCP, en este modo no se modifica el comportamiento de la gestión de la red.

El cuadro 8 muestra las capacidades afectadas por cada de uno de los modos operacionales descritos anteriormente.

Cuadro 8/J.191 – Infraestructuras de portal

Modo	Capacidad directamente afectada
Modo de prestación SNMP	Descarga del fichero de configuración
Modo de prestación DHCP	Descarga del fichero de configuración
Modo de prestación DHCP: Modo NmAccess	Versión de SNMP utilizada entre el NMS y el PS
Modo de prestación DHCP: modo de coexistencia	Versión de SNMP utilizada entre el NMS y el PS

Los distintos modos operacionales tienen por objeto contemplar una diversidad de infraestructuras desde el punto de vista del servidor interno, y entre ellas varias versiones SNMP y diversos tipos de servidores de seguridad. Esta información se expone más detalladamente en 13.1 a 13.3.

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 portal de servicio 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 PS 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 implementan el conjunto de protocolos Internet (IP, *Internet protocol*).
- Para el intercambio de mensajes de gestión entre el NMS de la red de cable y el portal de servicio IP en el módem de cable se utiliza SNMP. El SNMP permite observar al NMS las interfaces del portal, mediante el acceso a datos internos del portal, a través de las MIB necesarias.
- Se puede utilizar SNMPv1/v2c/v3 como protocolo de gestión entre el NMS y el servicio 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 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 9 contiene las directrices del diseño del sistema de herramientas de gestión. Esta relación sirve de orientación para el desarrollo de las especificaciones de las herramientas de gestión.

Cuadro 9/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 del PS.
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 remoto 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 9, 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 servidor 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.

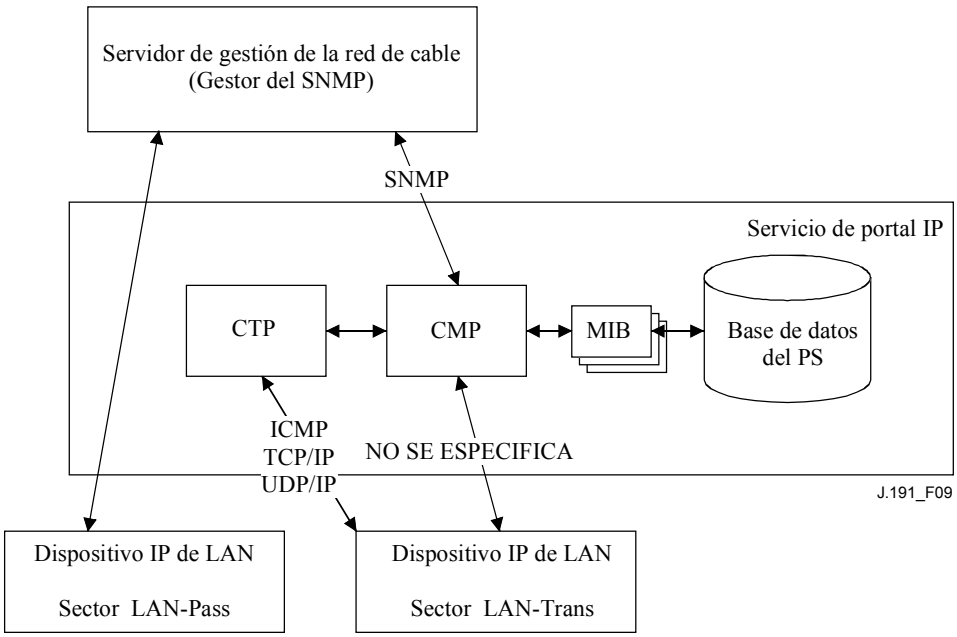


Figura 9/J.191 – Arquitectura de gestión

Los elementos funcionales CMP y CTP se encuentran en el interior del PS.

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. Se accede a los objetos docsDevSoftware 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. Esto no impide la utilización de un único agente SNMP.

El elemento PS soporta los protocolos SNMPv1, SNMPv2c y SNMPv3. En la cláusula 5.7 se presenta los dos modos de prestación soportados por un elemento PS, y la cláusula 7 contiene detalles adicionales de estos modos. El modo de prestación 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 la observación y actualización de la información de configuración del portal de dirección del cable (CAP).
- Permitir la visualización y actualización de la información de configuración de la barrera contra fuegos.
- Permitir el ping remoto para los dispositivos IP de LAN del sector de direcciones LAN-Trans, a través del portal de pruebas 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 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 10 contiene las directrices de diseño del CMP. Esta relación sirvió de orientación para la especificación de la funcionalidad CMP.

Cuadro 10/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 el hogar.
CMP 2	La desconexión entre el proveedor, o proveedores, de servicios de ancha banda y el dispositivo mejorado en IP no desactivará ni degradará el funcionamiento de otras funciones internas del hogar.
CMP 3	El PS se recuperará automáticamente tras un corte de corriente, debiendo volver los dispositivos conectados al PS al estado operacional en que se encontraban antes del corte.
CMP 4	Los dispositivos 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.

De acuerdo con lo expuesto en 5.7, cuando se encuentra en el modo de prestación SNMP, el PS:

1) opera utilizando el protocolo SNMPv3;
2) soporta USM y VACM; y
3) utiliza Kerberos para la distribución del material de claves.

De acuerdo con lo expuesto en 5.7, cuando se encuentra en el modo de prestación DHCP, el PS puede funcionar en uno de los otros dos modos de gestión de red, el modo de NmAccessTable y el modo de coexistencia. En el modo de NmAccessTable, el acceso de gestión viene controlado por el NmAccessTable de [RFC 2669], soportándose los protocolos SNMPv1/v2c. En el modo de coexistencia, el acceso de la gestión se controla de acuerdo con lo descrito en [RFC 2576] soportándose los protocolos SNMPv1/v2c/v3, permitiéndose USM y VACM y distribuyéndose el material de claves SNMPv3 de acuerdo con [RFC 2786] y TLV en el fichero de configuración del PS.

El cuadro 11 contiene las definiciones de los términos específicos del CMP.

Cuadro 11/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 [RFC 2574, sección 2.1], 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 [RFC 2575, sección 2.4].
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. La autorización final PUEDE conmutarse entre un usuario del NMS de la red de cable y un usuario del hogar pero NO DEBERÍA residir en ambos. 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 10 muestra tres interfaces de mensajería de gestión posibles:

- 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).
- 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).
- 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.

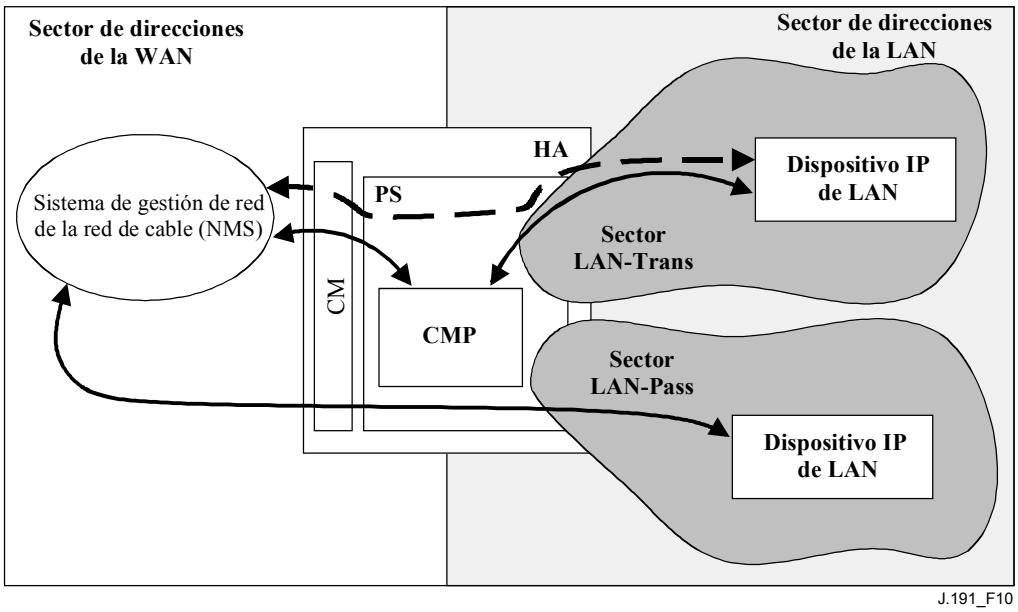


Figura 10/J.191 – Interfaces de los mensajes de gestión

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 11 muestra un ejemplo de implementación del CNP para ilustrar los conceptos de la funcionalidad CMP.

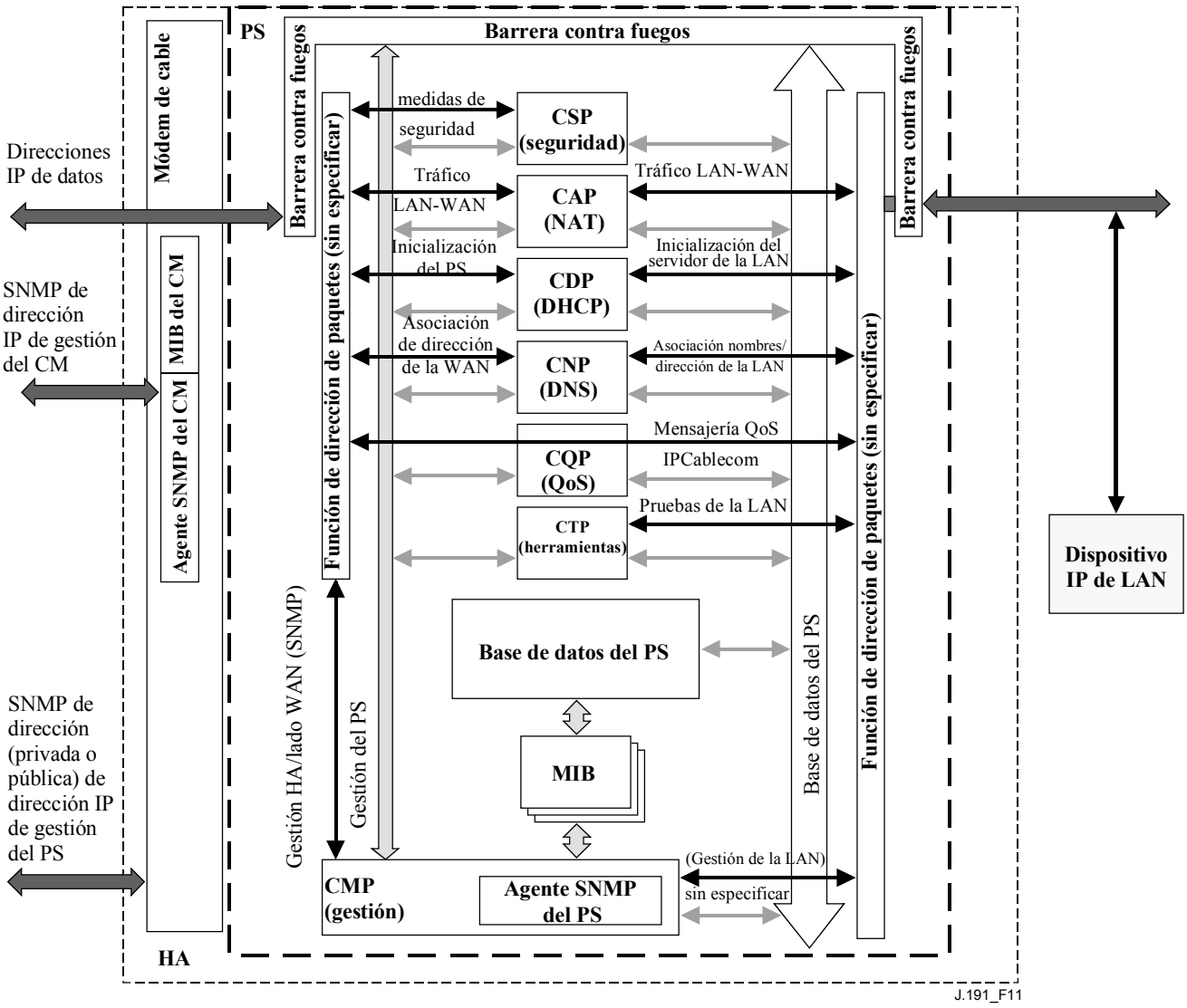


Figura 11/J.191 – Diagramas de bloque del PS

Las herramientas de gestión del NMS utilizan el SNMP para acceder a objetos del PS y gestionarlos. 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 agente SNMP del PS 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 CMP DEBE proporcionar control de gestión a la WAN mediante SNMPv3 [RFC 2571, RFC 2572].

El CMP DEBE implementar ICMP [RFC 792] y contestar a las peticiones de eco del ICMP procedentes del NMS.

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

El CMP DEBE poder otorgar autorización final o bien al administrador de la LAN o bien al administrador de la WAN de cable (administrador del PS).

El valor por defecto de la autorización final DEBE ser administrador WAN. El valor de la autorización final PUEDE ser alterado por acceso del SNMP o por un fichero de configuración.

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

El objeto sysDescr del grupo de sistemas MIB-2 (MIB-2 1 [RFC 1907] DEBE implementarse y DEBE conservarse en las reactivaciones de los dispositivos y en los ciclos de alimentación.

El sysDescr DEBE contener cinco campos en el orden específico siguiente: HW_REV: hardware_version; VENDOR: vendor_name; BOOTR: Boot_ROM_version; SW_REV: Software_version; Model: Model_number.

El sysDescr se compone de cinco pares tipo/valor. El tipo y el valor vienen separados por el carácter ":" seguido de un espacio en blanco. Un par tipo/valor y el siguiente vienen separados por un símbolo ";" seguido de un espacio en blanco. El conjunto de los cincos pares del SysDescr necesarios DEBE venir encerrado entre ángulos dobles. Por ejemplo, un sysDescr para PS del fabricante XYZ, versión 5.2 de equipo físico, ROM de arranque versión 1.4, versión de soporte lógico (SW) 2.2 y número de modelo ABC DEBE presentarse del siguiente modo:

> cualquier texto «HW_REV: 5.2; VENDOR: XYZ; BOOTR: 1.4; SW_REV: 2.2; MODEL: ABC» cualquier texto

El PS necesita comunicar toda la información necesaria, mediante los campos de sysDescr, para poder determinar a qué versión de soporte lógico puede actualizarse el PS. Si alguno de los campos del sysDescr necesarios no fuera aplicable, el SysDescr DEBE contener el valor "NONE". Por ejemplo, un PS sin BOOTR indicará BOOTR: NONE.

El objeto sysObjectID del grupo del sistema MIB-2 [RFC 1907] 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 1907] 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 1907] 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 1907] DEBE implementarse y DEBE conservarse en las reactivaciones de dispositivos y ciclos de alimentación.

El objeto sysServices del grupo de sistema MIB-2 [RFC 1907] 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 1907] 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.

El grupo SNMP de MIB-2 [RFC 1907] DEBE implementarse.

El objeto snmpSetSerialNo del grupo snmpSet [RFC 1907] 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.

6.3.5 Requisitos del protocolo SNMP

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

- Un protocolo de gestión de red simple [RFC 1157].
- Introducción al SNMPv2 orientado a comunidades [RFC 1901].
- Operaciones de protocolo para SNMPv2 [RFC 1905].
- Correspondencias de transporte para SNMPv2 [RFC 1906].
- Base de información de gestión para la versión 2 del protocolo de gestión de red simple (SNMPv2) [RFC 1907].
- Introducción al SNMPv3 [RFC 2570].
- MIB en el marco SNMP [RFC 2571].
- Proceso y despacho de mensajes para SNMP [RFC 2572].
- MIB de aplicaciones SNMP [RFC 2573].
- Grupo de SNMP MIBUSM [RFC 2574].
- Grupo de SNMP MIBVACM [RFC 2575].
- MIB de comunidades SNMP [RFC 2576].
- SNMPv2-CONF.

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

- Estructura de la información gestionada versión 2 (SMIv2) [RFC 2578].
- Convenios textuales para el SMIv2 [RFC 2579].
- Declaraciones de conformidad para SMIv2 [RFC 2580].

6.3.6 Requisitos del modo de gestión de red

En esta cláusula se describen reglas aplicables a los modos de gestión de red que el PS debe soportar. La cláusula 6.3.6.1 y sus subcláusulas describen los modos de gestión de red para un PS que funcione en el modo de prestación DHCP. La cláusula 6.3.6.2 y sus subcláusulas describen los modos de gestión de red para un PS que funcione en el modo de prestación SNMP.

6.3.6.1 Modo NmAccessTable y modo de coexistencia para un PS funcionando en el modo de prestación DHCP

El PS DEBE soportar la coexistencia entre SNMPv1, SNMPv2c, y SNMPv3 y SNMP de acuerdo con lo expuesto en [RFC 2571] a [RFC 2576]. El PS DEBE asimismo soportar el modo NmAccessTable definido por [RFC 2669]. El soporte de modos de gestión de red para un PS que funciona en el modo de prestación DHCP se rige por las siguientes directrices:

6.3.6.1.1 Principios de funcionamiento de un PS funcionando en el modo de prestación DHCP

a) Tras la recepción de un DHCP ACK, un PS que funcione en el modo de prestación DHCP [indicado por el valor '1' de cabhPsDevProvMode (DHCPmode)] DEBE funcionar del siguiente modo:

- Se permite el acceso de sólo lectura SNMPv1/v2c a todas las variables de la MIB que necesiten observarse durante el funcionamiento SNMPv1/v2c. No se permite el acceso desde la WAN para evitar el acceso de gestión no autorizado antes de que el PS quede configurado por el fichero de configuración del PS.
- Se aceptan los paquetes de SNMPv1/v2c que contengan cadenas de la comunidad.
- Se ignoran todos los paquetes SNMPv3.
- DEBERÍA prohibirse el acceso a las variables MIB que permitieran la determinación de la dirección IP WAN-Man del PS, como la IpAddrTable de la MIB-2.
- No son accesibles ninguna de las SNMPv3 MIB (la MIB de comunidad, la TARGET-MIB, la VACM-MIB, la USM-MIB, ni la NOTIFICATION-MIB) salvo que se establezca en el fichero de configuración del PS.
- No se puede acceder a ninguno de los elementos SNMP-USM-DH-OBJECTS-MIB salvo que se establezca lo contrario en el fichero de configuración del PS.
- El proceso de todos los elementos MIB del fichero de configuración del PS DEBE llevarse a buen fin antes de que comience el cálculo de los valores públicos del cuadro USMDHKickstart.

b) Si el PS está funcionando en el modo de prestación 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.

c) Tras completar el proceso de prestación 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.

Modo NmAccess (utilizando el cuadro docsDevNmAccess) con SNMPv1/v2c:

- Sólo se procesan los paquetes SNMPv1/v2c.
- Se ignoran los paquetes SNMPv3.
- docsDevNmAccessTable controla el acceso y los destinos de las trampas descritos [RFC 2669].
- No se puede acceder a ninguna de las SNMPv3 MIB (la MIB comunidad, ni la TARGET-MIB, ni la VACM-MIB, ni la USM-MIB, ni la NOTIFICATION-MIB).

Modo de coexistencia utilizando SNMPv1/v2c/v3

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 2571] y [RFC 2576].
- 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.
- 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).

6.3.6.1.2 Inicialización del SNMPv3 en modo de coexistencia y modificaciones de clave

Cuando se encuentra en el modo de coexistencia, el PS DEBE soportar los requisitos de "inicialización SNMPv3" y "modificaciones de claves DH" especificados en las cláusulas siguientes.

6.3.6.1.2.1 Inicialización del SNMPv3

Para cada uno de los distintos nombres de seguridad, de los que habrá cinco como máximo, el administrador del PS generará un par de números. En primer lugar, el administrador del PS generará un número aleatorio Rm.

Acto seguido, el administrador del IPcable2Home 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 un parámetro del conjunto Diffie-Hellman y p el primo de dichos parámetros.

El fichero de configuración del PS se crea para introducir el par (número de seguridad, número público). El PS DEBE soportar cinco pares como mínimo. Por ejemplo:

TLV tipo 34.1 (Nombre de seguridad de arranque del SNMPv3) = Administrador del PS.

TLV tipo 34.2 (Número de seguridad de arranque del SNMPv3) = z.

El PS DEBE soportar las entradas VACM definidas en 6.3.6.4. Sólo estarán (DEBEN ESTAR) activas las entradas especificadas por el nombre de seguridad correspondiente en el fichero de configuración del PS.

Durante el proceso de arranque del PS, los anteriores valores (nombre de seguridad, número público) DEBEN rellenarse en usmDHKickstartTable.

En este momento:

usmDHKickstartMgrpublic.1 = "z" (cadena de octetos);

usmDHKickstartSecurityName.1 = "PS Administrator".

Cuando se otorga un valor válido a usmDHKickstartMgrpublic.n durante el registro, se crea la fila correspondiente en usmUserTable con los siguientes valores:

usmUserEngineID: localEngineID;

usmUserName: usmDHKickstartSecurityName.n value;

usmuserSecurityName: usmDHKickstartSecurityName.n value;

usmUserCloneFrom: ZeroDotZero;

usmUserAuthProtocol: usmHMACMD5AuthProtocol;

usmuserAuthKeyChange: (derivado del valor establecido);

usmUserOwnAuthKeyChange: (derivado del valor establecido);

usmUserPrivProtocol: usmDESPrivProtocol;

usmUserPrivKeyChange: (derivado del valor establecido);

usmUserOwnPrivKeyChange: (derivado del valor establecido;

usmUserPublic;

usmUserStorageType: permanent;

usmUserStatus: activo.

NOTA – En lo que se refiere a las entradas dhKickstart (PS) de usmUserTable, permanente quiere decir que DEBEN escribirse pero no suprimirse y que no se salvan en los rearranques.

Una vez completada la inicialización del PS (indicada por el valor '1' (pass) de cabhPsDevProvState):

1) El PS genera un número aleatorio xa para cada una de las filas rellenas de usmDHKickstartTable que tengan un usmDHKickstartSecurityName y un usmDHKickstartMgrPublic de longitud no nula.

2) El PS utiliza la ecuación DH para traducir xa un número público c (para cada una de las filas definidas anteriormente).

$$c = (g \wedge xa) \text{ MOD } p$$

siendo g un parámetro del conjunto Diffie-Hellman y el primo de dichos parámetros.

En este instante:

usmDHKickstartMyPublic.1 = "c" (cadena de octetos);

usmDHKickstartMgrPublic.1 = "z" (cadena de octetos);

usmDHKickstartSecurityName.1 = "docsisManager".

3) El PS calcula el secreto compartido sk de acuerdo con la expresión sk = z ^xa mod p.

4) El PS utiliza el sk para calcular la clave de privacidad y la clave de autenticación para cada una de las filas de usmDHKickstartTable y establece los valores de usmUserTable.

Como especifica [RFC 2786], la clave de privacidad y la clave de autenticación para el nombre de usuario asociado, "PS Administrator" en este caso, se calcula a partir de sk por aplicación de la función de derivación de clave 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 el proceso de inicialización del SNMPv3 y DEBE otorgar el nivel de acceso adecuado a un securityName válido con la clave de autenticación y/o clave de privacidad correctas.

El PS DEBE rellenar las claves de los cuadros correspondientes especificados en las RFC relacionadas con el SNMPv3- y en [RFC 2786].

5) A continuación se describe el proceso utilizado por el gestor para obtener la clave de autenticación y la clave de privacidad únicas del PS.

El gestor del SNMP accede al contenido de usmDHKickstartTable utilizando el nombre de seguridad 'dhKickstart' sin autenticación.

El PS DEBE proporcionar entradas de los cuadros USM y VACM introducidas previamente a fin de crear correctamente el 'dhKickstart' de usuario de nivel de seguridad noAuthNoPriv con acceso de sólo lectura al grupo del sistema y a usmDHkickstartTable.

Si el PS se encuentra en el modo de coexistencia y está configurado para utilizar SNMPv3, la especificación de grupo para la vista dhKickstart DEBE implementarse del siguiente modo:

dhKickstart Group	
vacmGroupName	'dhKickstart'
vacmAccessContextPrefix	"
vacmAccessSecurityModel	3 (USM)
vacmAccessSecurityLevel	NoAuthNoPriv
vacmAccessContextMatch	exacta
vacmAccessReadViewName	'dhKickstartView'
vacmAccessWriteViewName	"
vacmAccessNotifyViewName	"
vacmAccessStorageType	permanente
vacmAccessStatus	activo

La vista VACM para la vista dhKickstart DEBE implementarse del siguiente modo:

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 del SNMP obtiene el valor del número usmDHKickstartMypublic del PS asociado al securityName para el que el gestor desea obtener las claves de autenticación y de privacidad. A partir del número aleatorio privado, el gestor puede calcular el secreto compartido DH. A partir de dicho secreto compartido, el gestor puede obtener claves de autenticación y confidencialidad operacionales para el securityName que el gestor va a utilizar para comunicarse con el PS.

6.3.6.1.2.2 Modificaciones de clave Diffie-Hellman

El PS DEBE soportar el mecanismo de modificación de claves especificado en [RFC 2786].

6.3.6.2 Modo de prestación SNMP

Si el PS está funcionando en el modo de prestación SNMP después de un DHCP ACK [indicado por el valor '2' (SNMPmode) de cabhPsDevProvMode], funciona en el modo de gestión de red utilizando SNMPv3, USM y VACM y Kerberos para el intercambio de material clave (descrito en 6.3.3) o venciendo las reglas descritas en dicha cláusula.

6.3.6.2.1 Vistas de gestión

Los controles de gestión se encuentran en el elemento PS. Los valores, basados en el modo de gestión, definen los derechos de acceso otorgados a un generador de mandatos para acceder a la base de datos del PS, a través de las MIB especificadas, mediante el SNMP del NMS de la red de cable. La especificación define un único generador de mandatos.

La figura 12 muestra ejemplos de vistas de gestión utilizando SNMPv3. Se definen una vista del administrador de la WAN (vista del administrador del PS) y un usuario administrador de la WAN (usuario administrador del PS). Pueden establecerse otras vistas y usuarios, tales como la vista de mantenimiento de la WAN, la vista del administrador de la LAN y la vista del usuario de la LAN, mediante la autorización final (administrador del PS), en virtud de las reglas definidas en [RFC 2574] y [RFC 2575].

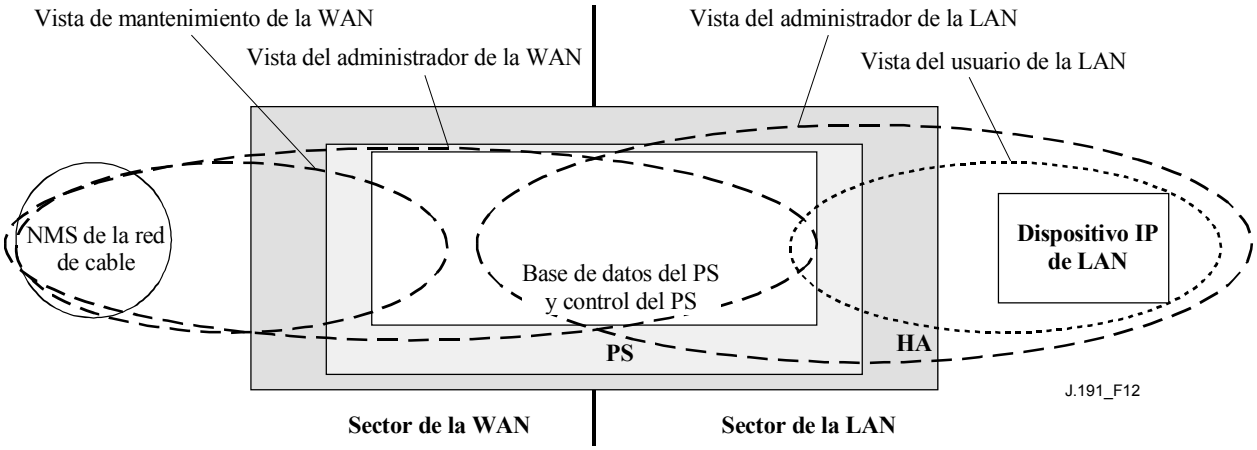


Figura 12/J.191 – Vistas de gestión

Los parámetros gestionados se almacenan en la base de datos del PS. Como muestra la figura 12, 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.

Es responsabilidad de la autorización final (usuario administrador del PS) lo siguiente:

- El establecimiento de todas las vistas de acceso en las interfaces de gestión de la LAN y de la WAN.
- La disponibilidad del propio ID y claves de usuario.
- 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 6.3.6.4 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 6.3.6.4.

6.3.6.2.2 Control de acceso WAN

El control de acceso SNMP, de acuerdo con [RFC 2575], se utilizará para las vistas del lado WAN. El modelo de control de acceso basado en vistas (VACM, *view-based access control model*) [RFC 2575] define un conjunto de servicios que pueden utilizarse para la comprobación de derechos de acceso. Los grupos VACM definen en los derechos de acceso al CMP.

De acuerdo con lo definido en la sección 2.4 de [RFC 2575], la "vista MIB" es un conjunto específico de tipos de objetos gestionados que pueden definirse, utilizándose este concepto 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 6.3.6.4. 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 SNMP v3 para responder a las amenazas definidas en el anexo C.

Como protección contra los ataques de repetición de la reproducción, se utiliza un reloj en tiempo real 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 de seguridad

Los requisitos de seguridad de los mensajes de gestión se especifican en 11.3.3.

6.3.6.4 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 DEBE utilizarse el modelo de control de acceso basado en vistas (VACM) definido en [RFC 2575].

La vista del administrador de la WAN DEBE implementarse en el elemento PS. Las vistas por defecto distintas de la vista del administrador de la WAN, NO DEBEN estar disponibles en el PS. PUEDEN crearse otras vistas por parte 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).

6.3.7 Requisitos de la MIB

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

MIB del grupo de interfaces de [RFC 2863].

1) MIB del dispositivo de cable DOCSIS [RFC 2669].
2) MIB DEF CLAB de cable [anexo E.4].
3) MIB PSDev de cable [anexo E.1].
4) MIB CAP de cable [anexo E.6].
5) MIB CDP de cable [anexo E.5].
6) MIB CTP de cable [anexo E.2].
7) MIB de seguridad de cable [anexo E.3].
8) draft-ietf-ipcdn-bpiplus-mib-06.txt.

9) IP MIB (SNMPv2) [RFC 2011].

10) UDP MIB (SNMPv2) [RFC 2013].

11) Clave USM Diffie-Hellman [RFC 2786].

12) MIB de dirección INET [RFC 2851].

13) MIB DOCS IF [RFC 2670].

14) MIB IANA ifType.

Con la excepción del grupo SNMP de la MIB 2, de la MIB USM y de la MIB VACM, a las que el agente SNMP del PS (CMP) tiene acceso directo, Y la MIB del dispositivo de cable DOCSIS en el caso de descarga de soporte lógico a un PS, el PS DEBE mantener ejemplares separados de las MIB especificados para el PS del módem de cable. La información de la base de datos del PS a la que se accede a través de la dirección WAN-Man del PS DEBE ser independiente y diferente de la información a la que se accede a través de la dirección de gestión del CM.

La jerarquía MIB genérica se ilustra en la figura 13. Los OID específicos requeridos para MIB individuales se relacionan en el anexo A.

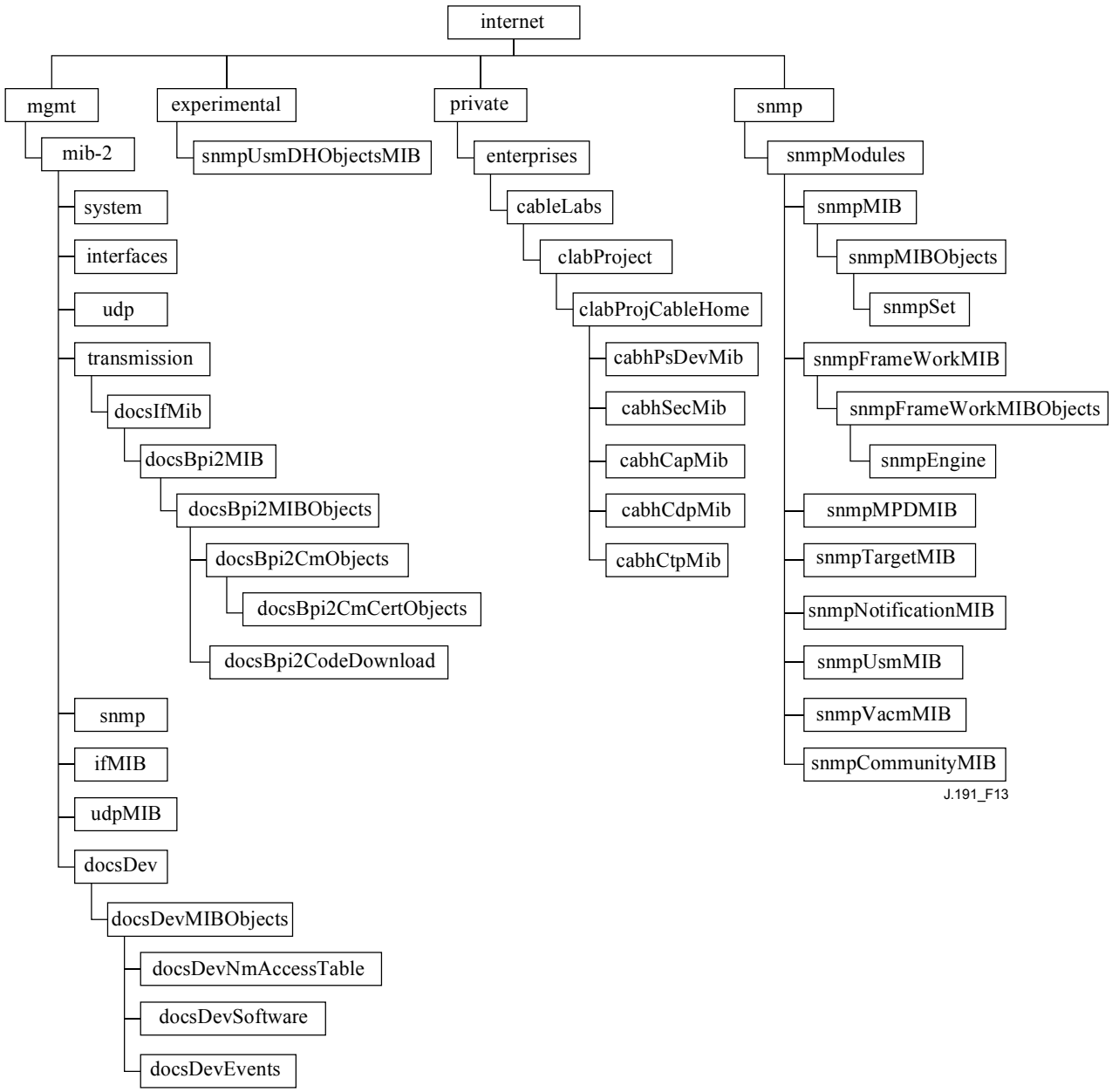


Figura 13/J.191 – Jerarquía MIB

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 del elemento PS, aunque dicha interfaz WAN sea interna – como existe en el caso de los PS integrados diseñados con circuitos integrados.

DEBE existir un ejemplar IfEntry para cada interfaz física de LAN del elemento PS.

Las interfaces DEBEN numerarse como indica el cuadro 12.

Cuadro 12/J.191 – Numeración de interfaces de la ifTable

Interfaz	Descripción
1	Interfaz de WAN
1 + n	Cada una de las interfaces de LAN

Si para una determinada interfaz ifAdminStatus = down, dicha interfaz NO DEBE aceptar ni entregar ningún tráfico.

6.3.9 Requisitos de proceso del fichero de configuración CMP

El CMP es la entidad funcional del PS que se encarga de procesar los parámetros pasados en el fichero de configuración del PS. Los ficheros de configuración del PS se utilizan para la reconfiguración del PS proporcionando valores a los parámetros gestionables de la base de datos del PS.

El fichero de configuración del PS recibido se verifica en primer lugar en cuanto a integridad y autenticación, de acuerdo con lo descrito en 11.3.7. A continuación, se analizan las tuplas TLV del fichero de configuración del PS y se extraen los identificadores de objeto del SNMP y sus parámetros. El CMP DEBE utilizar parámetros extraídos del fichero de configuración del PS para establecer los objetos gestionados en la base de datos PS. Este proceso es funcionalmente equivalente a una operación SNMP SET, pero no depende del usuario ni de los permisos de accesos basados en vistas. El CMP DEBE actualizar incondicionalmente los objetos correspondientes a OID reconocidos.

Los valores de configuración DEBEN procesarse en el mismo orden en que aparecen en el fichero de configuración del PS. El CMP DEBE poder admitir una serie de parámetros TLV contenidos en un fichero de configuración del PS. No hay ningún estado del PS preconcebido cuando se recibe el fichero de configuración del PS. El proceso de cargar y ejecutar un fichero de configuración del PS puede interrumpir el proceso de los datos del PS. El CMP DEBE ignorar cualquier valor de configuración para el que no exista un parámetro de base de datos válido.

Para los valores SNMP del fichero de configuración del PS, el PS DEBE tratar todas las vinculaciones variables SNMP (Varibinds) del fichero de configuración del PS como si se hubieran recibido en una única PDU SNMP. Si se reciben Varibinds duplicadas en el fichero de configuración del PS, el PS DEBE detener el proceso de recepción.

Los objetos definidos por TLV que se pasen en el fichero de configuración del PS y no se soporten o no puedan escribirse en la implementación PS específica DEBEN ignorarse. El CMP DEBE ignorar los TLV desconocidos.

El tamaño del fichero de configuración del PS, el número de TLV procesados y el número de TLV ignorados DEBEN actualizarse en los objetos MIB: cabhPsDevProvConfigFileSize, cabhPsDevProvConfigTLVProcessed y cabhPsDevProvConfigTLVRejected, respectivamente.

Los requisitos del fichero de configuración del PS se especifican en 7.3.

6.4 El portal de prueba del cable (CTP, *cableHome testing portal*)

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 se relacionan en el cuadro 13. Algunas de estas directrices coinciden con las de diseño del CMP. Esta relación proporciona orientaciones para la especificación de la funcionalidad CTP.

Cuadro 13/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 el hogar.
CTP 2	Se necesitan capacidades de supervisión locales y remotas que puedan controlar el funcionamiento en el hogar 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 en el hogar.
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 remotas" mediante las cuales la gestión del NMS puede recoger más información de los dispositivos de la LAN. Las pruebas deben efectuarse en remoto, 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: conectividad y diagnósticos de caudal.

Estas funciones reciben el nombre de herramienta de velocidad de la conexión CTP y herramienta de ping remoto del CTP. Las herramientas de velocidad de conexión y de ping remoto 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 del hogar.

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 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 retardo 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 velocidad de conexión se apoya en los dispositivos IP de LAN para poder integrar una "función de bucle" o "servicio de eco". La Autoridad de asignación de números Internet (IANA, *Internet assigned numbers authority*) ha asignado el puerto 7 del servicio de eco tanto para el TCP como el UDP [RFC 347]. La dirección IP de origen siempre es la de la pasarela por defecto de la LAN del PS (cabhCdpServerRouter). Esta característica de prueba sólo funciona en los dispositivos IP de LAN en el sector de direcciones LAN-Trans.

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.

La cláusula 6.4.4 contiene una relación de los parámetros y respuestas correspondientes a la herramienta ping. Obsérvese que el tiempo correspondiente a la respuesta de la petición no se almacena, ya que los tiempos de propagación de las tramas en el hogar suelen ser más rápidos que los que pueden medirse con precisión con las unidades de tiempo normales (ms). Para medir la calidad de funcionamiento debe utilizarse la herramienta de velocidad de la conexión.

La cláusula 12.2.1.2 explica detalladamente el funcionamiento de la herramienta ping.

6.4.4 Requisitos del CTP

El CTP DEBE implementar la herramienta de velocidad de la conexión con los parámetros enumerados a continuación, indicando los corchetes el objeto de la MIB del CTP. Los números encerrados entre corchetes son las opciones o bien los límites inferior y superior del intervalo de parámetros, mientras que los números en paréntesis indican los valores por defecto:

– <cabhCtpConnSrcIp> (igual al valor de cabhCdpServerRouter) – dirección IP de LAN utilizada como origen de la herramienta de velocidad de la conexión.

– <cabhCtpConnDestIp> – dirección IP de LAN utilizada como destino de la herramienta de velocidad de la conexión.

  NOTA 1 – Puede otorgársele cualquier dirección IPv4 válida, a fin de encontrar dispositivos IP de LAN en el sector de direcciones LAN-Trans.

– <cabhCtpConnProto> [UDP (1), TCP (2)] (UDP) – protocolo utilizado para la herramienta de velocidad de la conexión.

– <cabhCtpConnPort> [1 a 65535] (7) – puerto utilizado por la herramienta de velocidad de la conexión.

  NOTA 2 – La IANA reserva el puerto 7 para este fin. Podrían utilizarse asimismo otros puertos.

– <cabhCtpConnNumPkts> [1 a 255] (1) – número de paquetes que la herramienta de velocidad de la conexión ha de enviar.

– <cabhCtpConnPktSize> [–64 a 1518] (64) – tamaño de las tramas de prueba correspondientes a la herramienta de velocidad de la conexión en bytes.

– <cabhCtpConnTimeOut> [0 a 600000] (600000) – límite temporal, en milisegundos de la respuesta a la herramienta de velocidad de la conexión.

  NOTA 3 – El valor cero indica la ausencia de límites, pero sólo puede utilizarse con TCP.

– <cabhCtpConnControl> [notRun (1), start (2), abort (3)] – control para las pruebas de velocidad de conexión.

– <cabhCtpConnStatus> [running (1), complete (2), aborted (3)] – estado de la prueba de la velocidad de la conexión.

– <cabhCtpConnPktsSent> [1 a 255] – número de paquetes enviados durante la prueba de velocidad de la conexión.

– <cabhCtpConnPktsRecv> [0 a 255] – número de paquetes recibidos durante la prueba de velocidad de la conexión.

NOTA 4 – Este valor permite al operador establecer si se ha alcanzado el límite temporal (PktsSent > PktsRecv) debido a pérdidas de paquetes, suponiendo que el límite temporal se calculara correctamente. Este par de parámetros se ha incluido para soportar la detección de la pérdida de paquetes UDP. En circunstancias normales, PktsRecv es igual a PktsSent.

– <cabhCtpConnAvgRTT> [0 a 600000] – promedio resultante del tiempo de ida y vuelta de los paquetes aceptados en milisegundos.

– <cabhCtpConnMaxRTT> [0 a 600000] – máximo resultante de los tiempos de ida y vuelta de los paquetes aceptados en milisegundos.

– <cabhCtpConnMinRTT> [0 a 600000] – mínimo resultante de tiempos de ida y vuelta de los paquetes aceptados en milisegundos.

– <cabhCtpConnNumIcmpError> [0 a 255] – número de errores ICMP.

NOTA 5 – Este valor puede incluir los "prohibidos" o "inalcanzables" de la red o del servidor. El valor por defecto de este parámetro es nulo, tomando asimismo el valor nulo cuando no hay errores.

– <cabhCtpConnIcmpError> [0 a 255] – último error ICMP.

El CTP DEBE implementar la herramienta ping del CTP con los parámetros listados a continuación, indicando los corchetes el objeto de la MIB del CTP, correspondiendo los números entre corchetes a los límites inferior y superior del intervalo de parámetros e indicando el número entre paréntesis el valor por defecto:

– <cabhCtpPingSrcIp> (igual al valor de cabhCdpServerRouter) – dirección IP de LAN utilizada como origen de la herramienta ping remota.

– <cabhCtpPingDestIp> – dirección IP de LAN utilizada como destino para la herramienta ping remota.

– <cabhCtpPingProto> [icmp (1)] (icmp) – protocolo utilizado para la herramienta ping remota.

– <cabhCtpPingNumPkts> [1 a 4] (1) – número de paquetes enviados a cada uno de los servidores para la prueba ping remoto.

– <cabhCtpPingPktSize> [–64 a 1518] (64) – tamaño de las tramas de prueba correspondientes a la prueba del ping remoto en bytes.

– <cabhCtpPingTimeBetween> [0 a 600000] (1000) – tiempo transcurrido entre el envío de los paquetes consecutivos durante la prueba del ping remoto en milisegundos.

– <cabhCtpPingTimeOut> [0 a 600000] (5000) – límite temporal para la respuesta al envío de un ping sencillo durante la prueba del ping remoto en milisegundos.

– <cabhCtpPingControl> [notRun(1), start (2), abort (3)] – control para la prueba del ping remoto.

– <cabhCtpPingStatus> [running (1), complete (2), aborted (3)] – estado de la prueba del ping remoto.

– <cabhCtpPingNumSent> [0 a 254] – número de pings enviados durante la prueba del ping remoto.

– <cabhCtpPingNumRecv> [0 a 254] – número de pings recibidos durante la prueba del ping remoto.

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 en 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 predefinido.

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)
- 5: informativo(4)

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 no volátil en el registro local 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 2571]. El PS DEBE soportar la PDU SNMP INFORM descrita en [RFC 2571]. INFORM es una variante de TRAP 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 "CABLE" para los mensajes de cable 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 cable 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 cable (0 a $2^{31} – 1$). La primera letra de un código de error siempre va en mayúsculas.

texto – para los mensajes de cable 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>PS Element[CABLE]: <68000402> Time of the day received in invalid format.

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

6.5.2 Formato de los eventos

Los mensajes de eventos de gestión 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 se definen en el anexo B. Cada evento de gestión descrito en este anexo tiene asignado un ID de evento.
- Texto del evento – describe el evento de manera inteligible.
- Dirección MAC – describe la dirección MAC del dispositivo.

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 subcláusula.

6.5.2.1 Prioridad de los eventos

[RFC 2669] define ocho niveles de prioridad distintos y los mecanismos de información correspondientes a cada nivel. Los eventos normales especificados en este documento utilizan los siguientes niveles de prioridad.

1) Evento de emergencia (prioridad 1)

   Se reserva para errores '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.

2) 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.

3) 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.

4) 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.

5) Evento de alarma (prioridad 5)

   Avería que podría interrumpir el flujo normal de datos. Los informes de SYSLOG y TRAP están desactivados por defecto para este nivel.

6) 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'.

7) 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.

8) 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 14 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 14/J.191 – Tipos de notificación por defecto de las prioridades de eventos del PS

Prioridad del evento	No volátil local (bit-0)	SNMP TRAP (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	No	Sí	Sí	Sí	Normal
5) Alarma	No	No	No	Sí	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 cuadro 15 muestra el nivel de soporte mínimo necesario para los tipos de notificación correspondientes a las diversas prioridades de eventos. Por ejemplo, el PS tiene que dar un soporte mínimo a las anotaciones no volátiles en el registro histórico local correspondientes a las prioridades de eventos de emergencia, de alerta y críticos. El PS DEBE soportar los requisitos mínimos para la implementación de las prioridades de eventos correspondientes a cada tipo de comunicación de eventos. El PS PUEDE optar por comunicar una prioridad de evento con más tipos de notificación que los que se exigen en el cuadro 15.

Cuadro 15/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)	SNMP TRAP (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 1907] y [RFC 2863]:

- coldStart [RFC 1907];
- linkUp [RFC 2863];
- linkDown [RFC 2863];
- SNMP authentication-Failure [RFC 1907] (fallo de autenticación SNMP).

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 los mensajes TRAP y SYSLOG se suprima 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.

7 Herramientas de prestación

7.1 Introducción y presentación

El elemento PS 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 prestación 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 prestación definidas para acometer estas tareas son las siguientes:

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

7.1.1 Modos de prestación

Se soportan dos modos de prestación, a saber el modo de prestación DHCP (modo DHCP) y el modo de prestación SNMP (modo SNMP). El cuadro 16 compara los dos modos de prestación.

Cuadro 16/J.191 – Modos de prestación

	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 prestación depende del modo de prestación en el que funcione el PS.

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

7.1.2 Arquitectura de prestación

La figura 14 ilustra la arquitectura de prestación. Los elementos PS 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.

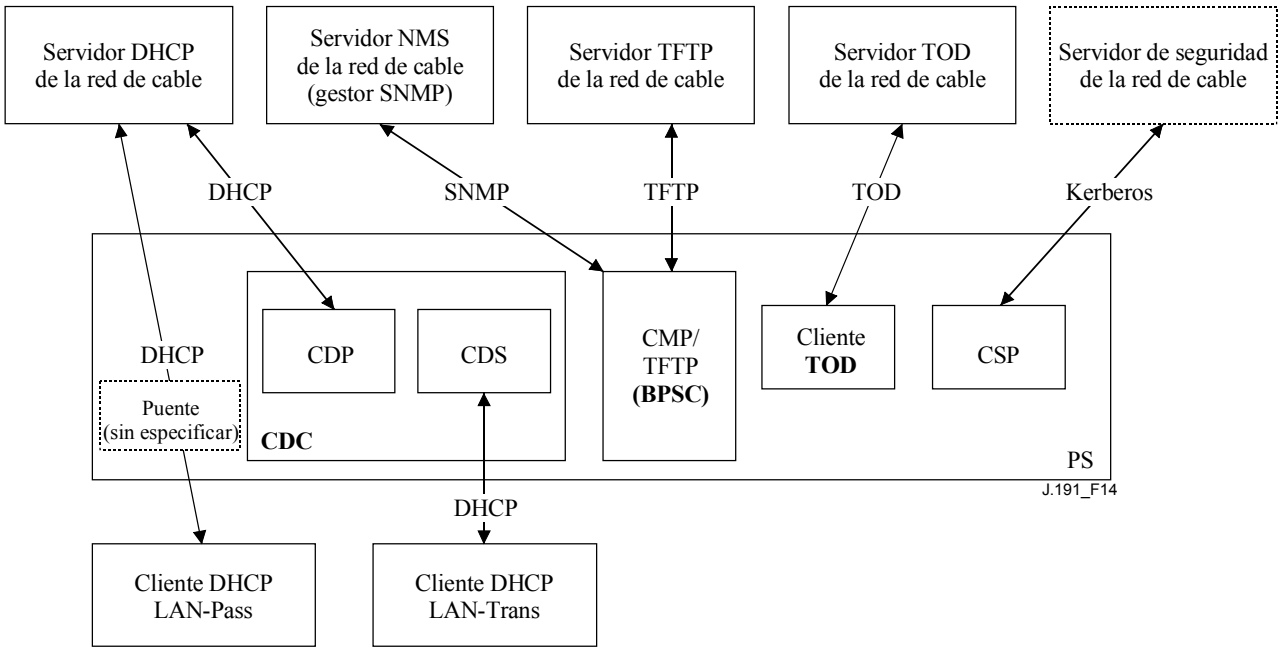


Figura 14/J.191 – Arquitectura de prestación

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 PS de acuerdo con las reglas especificadas en esta cláusula.

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

- 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 prestación de la red de cable implementa un servidor DHCP definido por [RFC 2131].

3) Si el servidor DHCP del sistema de prestación 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 cable (CDP) es una de las tres herramientas de prestación 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 en el cuadro 17 permiten obtener las capacidades definidas para el CDP:

Cuadro 17/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 de cable conocimiento del **servicio de portal** 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. Entre las responsabilidades de petición y atribución de direcciones del CDP 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 PS.
- Información al portal de nombres de cable (CNP) como soporte de los servicios de nombre de servidor del dispositivo IP de LAN.

El elemento PS necesita una dirección IP para poder funcionar como encaminador de tráfico en el hogar (véase la cláusula 8, Tratamiento de paquetes y traducción de direcciones), servidor DHCP (CDS, *DHCP server*), y servidor DNS (véase la cláusula 9, Resolución de nombres). 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 17.

Dirección del encaminador (pasarela por defecto)	cabhCdpServerRouter
Dirección del sistema 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 15, 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).

La figura 15 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.

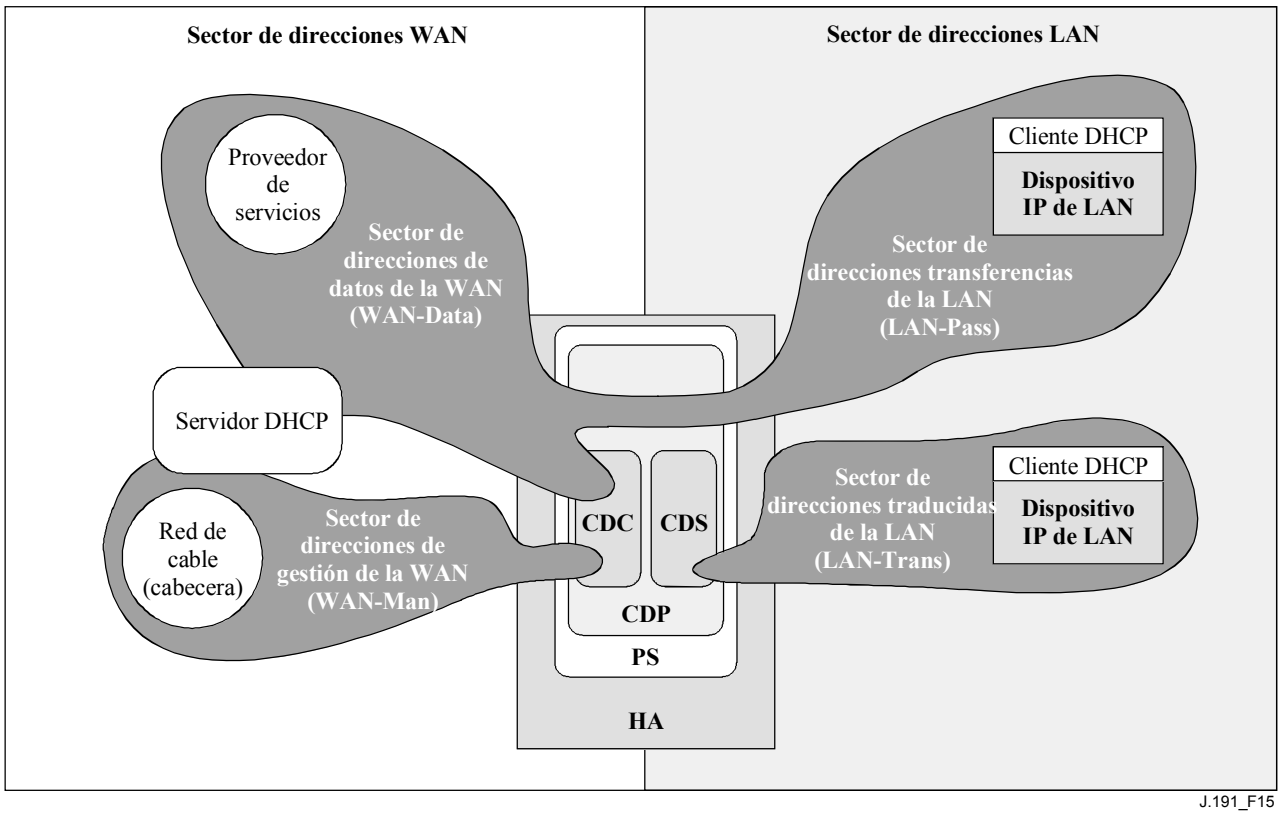


Figura 15/J.191 – Funciones del CDP

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.
- A falta de información horaria procedente del servidor de hora del día (TOD, *time of day*), el CDS utiliza la hora 0 de arranque del PS por defecto (1 de enero de 1900), 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 o reactivarse el PS, el CDS se mantiene inactivo hasta ser activado por el PS tras terminar con éxito la descarga del fichero de configuración del PS o tras cinco intentos infructuosos de descarga del fichero de configuración del PS por parte de éste, si no hubiera ocurrido lo anterior. De este modo se evita que el CDS otorgue licencias DHCP en el sector LAN-Trans hasta que el operador de cable haya tenido oportunidad, dentro de lo razonable, de actualizar los parámetros de la licencia LAN-Trans tales como cabhCdpServerLeaseTime, cabhCdpLanPoolStart y cabhCdpLanPoolEnd.
- Si el modo de tratamiento de paquetes primario del PS (cabhCapPrimaryMode) tuviera el valor Passthrough (transferencia), se desactivaría el CDS.

Los dispositivos IP de LAN pueden recibir direcciones que residan en el sector LAN-Pass. Como muestra la figura 15, 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 automática", "asignación dinámica" y "asignación manual" se utilizan con arreglo a la definición de [RFC 2131]. La asignación automática de direcciones IP del sector de direcciones LAN-Trans será permanente, pudiendo reutilizar el CDS direcciones automáticas siempre que todas las direcciones disponibles ya hayan sido asignadas. El CDS utiliza las **opciones DHCP proporcionadas por el CDS**, objetos cabhCdpServer de la MIB del CDP, para indicar las opciones DHCP ofrecidas a los dispositivos IP de LAN a los que se ha asignado 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 17) 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 automáticamente (a través del CDP) (cabhCdpLanAddrConfig).

El CDS utiliza direcciones MAC para identificar los dispositivos IP de LAN.

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], como se describe en 7.2.2.2.1. Opciones 60 y 43 del cliente DHCP del cable.

La opción de identificador de la clase de fabricante (opción 60 del DHCP) define una clase de dispositivo específica. La opción de identificador de la clase de fabricante contendrá una cadena

específica para identificar un elemento lógico PS, 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, los componentes que contiene el dispositivo (CM, MTA, PS, etc.), el número de serie del dispositivo y admite asimismo parámetros específicos del dispositivo.

Los cuadros 19 y 20 contienen detalles de los requisitos para soportar las opciones 60 y 43 del DHCP.

7.2.2.2.1 Opción de cliente 61 DHCP del cable

El elemento PS puede tener una o varias direcciones IP de la 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 contempla la utilización de la opción de identificador del cliente (Opción 61 del DHCP), sección 9.14 de [RFC 2132] para identificar exclusivamente la interfaz WAN lógica asociada a una dirección IP determinada.

Para ser compatible con el mayor número de sistemas de prestación de operador de cable posible, el CDC deberá soportar los siguientes modos de direccionamiento WAN configurables:

Modo 1 de direccionamiento de la WAN: el elemento PS utiliza una única dirección IP de la WAN. El elemento PS tiene una interfaz IP WAN-Man y otra WAN-Data, que comparten una dirección MAC común. Estas dos interfaces comparten una única dirección IP común. Ésta es la configuración por defecto del fabricante para el elemento PS. Normalmente el servidor DHCP de cabecera del operador de cable no necesita modificar sus programas para soportar este modo de prestación.

Modo 2 de direccionamiento de la WAN: El elemento PS utiliza dos o más direcciones IP de la WAN distintas. El elemento PS puede tener una interfaz IP WAN-Man y una o varias WAN-Data, compartiendo una dirección MAC común. Estas dos, o varias, interfaces tendrían sus propias direcciones IP no compartidas. Podría ser necesario modificar los programas informáticos del servidor DHCP de cabecera del operador de cable para soportar la asignación de varias direcciones IP a una única dirección MAC. En este modo, el servidor DHCP de la cabecera necesitará soportar la asignación IP en base al ID de cliente (opción 61) así como en base a la dirección MAC.

El modo 2 de direccionamiento de la WAN se activa mediante la escritura de una única cadena de ID de cliente en la entrada cabhCdpWanDataAddrClientId de cabhCdpWanDataAddrTable de las MIB del CDP, para cada interfaz WAN-Data que vaya a utilizarse. Para soportar este modo de prestación, el operador de cable necesitará proporcionar al elemento PS (mediante el NMS, el fichero de configuración o mediante introducción manual por parte del cliente a través de una interfaz propietaria) una cadena de ID de cliente única para cada interfaz IP WAN-Data.

7.2.3 Requisitos del portal DHCP de cable

7.2.3.1 Requisitos del CDP

La asignación manual de direcciones del CDP DEBE soportarse utilizando las anotaciones del cuadro CDP (cabhCdpLanAddrTable) generadas por el sistema NMS o el fichero de configuración.

Las anotaciones del cuadro de gestión de direcciones de la LAN del CDP (cabhCdpLanAddrTable) recibidas DEBEN conservarse durante las desconexiones del cable y DEBEN conservarse tras un ciclo de alimentación del PS. El CDS DEBE poder suministrar servicios de direccionamiento DHCP a los dispositivos IP de LAN, independientemente del estado de conectividad de la WAN.

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 automática, dinámica y manual de direcciones conforme a la sección 1 de [RFC 2131].

En la reactivación o rearranque del PS el CDS NO DEBE intercambiar mensajes DHCP con dispositivos IP de LAN hasta que el PS active el CDS, tras la descarga con éxito del fichero de configuración del PS o tras cinco intentos de descarga consecutivos sin éxito del fichero de configuración del PS, si no hubiera ocurrido lo anterior.

El CDS DEBE asignar direcciones y entregar parámetros de configuración del DHCP únicamente a los dispositivos IP de LAN que reciban una dirección perteneciente al sector de direcciones LAN-Trans.

La asignación automática de direcciones del sector de direcciones LAN-Trans DEBE ser permanente aunque el CDS PUEDE reutilizar direcciones automáticas cuando se hayan asignado todas las direcciones disponibles.

El CDS DEBE utilizar las direcciones físicas (MAC) de los dispositivos IP de LAN como valores identificativos de los clientes.

El CDS DEBE soportar la MIB del CDP incluidos todos los objetos de la cabhCdpLanAddrTable, los objetos del cabhCdpLanPool, los objetos cabhCdpServer, y los objetos cabhCdpLanTrans.

El CDS DEBE soportar las opciones DHCP señaladas como obligatorias en la columna de soporte del protocolo CDS del cuadro 18.

Cuadro 18/J.191 – Opciones DHCP del CDS

Número de la opción	Función de la opción	Soporte del protocolo CDS (M) obligatorio u (O) opcional	Soporte de gestión del CDS (M) obligatorio u (O) opcional	Datos por defecto de fábrica del CDS	Retención por desconexión del cable del CDS (M) obligatorio	Conservación tras interrupción de alimentación del CDS (M) obligatorio	Nombre del objeto de la MIB
0	Rellenar	M	–	N/A	N/A	N/A	N/A
255	Terminar	M	M	N/A	N/A	N/A	N/A
1	Máscara de subred	M	M	255.255.255.0	M	M	cabhCdpServer SubnetMask
2	Diferencia horaria	M	O	O	N/A	N/A	cabhCdpServer TimeOffset
3	Opción del encaminador	M	M	192.168.0.1	M	M	cabhCdpServer Router
6	Servidor de nombres de dominio	M	M	192.168.0.1	M	M	cabhCdpServer DnsAddress
7	Servidor de anotaciones históricas	M	M	0.0.0.0	M	M	cabhCdpServer SyslogAddress
12	Nombre del servidor	M	O	N/A	N/A	N/A	N/A
15	Nombre de dominio	M	M	Cadena nula	M	M	cabhCdpServer DomainName

Cuadro 18/J.191 – Opciones DHCP del CDS

Número de la opción	Función de la opción	Soporte del protocolo CDS (M) obligatorio u (O) opcional	Soporte de gestión del CDS (M) obligatorio u (O) opcional	Datos por defecto de fábrica del CDS	Retención por desconexión del cable del CDS (M) obligatorio	Conservación tras interrupción de alimentación del CDS (M) obligatorio	Nombre del objeto de la MIB
23	Tiempo de vida por defecto	M	M	255	M	M	cabhCdpServer TTL
26	MTU de la interfaz	M	M	1520	M	M	cabhCdpServer InterfaceMTU
43	Información específica del fabricante	M	M	Seleccionado por el fabricante	M	M	cabhCdpServer VendorSpecific
50	Dirección IP solicitada	M	N/A	N/A	N/A	N/A	N/A
51	Tiempo de licencia de la dirección IP	M	M	60	M	M	cabhCdpServer LeaseTime
54	Identificador del servidor	M	M	192.168.0.1	M	M	cabhCdpServer DhcpAddress
55	Lista de petición de parámetros	M	N/A	N/A	N/A	N/A	N/A
60	Identificador de la clase de fabricante	M	N/A	N/A	N/A	N/A	N/A
61	Identificador del cliente	M	N/A	N/A	N/A	N/A	N/A

El CDS DEBE soportar la prestación por parte del NMS de las opciones señaladas como obligatorias en la columna soporte de gestión del CDS del cuadro 18.

Las opciones DHCP del CDS señaladas como obligatorias en la columna de retención de desconexión de cable del CDS del cuadro 18 DEBEN conservarse durante la interrupción del servicio del cable.

Las opciones DHCP del CDS señaladas como obligatorias en la columna conservación tras interrupción de alimentación del CDS del cuadro 18 DEBEN conservarse tras un ciclo de alimentación del CDP.

El CDS DEBE soportar la oferta de los valores por defecto indicados en la columna valores por defecto de fábrica del CDS del cuadro 18, no se ha proporcionado si la opción DHCP.

Si el modo tratamiento de paquetes primario del PS (cabhCapPrimaryMode) tuviera el valor transferencia (Passthrough), el CDS DEBERÍA desactivarse.

Para soportar la asignación automática de direcciones, el CDS DEBE poder crear, modificar y suprimir las entradas del cuadro CDP correspondientes a los dispositivos a los que se ha asignado una dirección LAN-Trans.

El CDS DEBE conservar el parámetro contador de direcciones (cabhCdpLanTransCurCount) que indica el número de direcciones LAN-Trans asignadas a los dispositivos IP de 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. 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.

La acción específica emprendida por el CDS DEBE ajustarse a lo indicado por el parámetro suministrado acción de umbral excedido (cabhCdpLanTransAction).

7.2.3.3 Requisitos del CDC

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

El elemento PS DEBE tener una dirección física de interfaz WAN distinta de la del módem de cable.

Si el CDC recibe en la respuesta DHCP [RFC 2131] del servidor DHCP de la red de cable, una dirección IP válida en el campo 'siaddr' Y un nombre de fichero válido en el campo 'file' Y no recibe la subopción 51 de la opción 177 del DHCP, el PS DEBE hacer cabhPsDevProvMode igual a '1' (Modo DHCP).

Si el CDC recibe del servidor DHCP de la red de cable, una dirección IP válida para la subopción 51 de la opción 177 del DHCP Y no recibe una dirección IP válida en el campo 'siaddr' Y no recibe un nombre de fichero válido en el campo 'file' el PS DEBE hacer cabhPsDevProvMode igual '2' (Modo SNMP).

Si el CDC recibe en el mensaje DHCP [RFC 2131] del servidor DHCP de la red de cable, la subopción 51 de la opción 177 del DHCP Y una dirección IP válida en el campo 'siaddr', O si el CDC recibe la subopción 51 de la opción 177 del DHCP Y un nombre de fichero válido en el campo 'file', el PS DEBE anotar en el registro histórico local un error y reemitir el mensaje DHCP DISCOVER (es decir, reiniciar la secuencia de prestación en el evento de esta condición no válida).

Si el CDC no recibe la subopción 51 de la opción 177 del DHCP Y no recibe una dirección IP válida en el campo 'siaddr' Y no recibe un nombre de fichero válido en el campo 'file' el PS DEBE anotar un error en el registro histórico local y reemitir el mensaje DHCP DISCOVER (es decir, reiniciar la secuencia de prestación en el evento de esta condición no válida).

La subopción 11 de la opción 43 del DHCP es un parámetro específico del dispositivo que indica si una dirección está siendo solicitada en el sector de gestión de la WAN del PS o en el sector de datos de la WAN del PS. El cuadro 19 indica cómo DEBEN establecerse los valores correspondientes a estas interfaces para la subopción 11 de la opción 43 del DHCP.

Cuadro 19/J.191 – Valores de la subopción 11 de la opción 43 del DHCP

Id del elemento	Descripciones y comentarios
PS WAN-Man = 0x01	Identifica las peticiones de dirección del sector WAN-Man
PS WAN-Data = 0x02	Identifica las peticiones de dirección del sector WAN-Data

El CDC DEBE implementar la opción de identificador de la clase de fabricante (opción 60 del DHCP) especificada en el cuadro 20.

El módem de cable y el elemento PS envían peticiones DHCP por separado. El cuadro 20 describe la manera en que el CDC DEBE fijar el contenido de las opciones 60 y 43 para el PS cuando se solicitan direcciones de gestión de la WAN y de datos de la WAN del PS por separado.

Cuadro 20/J.191 – Opciones DHCP para las peticiones de direcciones integradas de los sectores WAN-Man y WAN-Data del PS

Opciones de petición del DHCP	Valor	Descripción
Petición al DHCP del PS para direcciones de gestión de la WAN		
Opción 60 del CPE	"PS"	
Subopción 1 de la opción 43 del CPE	Vector de subopciones 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
Subopción 11 de la opción 43 del CPE	PS WAN-Man (0x01)	Define que la dirección está siendo solicitada en el sector de gestión de la WAN del PS
Petición DHCP del PS de direcciones WAN-Data		
Opción 60 del CPE	"PS"	
Subopción 1 de la opción 43 del CPE	Vector de subopciones 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"	Listas de dispositivos integrados (CM y PS integrados)
Subopción 4 de la opción 43 del CPE	Por ejemplo,"123456"	Número de serie del dispositivo
Subopción 11 de la opción 43 del CPE	PS WAN-Data (0x02)	Define que la dirección está siendo solicitada en el sector PS WAN-Data

El CDC DEBE soportar las opciones DHCP indicadas como obligatorias en la columna soporte de protocolo del CDC del cuadro 21.

Cuadro 21/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 servidor	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	Dirección IP del servidor Kerberos – subopción 51	M

El cuadro 21 representa las opciones DHCP que el CDC debe soportar obligatoria u opcionalmente. Las opciones DHCP señaladas como obligatorias en el cuadro 21 DEBEN incluirse en los mensajes DHCP DISCOVER y DHCP REQUEST enviados por el CDC al servidor DHCP de la red de cable.

El PS DEBE soportar una dirección de entidades SNMP del proveedor de servicios (subopción 3 de la opción 177 del DHCP) configurada como dirección IPv4.

Siempre que la primera interfaz PS WAN-Data no tenga una licencia DHCP vigente, dicha interfaz DEBE utilizar los siguientes parámetros IP por defecto:

(Esta dirección IP se utiliza para la correspondencia de la WAN con arreglo a la tupla NAPT dinámica. Esta dirección no puede utilizarse para la correspondencia NAT porque el lado WAN de la correspondencia NAT se conserva. Tampoco puede utilizarse para las direcciones transferencias porque éstas se seleccionan del grupo de direcciones IP del proveedor de servicios.)

Dirección IP de gestión: 192.168.100.5

Máscara de red: 255.255.255.0

Pasarela por defecto: 192.168.100.1

Aunque utilice la dirección IP 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 dicha interfaz WAN-Data del PS (o a la interfaz WAN-Man, si la WAN-Man y la WAN-data comparten una dirección IP).

Cuando el PS está adquiriendo una dirección IP de gestión de la WAN para su interfaz WAN-Man, el CDC DEBE insertar siempre su dirección física de WAN en el campo Client ID (opción 61 del DHCP) del mensaje DHCP DISCOVER.

Cuando un PS funcionando en el modo 2 de direccionamiento de la WAN (descrito en 7.2.2.2) esté adquiriendo una dirección IP WAN-Data para una interfaz WAN-Data que utilice una dirección IP distinta de la interfaz WAN-Man, el CDC DEBE incluir la opción de identificador del cliente (cabhCdpWanDataAddrClientId) en el mensaje DHCP DISCOVER. Para obtener estos ID de cliente Wan-Data únicos, el CDC DEBE encargar al sistema NMS la creación de entradas cabhCdpWanDataAddrClientId en cabhCdpWanDataAddrTable.

Si un PS está funcionando en el modo 2 de direccionamiento de la WAN (descrito en 7.2.2.2) el CDC DEBE intentar obtener una dirección IP a través del DHCP, para cada ID de cliente único (cabhCdpWanDataAddrClientId) del cabhCdpWanDataAddrTable.

El CDC DEBE continuar difundiendo su mensaje DHCP DISCOVER (con arreglo a [RFC 2131]) hasta que reciba una dirección y el DHCP ACK. El límite temporal específico para el acceso al servidor DHCP depende de la implementación. No obstante, el CDC NO DEBE emitir el mensaje DHCP DISCOVER más de 3 veces cada 30 segundos. Como mínimo, el CDC DEBE emitir el DHCP DISCOVER una vez en cada intervalo de 30 segundos, hasta que consiga adquirir la dirección.

Si el CDC no recibe un DHCP OFFER tras 5 intentos de emitir el mensaje DHCP DISCOVER, el PS DEBE iniciar el funcionamiento del CDS, de modo que los dispositivos IP de LAN del sector LAN-Trans puedan obtener direcciones IP.

7.3 Arquitectura de configuración del PS en bloque

7.3.1 Directrices de diseño del sistema de configuración del PS en bloque

Las siguientes directrices de diseño del sistema en el cuadro 22 permiten obtener las capacidades definidas para la herramienta de configuración del PS en bloque:

Cuadro 22/J.191 – Directrices de diseño del sistema del PS 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 del PS en bloque

La configuración del PS en bloque se suele llevar a cabo durante la prestación 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:

Formato del fichero de configuración:

1) Modos de desencadenar el proceso de la descarga.
2) Medios de autenticación del fichero.
3) 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 no necesita la carga de un fichero de configuración antes de su funcionamiento. Se prevé que un PS se inicializará por sí mismo para alcanzar un estado conocido pudiendo funcionar indefinidamente sin necesidad de cargar un fichero de configuración. 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 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 del PS en bloque

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 23 proporciona las definiciones de estos términos.

Cuadro 23/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). La longitud del fichero DEBE completarse a un número entero de palabras de 32 bits. 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 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 del PS es la marca de fin de datos (Tipo 255).

Para mayor uniformidad de la gestión de los módems de cable mejorados en IP conformes con esta Recomendación, los dispositivos homologados DEBEN soportar un fichero de configuración de 64 kilobytes de longitud como máximo.

Un elemento PS DEBE soportar, y el fichero de configuración del PS PUEDE incluir, los tipos de parámetro de configuración 0, 4, 9, 17, 21, 28, 32, 33 y 255, descritos en esta cláusula.

El tamaño del valor del campo Longitud para cualquier parámetro de configuración incluido en un fichero de configuración del PS DEBE ser de 2 octetos.

El valor de la longitud para cada tipo descrito en 7.3.3.1.1 a 7.3.3.1.10 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 Clave pública RSA

Este atributo consiste en una cadena que contiene una RSAPublicKey codificada en DER tipo ASN.1, definida en la norma de criptación RSA PKCS #1 v2.0 [RSA1].

PKCS #1 v2.0 especifica que una clave pública RSA consta de un módulo público RSA y un exponente público RSA; el tipo RSAPublicKey incluye ambos tipos INTEGER codificados en DER.

PKCS #1 v2.0 indica que el exponente público RSA puede normalizarse en aplicaciones específicas y sugiere valores de 3 ó 65537 (F4). La presente Recomendación requiere F4 para un exponente público y utiliza un módulo de 2048 bits.

Tipo	Longitud	Valor
4	106, 140, ó 270[a)]	RSAPublicKey codificada en DER tipo ASN.1
[a)] Longitud de la codificación DER, utilizando F4 como exponente público y el módulo público de 2048 bits, respectivamente.		

7.3.3.1.3 Nombre del fichero de actualización del soporte lógico

Se trata del nombre del fichero de actualización del soporte lógico del PS. 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[a)]	Nombre del fichero
[a)] La longitud NO DEBE provocar que los mensajes de gestión de la MAC resultantes superen el tamaño máximo permitido.		

7.3.3.1.4 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 [UIT-T X.690], más un byte para la bandera de control.

La bandera de control puede tener los siguientes 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.

7.3.3.1.5 Certificado CA

Este atributo consiste en una cadena que contiene un certificado X.509 CA, definido en [UIT-T X.509].

Tipo	Longitud	Valor
17	Variable[a)]	Certificado X.509 CA (codificado en DER ASN.1)
[a)] La longitud NO DEBE provocar que el mensaje de gestión MAC resultante sobrepase el máximo tamaño permitido.		

7.3.3.1.6 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 PS.

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

7.3.3.1.7 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[a)]	Vinculación variable
[a)] La longitud NO DEBE provocar que el mensaje de gestión MAC resultante supere el máximo tamaño admisible.		

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 65 535 bytes.

7.3.3.1.8 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. El fichero de configuración del PS DEBE contener un M-CVC y/o un C-CVC a fin de permitir que el dispositivo descargue el fichero de códigos del servidor TFTP.

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

Si la longitud del M-CVC supera 65 535 bytes, el M-CVC DEBE fragmentarse en dos o más elementos correlativos tipo 32. Cada fragmento, con excepción del último, DEBE tener una longitud de 65 535 bytes. El PS reconstruirá el M-CVC concatenando los contenidos (valor del TLV) de los elementos tipo 32 correlativos en su orden de aparición en el fichero de configuración. Por ejemplo, el primer byte tras el campo de longitud del segundo elemento del tipo 32 se trata como si siguiese inmediatamente al último byte del primer elemento tipo 32.

7.3.3.1.9 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. El fichero de configuración del PS DEBE contener un C-CVC y/o un M-CVC a fin de permitir que el dispositivo descargue el fichero de código del servidor TFTP.

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

Si la longitud del C-CVC supera 65 535 bytes, el C-CVC DEBE fragmentarse en dos o más elementos correlativos tipo 33. Cada fragmento, salvo el último, DEBE tener una longitud de 65 535 bytes. El PS reconstruirá el C-CVC concatenando el contenido (valor del TLV) de los elementos correlativos tipo 33 en el orden de aparición en el fichero de configuración. Por ejemplo, el primer byte tras el campo longitud del segundo elemento tipo 33 se trata como si siguiese inmediatamente al último byte del primer elemento tipo 33.

7.3.3.1.10 Valor de arranque del SNMPv3

Los elementos del PS 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.

7.3.3.1.10.1 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.

7.3.3.1.10.2 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.

7.3.3.1.11 Elemento docsisV3NotificationReceiver del fichero de configuración

Tipo	Longitud	Valor
38	Variable	(Véase a continuación.)

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. El fichero de configuración del PS puede incluir un máximo de 10 de dichos elementos.

El formato de este elemento es el siguiente:

Definición de los campos del elemento docsisV3NotificationReceiver;

Todos los campos multibyte comienzan por los bytes más significativos del campo.

Este TLV (38) consta de varios SubTLV que se encuentran dentro del elemento del fichero de configuración TLV:

SubTLV 38.1 – dirección IP del receptor de trampas, en binario

4 bytes con la dirección IP del receptor de trampas, en binario.

SubTLV 38.2 – número de puerto UDP del receptor de trampas, en binario

2 bytes para el número de puerto UDP del receptor de trampas, en binario.

(si no existe se utiliza el valor por defecto 162)

SubTLV 38.3 – tipo de trampa enviada por el PS (Nota 2)

2 bytes para el 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

SubTLV 38.4 – límite temporal, en milisegundos, para el envío del informativo

2 bytes para el límite temporal 0-65535.

SubTLV 38.5 – número de reintentos para el envío de un informativo

2 bytes para los reintentos 0-65535.

SubTLV 38.6 – parámetros de filtrado de la notificación

Si no existe este SubTLV, el receptor de notificaciones recibirá todas las 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 enviarán esta notificación y todas las subsiguientes. <z> es la longitud en bytes de la codificación ASN.1. El campo comienza con el byte ASN.1 Universal Tipo 6 (identificador de objeto), seguido por el campo de longitud ASN.1 y a continuación los componentes del identificador de objeto codificado en ASN.1.

SubTLV 38.7 – nombre de seguridad que ha de utilizarse en el envío de la notificación SNMP V3

Esta SubTLV no es necesario para el tipo de trampas 1, 2, 3 y superiores. Si no se suministra para una trampa de Tipo 4 ó 5, se enviará la notificación V3 en el nivel de seguridad noAuthNoPriv utilizando el nombre de seguridad "@config" (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 de configuración como parte del procedimiento de arranque DH. Las notificaciones se enviarán 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 DEBERÁ efectuar anotaciones en los siguientes cuadro 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 DEBERÁ ser "public". El nombre de seguridad en las trampas y en los informativos de los paquetes SNMP V3 en los que no se haya especificado nombre de seguridad DEBERÁ ser "@config" y en este caso el nivel de seguridad DEBERÁ ser noAuthNoPriv.

NOTA 3 – OID de filtro: el SNMP V3 permite especificar qué OID de trampas van a enviarse a un receptor de trampas. El filtro OID 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 este subárbol de filtro de trampas DEBERÁN enviarse al receptor de trampas.

NOTA 4 – Número TLV del fichero de configuración: el campo tipo de este TLV DEBERÁ ser (38).

NOTA 5 – El fichero de configuración del PS PUEDE contener asimismo elementos TLV MIB que efectúan anotaciones en cualquiera de los 10 cuadros enumerados en la nota 1. Estos elementos TLV MIB NO DEBERÁN utilizar columnas de índice que comiencen con los caracteres "@config".

NOTA 6 – Este elemento TLV DEBERÁ procesarse sólo si el PS ha adoptado el modo de coexistencia SNMP V3 durante el proceso de fichero de configuración del PS.

7.3.3.1.12 Marca de fin de datos

Se trata de una marca especial de fin de datos. No tiene campos de longitud ni de valor.

Tipo	Longitud	Valor
255	–	–

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 prestación 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 prestación 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 OFFER, 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 valor de troceo de configuración del PS añadido al nombre de fichero de configuración del PS NO DEBE incluirse en el valor codificado como URL.

La descarga del fichero de configuración del PS, efectuada por un PS funcionando en el modo de prestación 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 la cláusula 7.2.3.3.

Si el PS está funcionando el modo de prestación 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.

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

Si el PS está funcionando en el modo de prestación 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, Seguridad, 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).

Si el PS está funcionando en el modo de prestación SNMP (indicado por el valor de cabhPsDevProvMode) Y el objeto cabhPsDevProvConfigHash del MIB PSDev tiene un valor válido, la descarga del fichero de configuración del PS DEBE activarse cuando un mensaje de petición Set SNMP, dirigido a la interfaz PS WAN-Man contenga un valor válido para el objeto de la MIB PSDev cabhPsDevProvConfigFile. El formato de cabhPsDevProvConfigFile DEBE ser una dirección IP del servidor TFTP y un nombre del fichero de configuración codificados como URL.

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.

Si el fichero de configuración del PS está debidamente autenticado, una vez terminada la descarga TFTP del fichero de configuración del PS, el PS DEBE procesar los TLV contenidos en el fichero. Consúltese en 6.3.9 la descripción de cómo procesa el CMP el fichero de configuración.

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.

Para autenticar el fichero de configuración del PS se utiliza un cálculo de troceado. El NMS calcula el troceado del fichero de configuración del PS y a continuación envía el valor de troceado resultante al elemento PS. La identidad del NMS que generó el fichero de configuración del PS se autentica comparando el troceado del fichero de configuración del PS generado por el NMS y transportado al elemento PS con el troceado (calculado por el PS) del fichero de configuración del PS descargado del servidor TFTP. La identidad del elemento PS que solicita el fichero no es necesaria.

El algoritmo de seguridad utilizado para autenticar el fichero de configuración del PS depende del modo de prestación del elemento PS (véase 5.7). Hay dos tipos de modos de prestación: el modo de prestación DHCP y el modo de prestación SNMP. En las subcláusulas siguientes se describen los algoritmos de seguridad de los requisitos necesarios para autenticar el fichero de configuración del PS en función del modo de prestación del elemento PS. El elemento PS DEBE soportar ambos algoritmos de seguridad, especificados 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 prestación DHCP

A continuación se indica el procedimiento de autenticación del fichero de configuración del PS por el elemento PS en el modo de prestación DHCP:

1) Cuando el NMS crea un nuevo fichero de configuración del PS o modifica un fichero existente, el NMS creará un troceado SHA-1 de todo el contenido del fichero de configuración del PS, considerado como una cadena de bytes.
2) El NMS añadirá el valor troceado al nombre del fichero de configuración del PS que se envía al elemento PS en el DHCP OFFER (véanse 7.2.3.3 y 13.2). El delimitador utilizado entre el nombre del fichero de configuración del PS y el valor de troceo es el carácter '@' (por ejemplo,"configfile1.txt@23423487987345"). El elemento PS actualiza el objeto de la MIB cabhPsDevProvConfigHash con el valor de troceo recibido.
3) El elemento PS descarga el mencionado fichero del servidor TFTP configurado.
4) El elemento PS DEBE calcular el troceo SHA-1 para todo el contenido del fichero de configuración del PS y comparar el troceo calculado con el troceo del objeto de la MIB cabhPsDevProvConfigHash si coincide el valor del troceo calculado con el configurado, el fichero de configuración del PS se considera auténtico; de lo contrario, DEBE rechazarse el fichero.
5) Si tiene éxito la autenticación, el elemento PS DEBE utilizar el contenido del fichero de configuración del PS para llevar a cabo su propia configuración.

7.3.3.3.2 Algoritmo de autenticación del fichero de configuración para el modo de prestación SNMP

A continuación se indica el procedimiento de autenticación del fichero de configuración del PS por el elemento PS en el modo de prestación SNMP:

1) Cuando el NMS crea un nuevo fichero de configuración del PS o modifica uno existente, el NMS creará un troceo SHA-1 de todo el contenido del fichero de configuración del PS, considerado como una cadena de caracteres.

2) El NMS envía el valor de troceo calculado en el paso 1 al elemento PS mediante un SNMP SET y actualiza el objeto de la MIB cabhPsDevProvConfigHash.

3) El NMS envía el nombre y la posición del fichero de configuración del PS mediante un SNMP SET y actualiza el objeto de la MIB cabhPsDevProvConfigFile (lo que activa la descarga TFTP, véase 7.3.3.2).

4) El elemento PS descarga el fichero nombrado del servidor TFTP configurado.

5) El elemento PS debe calcular el troceo SHA-1 para todo el contenido del fichero de configuración del PS y comparar el troceo calculado con el que contiene el objeto de la MIB cabhPsDevProvConfigHash. Si el valor de troceo calculado y el configurado coinciden, el fichero de configuración del PS se considera auténtico; de lo contrario, DEBE rechazarse el fichero.

6) Cuando ha terminado con éxito la autenticación, el elemento PS DEBE utilizar el contenido del fichero de configuración del PS para su configuración.

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 comunicar el estado

El PS DEBE comunicar el estado de descarga del fichero de configuración y las condiciones de error por medio del proceso de comunicación de eventos descrito en 6.5.

El cuadro 24 identifica los modos de procesamiento que DEBEN manejarse y las acciones que DEBEN emprenderse cuando se detectan estos modos de procesamiento.

Cuadro 24/J.191 – Modos de procesamiento del fichero de configuración del PS

Modo de fallo	Acción
El campo de tipo no es válido	Desechar el TLV en cuestión y comunicar el evento. Continuar procesando el fichero.
Falla la verificación de integridad del fichero (la integridad del fichero sigue pendiente de definición)	Comunicar un evento. No intentar procesar el fichero.
El fichero es demasiado grande	Comunicar un evento. No intentar procesar el fichero.
No se ha encontrado el fichero de configuración	Comunicar un evento. No intentar procesar el fichero.
El fichero no está relleno adecuadamente	Comunicar un evento. No intentar procesar el fichero.
No hay marca de fin de fichero	Comunicar un evento. No intentar procesar el fichero.
Incapaz de establecer el valor	Comunicar el evento, rechazar el fichero de configuración y rearrancar. Retrotraer (a los valores previos al SNMP SET) los valores salvados en memoria no volátil.
Aparece un valor cuyo SNMP OID no se reconoce	Desechar el TLV en cuestión y comunicar el evento. Continuar procesando el fichero.

En el anexo B puede consultarse la lista de eventos, incluidos los del cuadro 24 y la información relativa a su procedimiento de comunicación.

Si se procesan valores de configuración DEBE generarse un evento cuando se detecte el fin de fichero, y este evento DEBE incluir el número de TLV procesados con éxito y el número de TLV omitidas.

Una vez activada la descarga del fichero de configuración del PS, el elemento PS DEBE continuar intentando descargar el fichero de configuración del PS especificado de la dirección especificada hasta que termine con éxito la descarga del fichero de configuración del PS y se logre calcular el troceo descrito en 7.3.3.3. El límite temporal específico para el acceso al servidor TFTP depende de la implementación. No obstante, el PS NO DEBE intentar acceder al servidor TFTP más de tres veces cada cinco minutos. El PS DEBE intentar, al menos una vez cada cinco minutos, la descarga del fichero de configuración del PS hasta que ésta se haya completado con éxito.

El PS DEBE generar el oportuno evento identificado en el anexo B que indique el fallo de la descarga del fichero de configuración del PS cada vez que el PS fracase en su intento de descargar el fichero de configuración del PS.

Si el PS consigue descargar el fichero de configuración del PS, el PS DEBE restaurar el contador de descargas del fichero de configuración del PS a cero y generar el oportuno evento identificado en el anexo B para indicar que se ha conseguido descargar el fichero de configuración del PS.

Si el PS está funcionando en el modo DHCP (indicado por el valor de cabhPsDevProvMode) Y aborta el proceso de descarga del fichero de configuración del PS, el PS DEBE generar el evento identificado en el anexo B para indicar el fallo del proceso de descarga del fichero de configuración del PS Y liberar su dirección IP WAN-Man del PS de acuerdo con [RFC 2131] Y reemitir un DISCOVER de DHCP de conformidad con [RFC 2131], es decir, el PS debe reemprender el proceso de inicialización.

El PS DEBE utilizar un límite temporal adaptable para el TFTP en base a la reducción exponencial binaria descrita en [RFC 1123] y [RFC 2349].

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 en el cuadro 25 permiten obtener las capacidades definidas para el cliente de hora del día del PS:

Cuadro 25/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 PS 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 funciones de mensajería de eventos y de seguridad.

Requisitos del cliente de hora del día

El elemento PS DEBE implementar un cliente de hora del día.

El cliente de hora del día del PS DEBE cumplir el protocolo de hora del día [RFC 868] y utilizar únicamente el protocolo UDP.

Una vez rearrancado, el elemento PS DEBE inicializar su hora a 0 (0:0.0 del 1 de enero de 1900) conforme a lo dispuesto en [RFC 868].

El elemento PS DEBE intentar sincronizar la hora del día con el servidor TOD indicado por la opción 4 del DHCP, que se recibe en el DHCP OFFER enviado a la interfaz WAN-Man.

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 PS 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 de mensajería de eventos y de seguridad, siendo la precisión máxima necesaria la del segundo más próximo.

El elemento PS DEBE continuar sus intentos de comunicarse con el servidor de hora del día, hasta establecer la hora local. El límite temporal específico para las peticiones de hora del día depende de la implementación. No obstante, el cliente de hora del día del PS NO DEBE sobrepasar tres peticiones de TOD cada 5 minutos. El cliente de hora del día del PS DEBE emitir como mínimo una petición de TOD cada 5 minutos, hasta establecer la hora local.

Si el servidor TOD no proporciona una respuesta válida, el PS DEBE proceder del siguiente modo, aunque no necesariamente en el mismo orden:

- otorgar a cabhPsDevTodSyncStatus el valor '2' (acceso fallido a TOD);
- si hay licencias activas en el sector LAN-Trans, como indica un valor no nulo de cabhCdpLanTransCurCount, otorgar a cabhCdpLanAddrCreateTime el valor de la hora actual y a cabhCdpLanAddrExpireTime el valor de cabhCdpLanAddrCreateTime más el valor de cabhCdpServerLeaseTime para cada licencia activa (Hora de expiración = Hora de Creación + Duración de la Licencia);
  - anotar en el registro histórico el fallo y generar un evento normal definido en el anexo B; y
  - continuar los reintentos de comunicación con el servidor TOD hasta tanto se establezca la hora local.

Si el PS consiguiese sincronizar su referencia temporal con el servidor TOD de la red de cable, el PS DEBE otorgar a cabhPsDevTodSyncStatus el valor '1' (sincronizado con éxito la TOD).

Si el valor de cabhPsDevTodSyncStatus es '1', es decir, si ya se ha establecido la hora local, no es necesario que el cliente de hora del día emita una petición TOD.

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 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 del hogar.
- 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.
- La función de tratamiento de paquetes del PS puede entregar tráfico de difusión a todas las interfaces LAN y WAN-Data de modo transparente. No es necesario el estrangulamiento del tráfico de difusión. Se supone que el módem de cable DOCSIS puede filtrar el tráfico IP de difusión.

8.2 Arquitectura

En esta cláusula se describen los conceptos clave de la funcionalidad de tratamiento de paquetes y de traducción de direcciones.

8.2.1 Directrices de diseño del sistema

Véase el cuadro 26.

Cuadro 26/J.191 – Directrices de diseño del sistema de tratamiento de paquetes y de traducción de direcciones

Número	Directrices del diseño del sistema
Pckt Handling 1	Los mecanismos de direccionamiento los controlará el operador y le proporcionarán conocimientos sobre el PS y la accesibilidad al mismo.
Pckt Handling 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).
Pckt Handling 3	Los mecanismos de gestión de tráfico aislarán la red de cable del tráfico generado por las comunicaciones entre entidades pares dentro del hogar, de haberlas.
Pckt Handling 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, *cable address translation*).
- Función transferencia.
- Conmutación de entrega selectiva hacia el origen (USFS, *upstream selective forwarding switch*).

Como muestra la figura 16, 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].

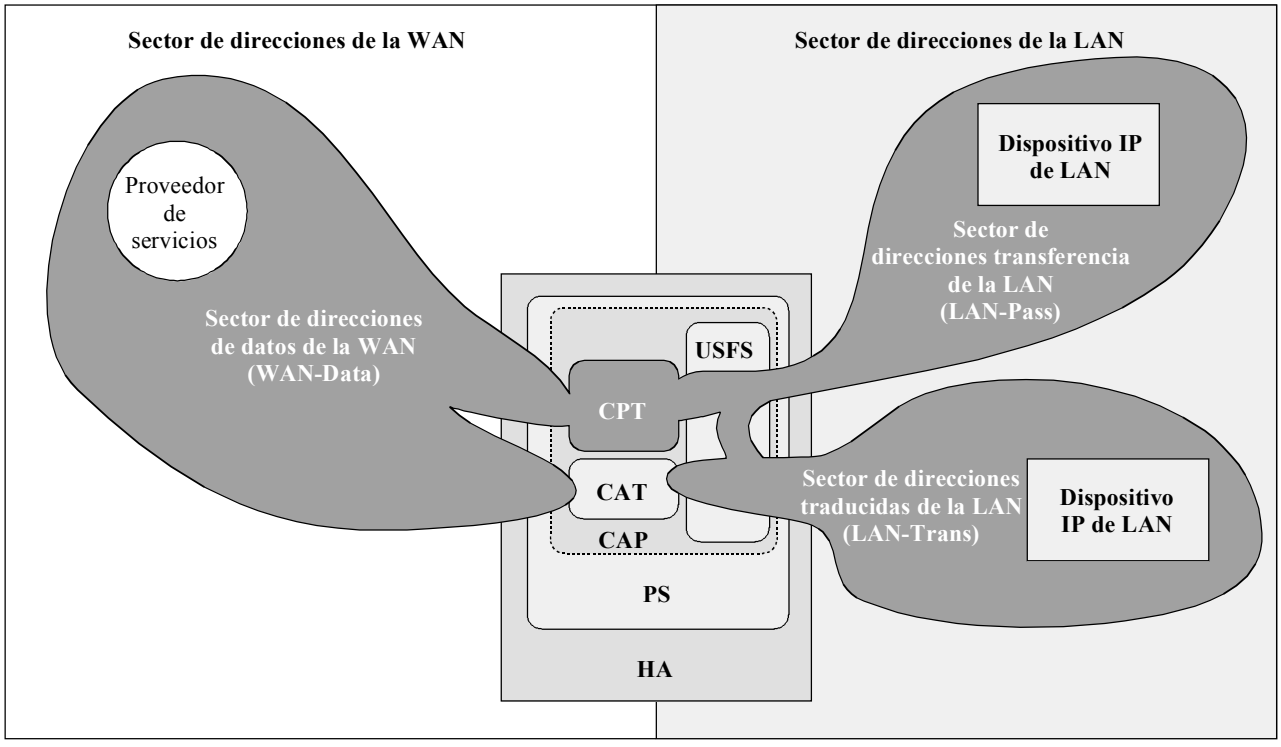


Figura 16/J.191 – Funciones del portal de dirección de cable (CAP)

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 CableHome Pass-through (CPT) 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 del hogar dentro de éste, aunque los dispositivos del hogar 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.

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 PS 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:

1) modo transferencia;
2) modo de encaminamiento transparente C-NAT; y
3) 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 DIS 10038 MAC Bridges] 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).

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 17 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.

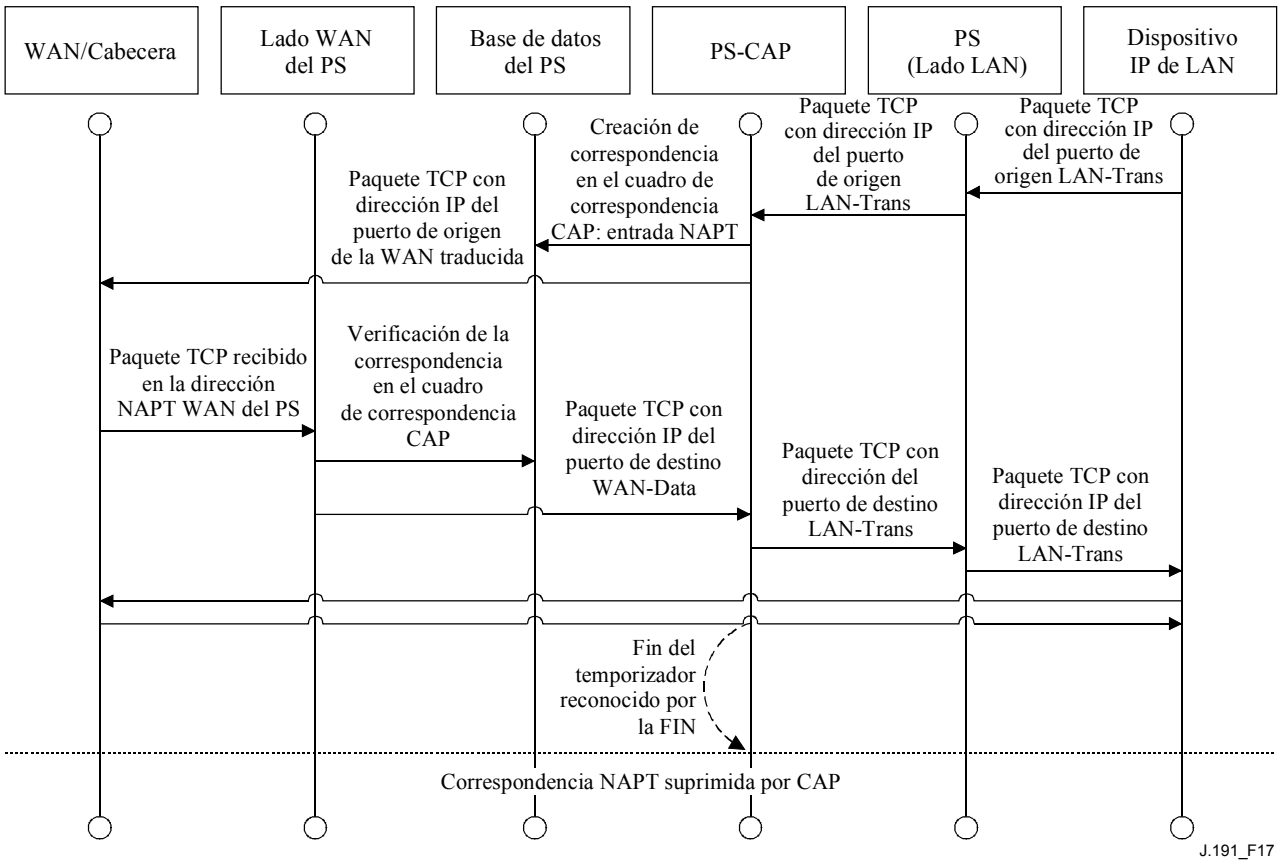


Figura 17/J.191 – Diagrama secuencial de la configuración del PS (cuadro de correspondencia CAP-NAPT)

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.

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 mediante el puenteo transparente de la mensajería IGMP [RFC 2236] y de los paquetes multidifusión IP. 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 las multidifusiones a las 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 18 proporciona un ejemplo detallado de los procesos IGMP y multidifusión atravesando un PS.

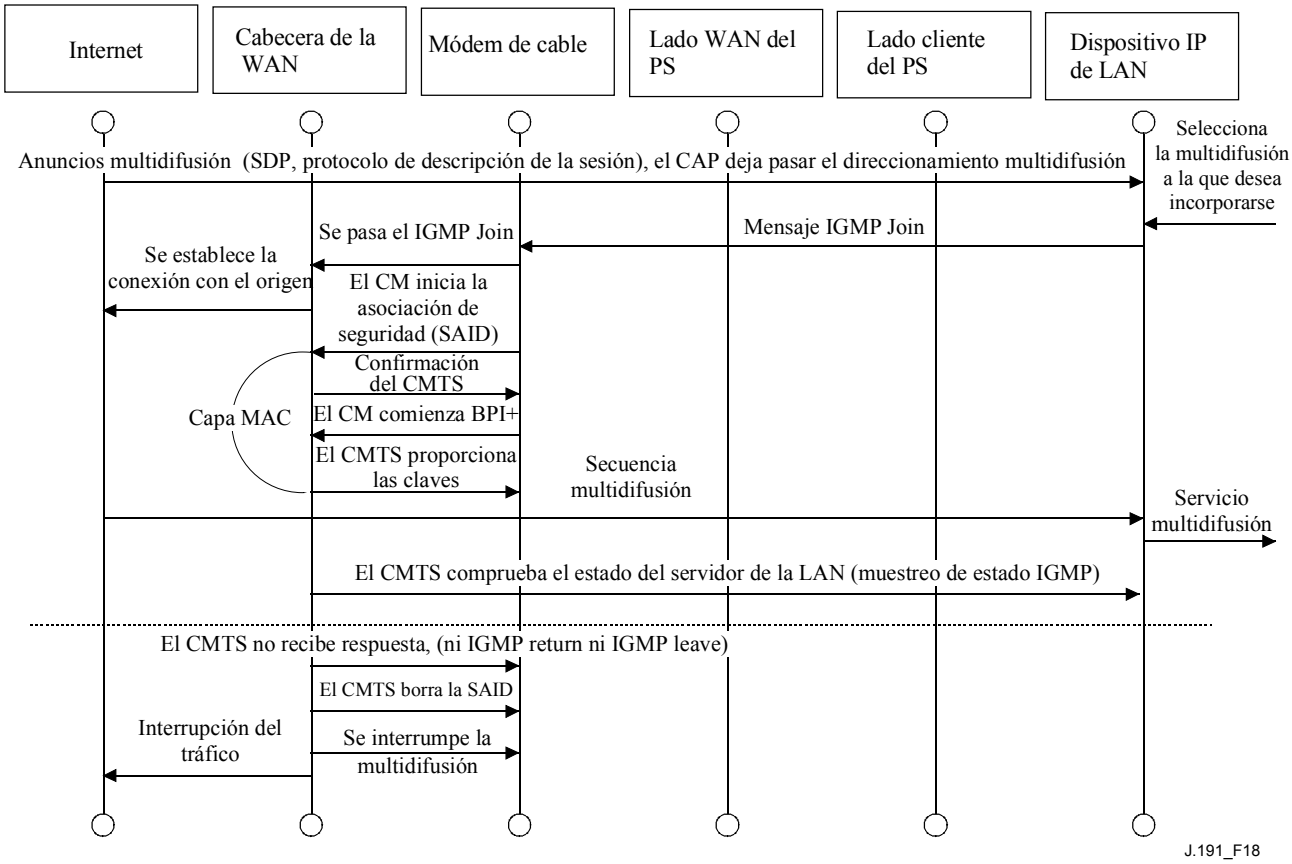


Figura 18/J.191 – Secuencia multidifusión mediante IGMP

8.2.2.5 Ejemplos de tratamiento de paquetes

Esta cláusula pretende informar sobre el proceso del tratamiento de paquetes. La figura 19 muestra un ejemplo de las posibles etapas de procesamiento de paquetes para el tráfico unidifusión LAN-a-WAN, mientras que la figura 20 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.

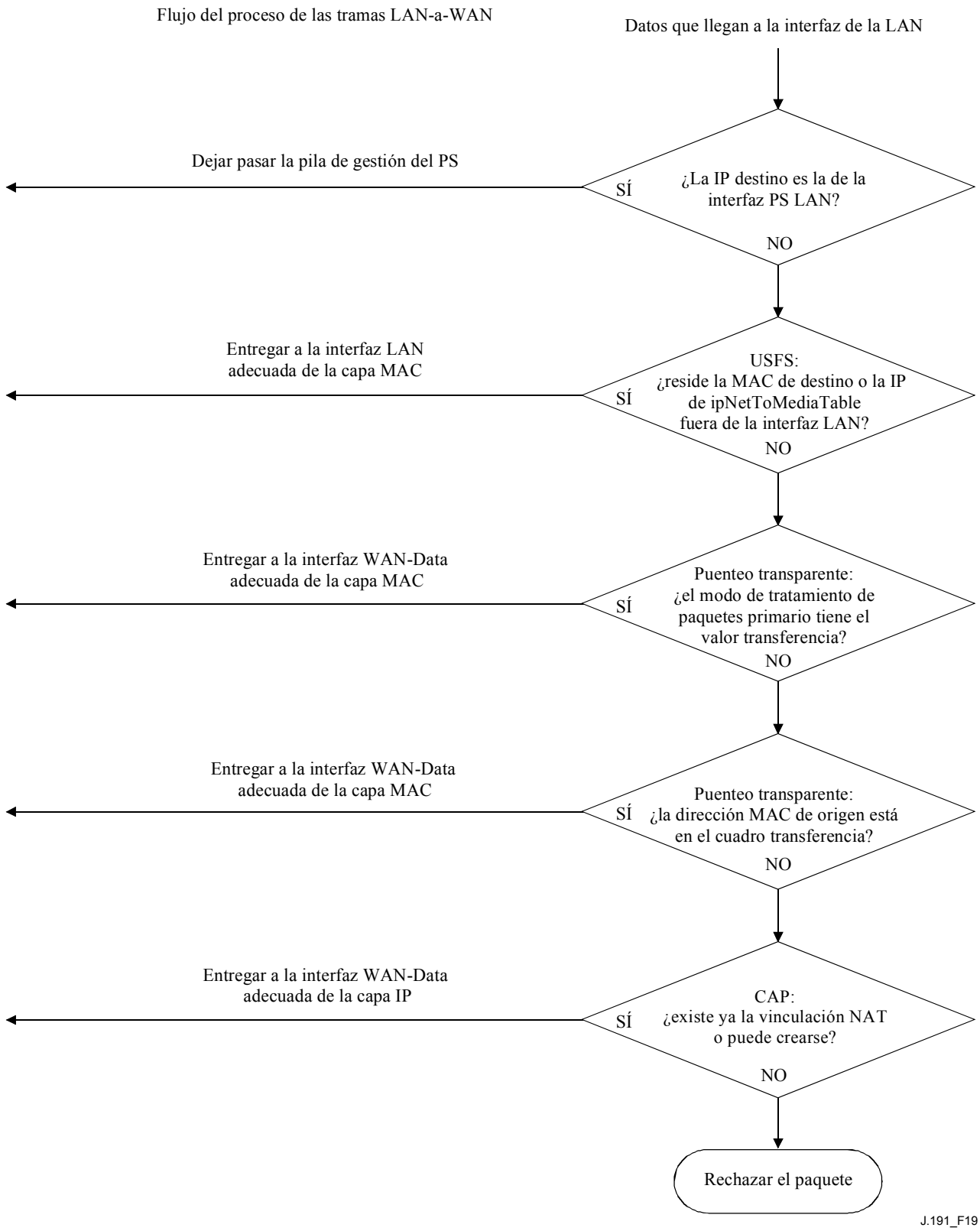


Figura 19/J.191 – Ejemplo de procesamiento de paquetes LAN-a-WAN

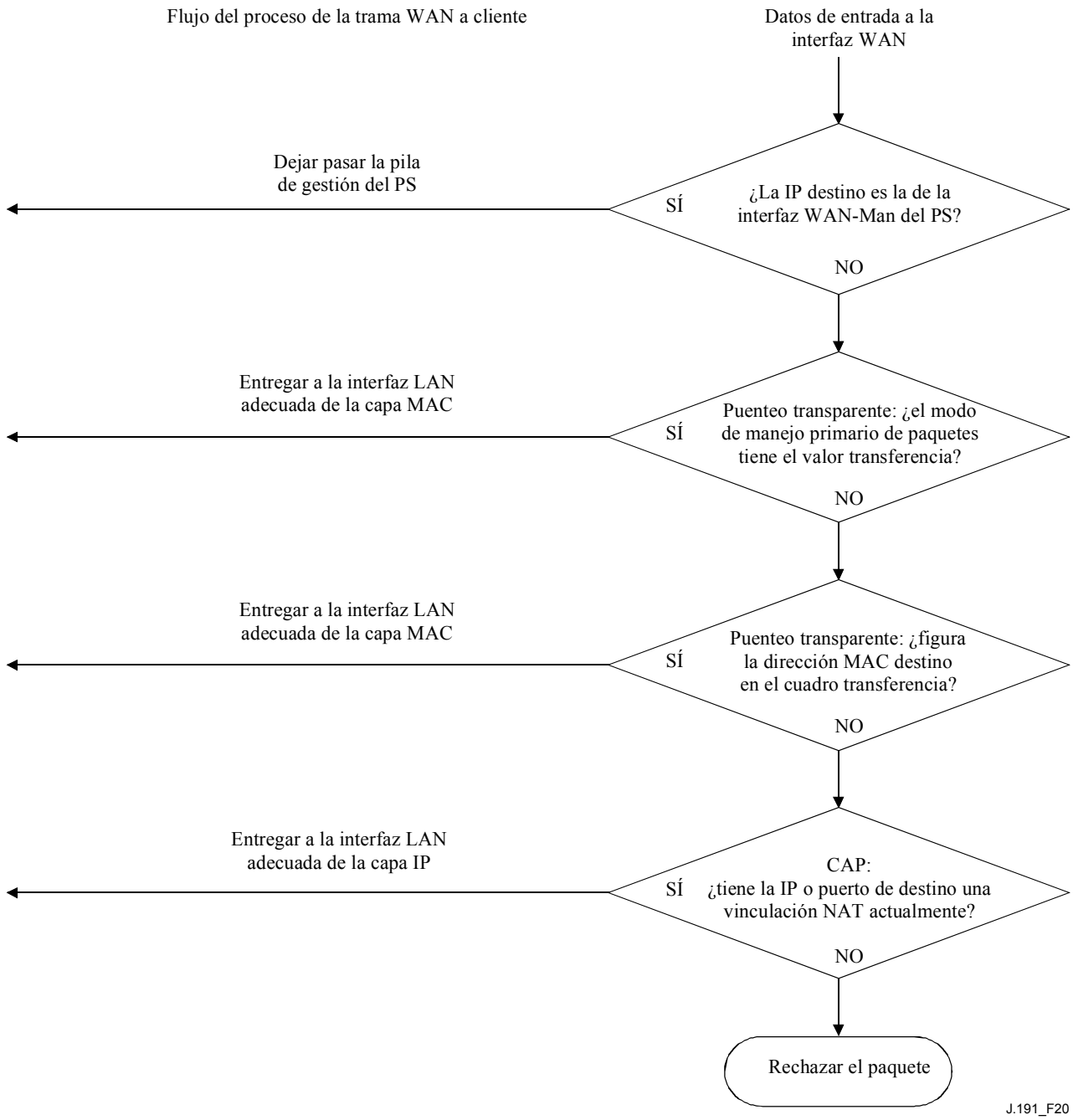


Figura 20/J.191 – Ejemplo de proceso de paquetes WAN-a-LAN

8.3 Requisitos CAP

8.3.1 Requisitos generales

Para poder comunicarse normalmente con los anfitriones de Internet, las interfaces IP lógicas del elemento PS DEBEN ser conformes con las secciones 3 y 4 de [RFC 1122].

El CAP DEBE soportar el tráfico multidifusión mediante el puenteo transparente de la mensajería IGMP y de los paquetes multidifusión IP definidos en [RFC 2236].

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).

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 LAN-a-LAN nunca DEBE encaminarse ni puentearse hacia el exterior de una interfaz WAN.

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 10038], 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 sistema 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.
- Remitir los clientes DNS de la LAN a servidores DNS de cabecera, para la 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

Véase el cuadro 27.

Cuadro 27/J.191 – Directrices de diseño del sistema de resolución de nombres

Referencia	Directriz de diseño del sistema
Name Rsln 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).
Name Rsln 2	Proporcionar referencias DNS a los servidores 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.
- Remite los dispositivos IP de LAN a servidores DNS externos 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 las instalaciones del cliente 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 resuelva un nombre de servidor, ejecuta el proceso de consulta mostrado en la figura 21. El CNP responde a las consultas iniciales DNS normales [RFC 1035], dirigidas a cabhCdpServerDnsAddress, en todas las búsquedas de nombres. Si la respuesta del CNP es una referencia a servidores DNS externos, se supone que es responsabilidad del dispositivo IP de LAN el envío de la consulta directamente al servidor referido.

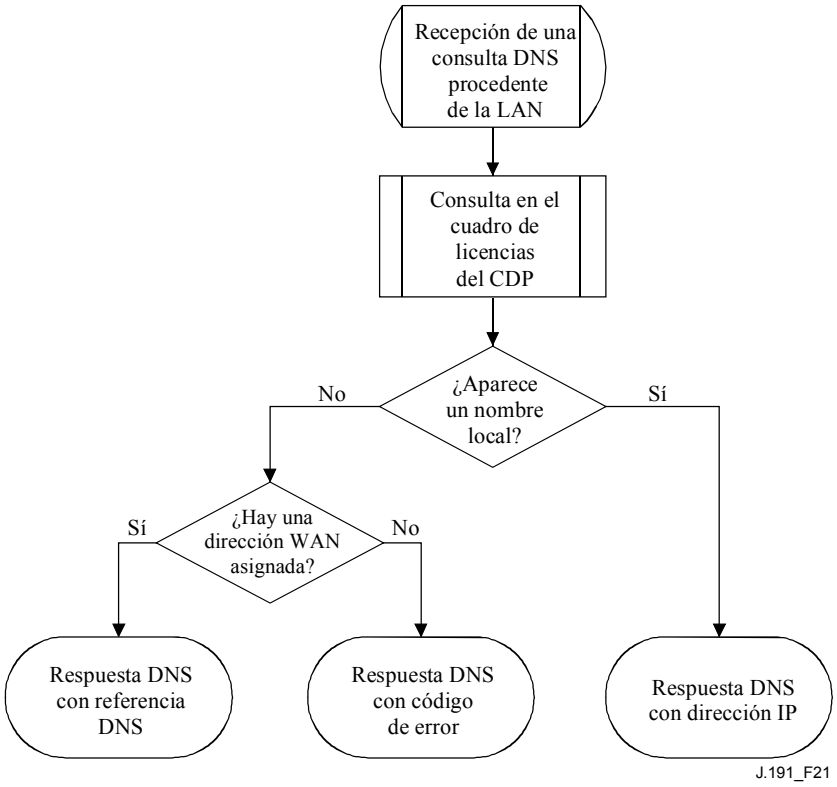


Figura 21/J.191 – Procesamiento de los paquetes del CNP

El CNP se apoya en cabhCdpLanAddrTable del CDP para obtener los nombres de anfitrión asociados a las direcciones IP vigentes en los dispositivos IP de LAN. Mientras un dispositivo IP de LAN mantenga una licencia DHCP activa con el CDP y haya suministrado un nombre de anfitrión al CDP (como parte de su proceso de adquisición de direcciones IP) el CNP puede resolver su nombre. Si el nombre de anfitrión cuya resolución se solicita no aparece en cabhCdpLanAddrTable, el CNP devuelve una referencia DNS que apunta a un servidor DNS externo (que el CDC obtiene a través de las opciones DHCP). La dirección IP del servidor DNS externo es la última entrada cabhCdpWanDataAddrDnsIp del cabhCdpWanDataAddrServerTable del CDP.

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, *authoritative nameserver*) autorizado a petición. En el cuadro 28 se presenta un ejemplo de los campos del registro SOA (véase la sección 3.3.13 de [RFC 1035]):

Cuadro 28/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, 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 funcionar como mínimo en modo no recursivo con arreglo a lo definido en [RFC 1034].

El CNP responde a las consultas sobre nombres utilizando exclusivamente información local del PS, y sus mensajes de respuesta DEBEN contener un error, una respuesta o una referencia a un servidor DNS externo.

El CNP DEBE responder 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 del estado de la entrada cabhCdpWanDataAddrDnsIp de cabhCdpWanDataAddrServerTable 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.

Cuando funciona como servidor DNS no recursivo: si el CNP no pudiera resolver el nombre del anfitrión a partir de datos locales Y la última entrada cabhCdpWanDataAddrDnsIP de cabhCdpWanDataAddrServerTable del CDP está ocupada, el CNP DEBE responder a la consulta de resolución de nombre de anfitrión con una referencia a un servidor DNS externo, representada por la dirección IP contenida en el objeto cabhCdpWanDataAddrDnsIp.

Si el CNP no puede resolver el nombre del anfitrión a partir de datos locales Y el objeto cabhCdpWanDataAddrDnsIp no está ocupado, el CNP DEBE responder a la consulta de resolución de nombre de anfitrión con el oportuno error especificado por [RFC 1035].

Cuando expira la última licencia WAN-Data DHCP vigente, el CDC DEBE suprimir todas las entradas cabhCdpWanDataAddrDnsIp de cabhCdpWanDataAddrServerTable.

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 módem de cable mejorado IP para permitir que las aplicaciones del hogar 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 del hogar 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:

- La QoS supone la existencia de sistemas 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 (CQoS) está integrada por elementos funcionales y por la clase de dispositivo HA. Los diseñadores de equipos de red (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 se relacionan en el cuadro 29.

Cuadro 29/J.191 – Directrices de diseño del sistema QoS

Número	Directrices de diseño del sistema QoS
QoS 1	Existirá un mecanismo de señalización normal QoS que permita a los módems de cable mejorados en IP soportar el establecimiento de sesiones de servicio de diferentes prioridades en la red DOCSIS para aplicaciones multimedios.
QoS 2	Las aplicaciones multimedios pueden estar integradas en el dispositivo HA o en un dispositivo externo conectado al dispositivo HA.
QoS 4	Las aplicaciones multimedios 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 cable (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, *portal service*) 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 el hogar. 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). El CQP se comporta como un portal CQoS para las aplicaciones homologadas con IPCablecom. Su función principal es la entrega de mensajes QoS entre el CMTS y las aplicaciones IPCablecom.

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 22 muestra un ejemplo de las relaciones entre los elementos funcionales CQoS y la clase de dispositivo HA.

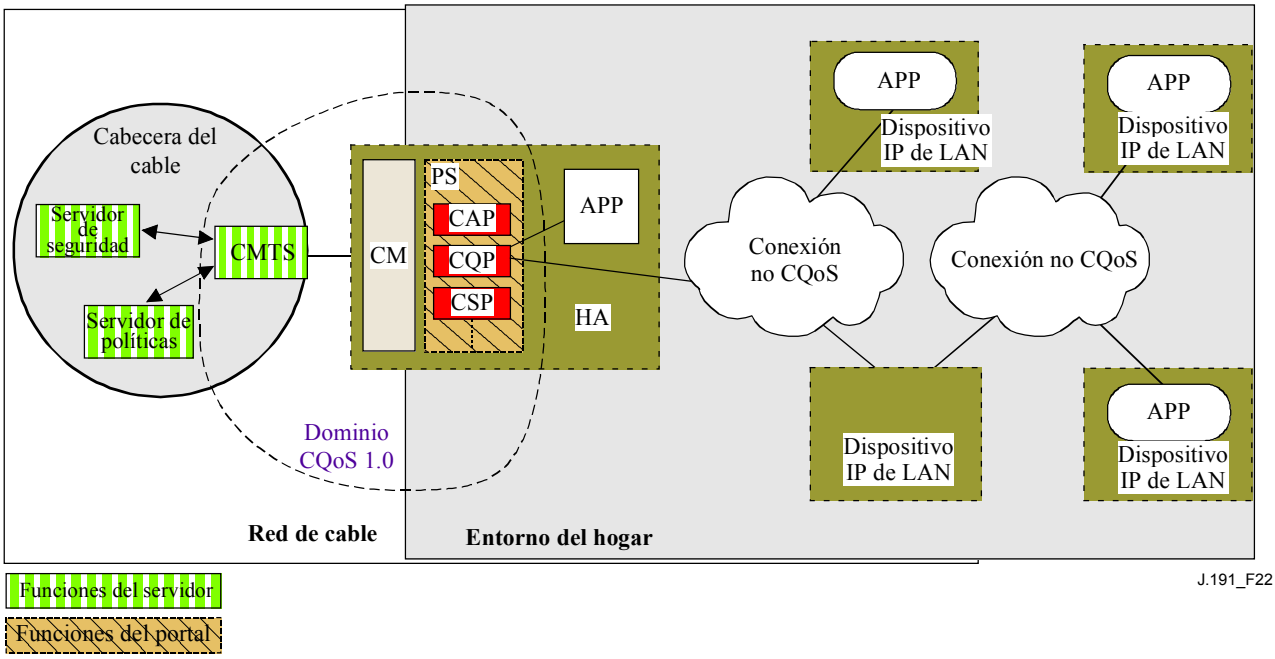


Figura 22/J.191 – Ejemplo de elementos funcionales CQoS

10.3 Requisitos de la mensajería QoS de cable

La arquitectura QoS (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 (Recomendaciones UIT-T 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 prestación DHCP como en el modo de prestación SNMP (véase 5.7).

10.3.2 Gestión de la política del QoS y control de admisión

La mensajería QoS se define en las especificaciones IPCablecom (Recomendaciones UIT-T J.161 y J.163). Por este motivo, las funciones de gestión de políticas del QoS y de control de la admisión 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 PS en un entorno seguro.

Para poder prestar servicios IP multimedios fiables a los dispositivos clientes en el hogar 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 prestación de servicios de valor elevado basados en cable, de modo que sean como mínimo tan seguros como las tecnologías DOCSIS e IPCablecom en la red híbrida fibra-coaxial (HFC).
- Proporcionar mecanismos de seguridad flexibles que sean compatibles con los mecanismos de seguridad DOCSIS e IPCablecom utilizados en la red HFC.

11.1.2 Hipótesis

Entre las hipótesis del entorno de seguridad se encuentran las siguientes:

- Las funcionalidades PS y CM residen en un único dispositivo físico.
- Pueden existir niveles de seguridad inferiores en el hogar 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 del portal de servicio IP (PS), que incluye las funciones de gestión y prestación, 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), el servidor de gestión de la red, el servidor de seguridad, etc.

La especificación de seguridad 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 30. Esta relación proporciona una orientación para el desarrollo de las especificaciones de seguridad.

Cuadro 30/J.191 – Directrices de diseño del sistema de seguridad

Referencia	Directrices de diseño del sistema de seguridad
SEC1	El operador podrá gestionar en remoto 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 prestación 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 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

Las siguientes subcláusulas proporcionan 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 portal de servicio IP (PS).
- Función de portal de seguridad de cable (CSP).
- Barrera contra fuegos (FW).
- Servidor de seguridad.

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 HA.

La figura 23 contiene un ejemplo de la relación entre los distintos elementos de seguridad y las clases de dispositivo HA. En la figura, las aplicaciones del hogar se representan como APP y el servidor OSS es el servidor NMS.

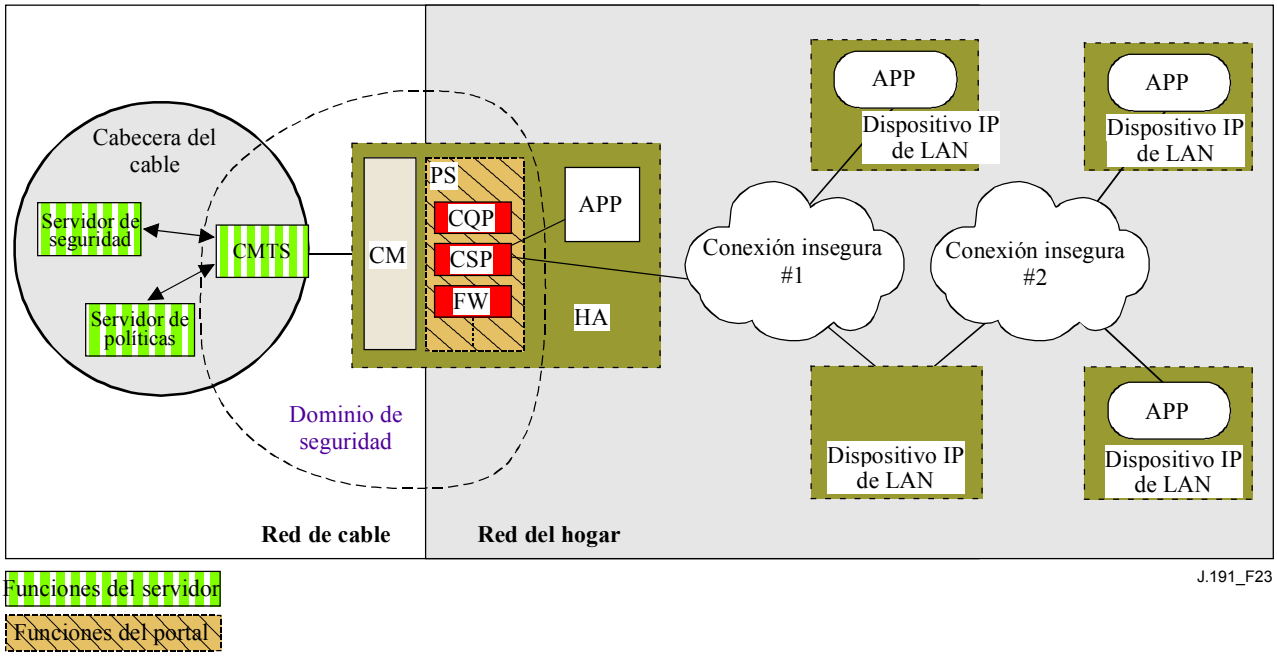


Figura 23/J.191 – Elementos de seguridad

11.2.2.1 El dominio de seguridad

El dominio de seguridad se define en la figura 23 y comprende el elemento PS del HA y los servidores de cabecera que se ilustran.

11.2.2.2 La función PS

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 y LAN. Dicho tráfico puede contener ataques deliberados contra la red del hogar 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 barrera contra fuegos. 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 24 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 24 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) 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.

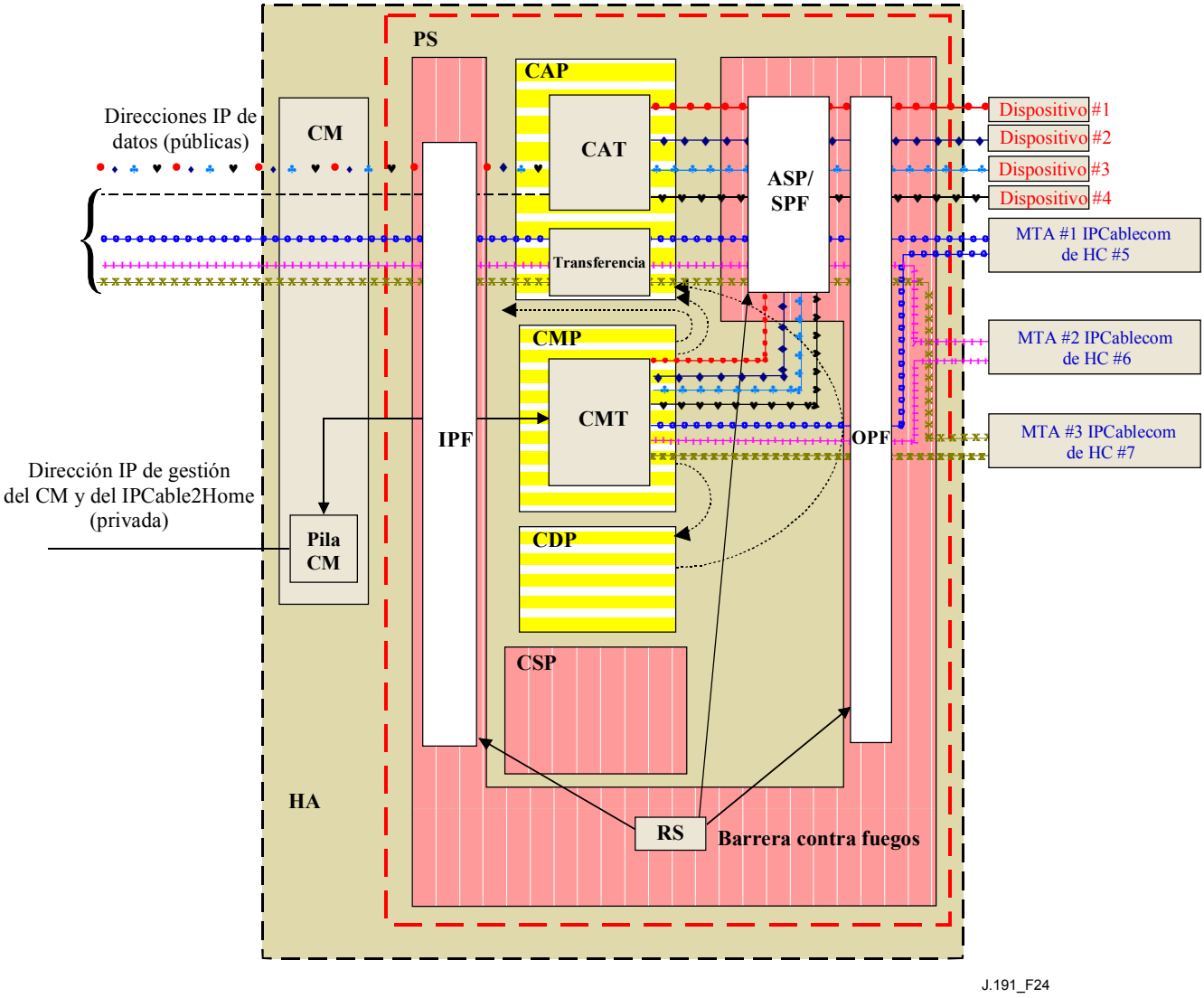


Figura 24/J.191 – Ejemplo de elemento PS de un dispositivo HA

11.2.3 Servidor del centro de distribución de claves (KDC)

El servidor de seguridad soportado se encuentra en el servidor del centro de distribución de claves (KDC, *key distribution center*). Si hay disponible un servidor KDC de soporte 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 (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 (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 2459]. El certificado del elemento PS proporciona la identidad del elemento PS asociado vinculando criptográficamente la dirección MAC del elemento PS a un certificado de clave pública emitido para dicho elemento PS. Además, los certificados de clave pública constituyen un modo seguro de comunicar la información de identidad.

Cuando un KDC que soporte esta aplicación 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 prestación SNMP (descrito en 5.1) 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. Como este modelo de autenticación ya ha sido especificado por 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 prestación 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.

La autenticación otorgada por el KDC DEBE seguir a la especificación para Kerberos/PKINIT definida en [UIT-T J.170]. El KDC es equivalente o idéntico al KDC del operador IPCablecom (IPCablecom especifica la utilización de varios KDC). El elemento PS DEBE comportarse como cliente del KDC. En la Recomendación de seguridad IPCablecom, el MTA es el cliente. Se prevé que las implementaciones utilicen la funcionalidad de cliente especificada para el MTA en relación con el elemento PS. El elemento PS utiliza Kerberos para SNMP. Los certificados utilizados en PKINIT se especifican en 11.3.2. Donde IPCablecom especifica un certificado de dispositivo MTA, esta Recomendación proporciona un certificado para el elemento PS (certificado del elemento PS) y las implementaciones del elemento PS DEBEN incluir el certificado del elemento PS.

La seguridad IPCablecom para la siguiente funcionalidad Kerberos no es aplicable en la presente Recomendación:

1) Gestión de versiones de claves de servicio (véase 6.4.10/J.170);
2) Funcionamiento entre sectores Kerberos (véase 6.4.11/J.170);
3) Mensajes de reutilización de clave (véase 6.5.4/J.170);
4) IPsec Kerberizado (véase 6.5.6/J.170);
5) Posiciones del servidor Kerberos y convenios de denominación (véase 6.4.6.3, CMS).

11.3.1.2 Variables de autenticación específicas

Las especificaciones del modelo IPCablecom especifican 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.
- Sustituir MTA-FQDN-Map definido en la Especificación de seguridad IPCablecom por FQDN-Map.

Las implementaciones de Kerberos DEBEN ignorar la porción de campo del identificador de objeto (OID), que introduce el valor de clabProjPacketCable (2) en AppSpecificTypedData en los mensajes KRB-ERROR.

11.3.2 Infraestructura de claves públicas (PKI)

La presente Recomendación utiliza certificados de claves públicas que cumplen la Rec. UIT-T X.509 y la [RFC 3280] de IETF.

11.3.2.1 Estructura genérica

11.3.2.1.1 Versión

La versión de los certificados DEBE ser 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 F4 – 65537.

11.3.2.1.3 Extensiones

Las extensiones (subjectKeyIdentifier, authorityKeyIdentifier, KeyUsage, BasicConstraints, Signature Algorithm, SubjectName e IssuerName) 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]).

11.3.2.1.3.3 KeyUsage

La extensión keyUsage DEBE utilizarse para todos los certificados de la autoridad de certificación (CA, *certification authority*) y certificados de verificación de código (CVC). 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 la inscripción de certificados (cuadros 31 a 42).

11.3.2.1.4 Algoritmo de firma

El mecanismo de firma utilizado DEBE ser SHA-1 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.

11.3.2.2 Jerarquías de los certificados

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 son genéricas por su propia naturaleza y aptas para todas las aplicaciones que necesitan certificados. Esto significa que la infraestructura básica puede reutilizarse en cada una de las aplicaciones (DOCSIS, IPCablecom y PS). 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 puede utilizarse para soportar el solapamiento. Por ejemplo, IPCablecom requiere un KDC para el proveedor de servicios y la presente Recomendación puede aprovechar un KDC que soporte IPCablecom para proporcionar la autenticación recíproca. Si el proveedor de servicios tiene instalada ambas arquitecturas de red en sus sistemas, pueden utilizar el mismo KDC y el mismo certificado KDC para la comunicación en ambos sistemas, es decir, IPCablecom y esta aplicación. En este caso, el KDC de esta aplicación es equivalente o idéntico al KDC del operador IPCablecom (IPCablecom especifica la utilización de varios KDC).

En la figura 25, el término "autoridad del certificado" se abrevia por CA y el "certificado de verificación de códigos" se abrevia por CVC.

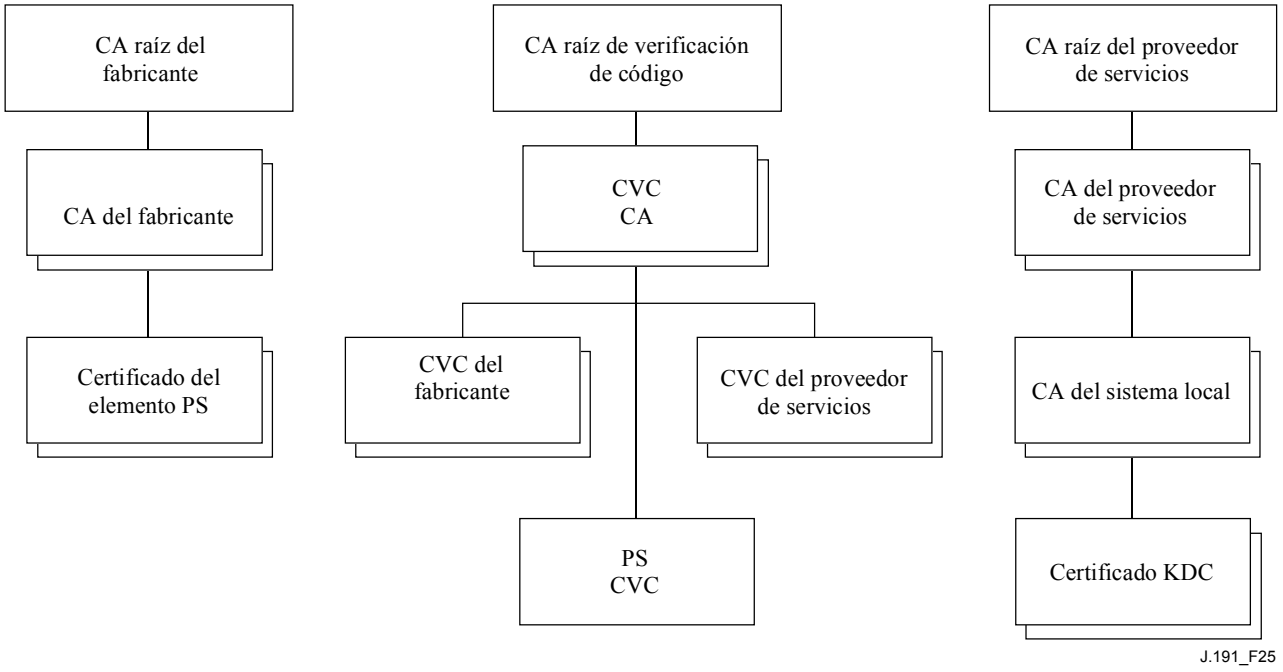


Figura 25/J.191 – Jerarquía de los certificados

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 31 a 33. 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 11.3.2, (PKI).

11.3.2.2.1.1 Certificado CA raíz del fabricante

El certificado CA raíz del fabricante (véase el cuadro 31) 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 31/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. Se prevé que el periodo de validez sea lo suficientemente largo como para que no haya que reemitir el certificado
Longitud del módulo	2048
Extensiones	keyUsage [c, m] (keyCertSign, cRL Sign), subjectkeyidentifier, basicConstraints [c, m](cA = true)

11.3.2.2.1.2 Certificado CA del fabricante

El certificado CA del fabricante (véase el cuadro 32) 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 32/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.

Cuadro 32/J.191 – Certificado CA del fabricante

Firmado por	CA raíz de fabricante
Periodo de validez	20 años
Longitud del módulo	2048
Extensiones	keyUsage[c, m](keyCertSign, cRLSign), subjectKeyIdentifier, authorityKeyIdentifier basicConstraints[c, m](cA = true, pathLenConstraint = 0)

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. Si existe, el authorityKeyIdentifier del certificado del elemento PS DEBE confrontarse con el subjectKeyIdentifier del certificado del fabricante descrito en [RFC 3280].

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 y planta del fabricante son atributos opcionales.

La dirección MAC 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 del dispositivo en cuestión (véase el cuadro 33).

Cuadro 33/J.191 – Certificado del dispositivo

Forma del nombre del sujeto	C = <país>, O = <nombre de la empresa>, [S = <Estado/provincia>,] [L = <ciudad>], OU = [OU = <nombre de producto>,] [OU = <planta del fabricante>,] CN = <dirección MAC>
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	20 años
Longitud del módulo	2048
Extensiones	keyUsage[n, o](digitalSignature, keyEncipherment), authorityKeyIdentifier, La extensión keyUsage es opcional. Cuando se utiliza la extensión keyUsage DEBERÍA marcarse como no crítica.

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 34 a 38 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 11.3.2 (PKI).

11.3.2.2.2.1 Certificado CA raíz de verificación de código

Este certificado (véase el cuadro 34) 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 34/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. Se prevé que el periodo de validez sea lo suficientemente largo como para no tener que volver a emitir ese certificado.
Longitud del módulo	2048
Extensiones	keyUsage [c, m] (keyCertSign, cRL Sign), subjectkeyidentifier, basicConstraints [c, m](cA = true, pathLenConstraint = 0)

11.3.2.2.2.2 Certificado CA de verificación de código

El certificado CA de verificación de código (véase el cuadro 35) 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. PUEDE haber más de un CA de verificación de código.

Cuadro 35/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 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, authorityKeyIdentifier, basicConstraints [c, m](cA = true, pathLenConstraint = 0)

11.3.2.2.2.3 Certificado de verificación de código del fabricante

Este certificado DEBE (véase el cuadro 36) 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 36/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.
Firmado por	CA de verificación de código
Periodo de validez	2 años
Longitud del módulo	2048
Extensiones	keyUsage[c, m](digitalSignature, keyEncipherment), authorityKeyIdentifier

11.3.2.2.2.4 Certificado de verificación de código

El certificado de verificación de código (véase el cuadro 37) 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 37/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 raíz de verificación de código
Periodo de validez	2 años
Longitud del módulo	2048
Extensiones	keyUsage[c, m](digitalSignature, keyEncipherment), authorityKeyIdentifier

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 (véase el cuadro 38) 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 38/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> Service Provider 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.
Firmado por	CA raíz de verificación de código
Periodo de validez	2 años
Longitud del módulo	2048
Extensiones	keyUsage[c, m](digitalSignature, keyEncipherment), authorityKeyIdentifier

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 39 a 42, 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 11.3.2 (PKI).

11.3.2.2.3.1 Certificado CA raíz del proveedor de servicios

Este certificado (véase el cuadro 39) 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 39/J.191 – Certificado CA raíz del proveedor de servicios

Forma del nombre del sujeto	C = <país>, O = , CN = Service Provider Root CA
Uso previsto	Este certificado se utiliza para expedir certificados CA del proveedor de servicios.
Firmado por	Autofirmado
Periodo de validez	Superior a 20 años. Se prevé que el periodo de validez sea lo suficientemente largo como para no tener que volver a emitir el certificado.
Longitud del módulo	2048
Extensiones	keyUsage [c, m] (keyCertSign, cRL Sign), subjectkeyidentifier, basicConstraints [c, m](cA = true)

11.3.2.2.3.2 Certificado CA del proveedor de servicios

El certificado CA del proveedor de servicios (véase el cuadro 40) 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 40/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> Service Provider CA
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 aplicación, 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.

Cuadro 40/J.191 – Certificado CA del proveedor de servicios

	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, authorityKeyIdentifier, basicConstraints[c, m](cA = true, pathLenConstraint = 1)

11.3.2.2.3.3 Certificado CA del sistema local

Este certificado (véase el cuadro 41) 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 41/J.191 – Certificado CA del sistema local

Forma del nombre del sujeto	C = <país>, O = <nombre de la empresa>, CN = <nombre de la empresa> Local System CA
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	2048
Extensiones	keyUsage[c, m](keyCertSign, cRLSign), subjectKeyIdentifier, authorityKeyIdentifier, basicConstraints[c, m](cA = true, pathLenConstraint = 0)

11.3.2.2.3.4 Certificado KDC

Este certificado (véase el cuadro 42) 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 indica la especificación de seguridad IPCablecom, en "Certificado del centro de distribución de claves".

Cuadro 42/J.191 – Certificado KDC

Forma del nombre del sujeto	C = <país>, O = <nombre de la empresa>, [OU = <nombre del sistema local>,] OU = <KDC>, CN = <dirección IP del servidor KDC>
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	2048
Extensiones	keyUsage[n, o](digitalSignature, keyEncipherment), authorityKeyIdentifier, La extensión keyUsage es opcional. Cuando se utiliza DEBERÍA marcarse como no crítica. subjectAltName [n, m] (véase la especificación de seguridad IPCablecom).

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. Esta seguridad 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, Descarga segura de soporte lógico.

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 es ajena al alcance de esta Recomendación.

11.3.3 Mensajería de gestión segura

El algoritmo de seguridad utilizado para inicializar la mensajería de gestión SNMP depende del modo de prestación del elemento PS (véase 5.7). Hay dos tipos de modo de prestación: el modo de prestación DHCP y el modo de prestación SNMP. El modo de prestación DHCP tiene submodos adicionales que identifican si está configurado para el modo NmAccess o para el modo de coexistencia. El modo de prestación 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 prestación 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 prestación DHCP

El modo de prestación 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 prestación 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 prestación 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 2574]. La autenticación SNMPv3 DEBE estar activa en todo momento y PUEDE utilizarse asimismo la privacidad SNMPv3.

A fin de establecer las claves SNMPv3 un CM de PS homologado DEBE soportar la "SNMPv3 Initialization" descrita a continuación.

NOTA – En el contexto del apéndice A de RFC-2574 y del apéndice A de RFC-2575, se designa la posición de seguridad del módem de cable como "very-secure". Esto quiere decir que las entradas por defecto usmUser y vacmAccess definidas en el apéndice A de RFC-2574 y en el apéndice A de RFC-2575 NO DEBEN aparecer.

1) Para cada uno de los distintos nombres de seguridad, con un máximo de 5, el gestor genera un par de números:
   a) el gestor genera un número aleatorio Rm;
   b) el gestor utiliza la ecuación DH para traducir Rm a un número público z:

      $$z = g \text{ ^ } Rm \text{ MOD } p$$

      donde g procede del conjunto de parámetros Diffie-Hellman y p es primo de dichos parámetros.
2) El fichero de configuración CM se crea para incluir el par (nombre de seguridad, número público) y el CM DEBE soportar un número mínimo de 5 pares. Por ejemplo:

   TLV type 34.1 (SnmpV3 Kickstart Security Name) = docsisManager

   TLV type 34.2 (SnmpV3 Kickstart Public Number) = z

Durante el proceso de arranque del CM, los anteriores valores (nombre de seguridad, número público) se rellena (o DEBEN rellenarse) en usmDHKickstartTable.

En este momento:

```
usmDHKickstartMgrpublic.1 = "z"  (cadena de octeto)
usmDHKickstartSecurityName.1 = "docsisManager"
```

Cuando se otorga a usmDHKickstartMgrpublic.n un valor válido durante el registro, se crea la correspondiente fila en usmUserTable con los siguientes valores:

```
usmUserEngineID: localEngineID
usmUserName: valor usmDHKickstartSecurityName.n
usmuserSecurityName: valor usmDHKickstartSecurityName.n
usmUserCloneForm: ZeroDotZero
usmUserAuthProtocol: usmHMACMD5AuthProtocol
usmuserAuthKeyChange: se obtiene del valor fijado
usmUserOwnAuthKeyChange: se obtiene del valor fijado
usmUserPrivProtocol: usmDESPrivProtocol
usmUserPrivKeyChange: se obtiene del valor fijado
usmUserOwnPrivKeyChange: se obtiene del valor fijado
usmUserPublic: ""
usmUserStorageType: permanente
usmUserStatus: activo
```

NOTA – En las entradas dhKickstart (CM) de usmUserTable, permanente quiere decir que DEBE escribirse pero no suprimirse y que no se conserva en los rearranques.

Una vez registrado el CM con el AN:

– El CM genera un número aleatorio xa para cada fila rellena de usmDHKickstartTable que tenga un usmDHKickstartSecurityName y usmDHKickstartMgrPublic de longitud no nulas.

– El CM utiliza la ecuación DH para traducir xa a un número público c (para cada una de las filas identificadas anteriormente):

$$c = g \text{ ^ } xa \text{ MOD } p$$

donde g pertenece al conjunto de parámetros Diffie-Hellman y p es el primo de dichos parámetros.

En este momento:

```
usmDHKickstartMyPublic.1 = "c" (cadena de octeto)
usmDHKickstartMgrPublic.1 = "z" (cadena de octeto)
usmDHKickstartSecurityName.1 = "docsisManager"
```

3) El CM calcula el secreto compartido sk como sk = z ^xa mod p.

4) El CM utiliza sk para obtener la clave de privacidad y el cable de autenticación para cada una de las filas de usmDHKickstartTable y otorga valores a usmUserTable.

De acuerdo con lo especificado en RFC 2786, la clave de privacidad y la clave de autenticación para el nombre de usuario asociado, "docsisManager" en este caso, se obtiene a partir de sk por aplicación de la función de derivación de clave PBKDF2 definida en PKCS#5v2.0.

```
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 CM ya ha completado el proceso de inicialización SNMPv3 y DEBE otorgar el oportuno nivel de acceso a un securityName válido con la clave de autenticación y/o clave de privacidad correcta.

Un CM homologado DEBE rellenar adecuadamente las claves de los cuadros correspondientes especificados por los RFC relativos a SNMPv3 y por RFC 2786.

5) A continuación se describe el proceso utilizado por el gestor para obtener la clave de autenticación y clave de privacidad únicas del CM.

El gestor SNMP accede al contenido de usmDHKickstartTable utilizando el nombre de seguridad 'dhKickstart' sin autenticación.

El CM homologado DEBE proporcionar entradas preinstaladas en el cuadro USM y en los cuadros VACM para crear correctamente el 'dhKickstart' de usuario de nivel de seguridad noAuthnoPriv que tenga acceso de sólo lectura al grupo del sistema y al usmDHkickstartTable.

El gestor SNMP obtiene el valor del número usmDHKickstartMypublic del CM asociado al nombre de seguridad para el que el gestor desea obtener las claves de autenticación y de privacidad. Una vez conocido por el gestor el número aleatorio privado, puede calcular el secreto compartido DH. A partir de dicho secreto compartido, el gestor puede obtener las

claves operativas de autenticación y confidencialidad para el nombre de seguridad que el gestor va a utilizar en su comunicación con el CM.

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 de la especificación de la interfaz de radio frecuencia DOCSIS, e implementar el mecanismo de modificación de claves especificado en [RFC 2786] que incluye el objeto de la MIB usmDHKickstartTable.

11.3.3.2 Algoritmos de seguridad para SNMPv3 en el modo de prestación SNMP

Si el elemento PS se provee en el modo de prestación SNMP, la gestión de red basada en SNMP del interior del elemento PS DEBE funcionar con SNMPv3 con la seguridad especificada por [RFC 2574]. 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 DEBEN utilizar la gestión de claves SNMPv3 kerberizada, especificada en 11.3.3.2.3.

11.3.3.2.1 Algoritmos de criptación SNMPv3

Los identificadores de transformación de criptación que vaya a utilizar la gestión de claves kerberizada para negociar un algoritmo de criptación a utilizar en SNMPv3 son idénticos a los definidos en 6.3.1/J.170.

11.3.3.2.2 Algoritmos de autenticación SNMPv3

Los identificadores de transformación de autenticación que haya de utilizar la gestión de claves kerberizada para negociar un algoritmo de autenticación de mensajes para utilizar en SNMPv3 son idénticos a los definidos en 6.3.2/J.170.

11.3.3.2.3 SNMPv3 kerberizada

El perfil de gestión de claves kerberizadas específico para SNMPv3 coincide con el perfil 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 [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 2571], es decir, el primer bit se pone a 1 (uno) y se utiliza el valor adecuado para los primeros cuatro bytes [RFC 2571];
- 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 2571]. 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 2571].

11.3.3.2.5 Relleno de usmUserTable

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, DEBE introducirse la información de usuario necesaria en usmUserTable [RFC 2574] 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.

El valor XXXXXX será la dirección MAC de elemento 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 es necesario que los mensajes IPCablecom, que ya han sido asegurados por IPCablecom, puedan atravesar la barrera contra fuegos del PS. No es objeto de la presente Recomendación la adición de seguridad a los mensajes IPCablecom. Como 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 prestación DHCP y en el modo de prestación SNMP (véase 5.7).

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 PS. Véase la cláusula 10. El elemento CQP actúa como puente transparente para la mensajería CQoS entre las aplicaciones homologadas IPCablecom y el CMTS. La barrera contra fuegos tendrá que dejar pasar la seguridad homologada IPCablecom y la mensajería QoS.

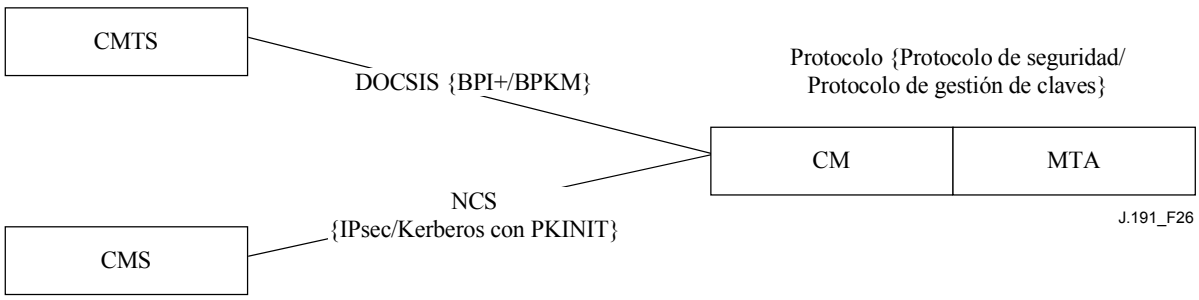
Véase en la cláusula 10 una exposición más detallada sobre la CQoS.

11.3.4.2 Arquitectura DQoS con seguridad IPCablecom

Esta cláusula describe la arquitectura DQoS con seguridad IPCablecom a fin de exponer la interacción de estos mensajes con la barrera contra fuegos del PS. Dentro de la DQoS, el adaptador del terminal multimedios (MTA, *multimedia terminal adaptor*) se comunica con el CMTS y con el servidor de gestión de llamadas (CMS, *call management server*) para establecer la QoS necesaria para sus servicios IPCablecom. El MTA está integrado en el CM DOCSIS. A continuación se presenta un cuadro (cuadro 43) y el diagrama (figura 26) de los dispositivos, el protocolo de comunicación y el protocolo de seguridad correspondientes a la DQoS.

Cuadro 43/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+

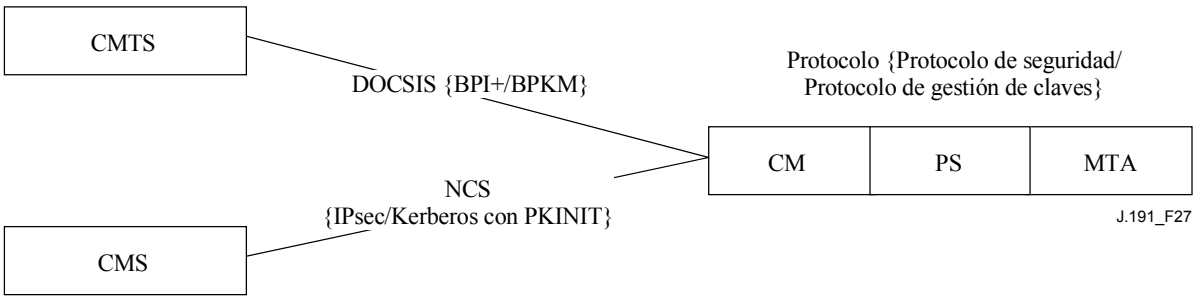


Comunicaciones DQoS E-MTA

Figura 26/J.191 – Arquitectura DQoS segura en el MTA

11.3.4.3 Arquitectura de seguridad del CQoS

El CQoS requiere la mensajería DQoS de IPCablecom [UIT-T J.163]. Toda la mensajería CQoS DEBE asegurarse conforme a lo descrito en la especificación de seguridad IPCablecom. La figura 27 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.



Comunicaciones CQoS E-CM-IPSP-MTA

Figura 27/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 PS en esta arquitectura; 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, *cable modem*) 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".

– "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".

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 romper IPCablecom (véase el cuadro 44) ni los protocolos 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 44/J.191 – Recomendaciones IPCablecom pertinentes para la barrera contra fuegos

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.cmss

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 la aplicación 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 del hogar. 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 nuestros efectos, 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 remota del conjunto de reglas de la barrera contra fuegos

Se activarán características en el elemento PS para permitir que el operador gestione en remoto 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. Para autenticar la descarga del fichero del conjunto de reglas, DEBE utilizarse el algoritmo de autenticación definido en 7.3.3.3.2 junto con los correspondientes parámetros de troceo y nombre de fichero definidos en 11.3.5.2 a continuación.

Mediante la interfaz de gestión de la MIB de seguridad, el operador configura los parámetros del fichero del conjunto de reglas de la política de seguridad relacionados en 11.3.5.2 y ejecuta, a continuación, el procedimiento definido en 7.3.3.3.2 para descargar y autenticar el fichero. Si la descarga llega a buen término, DEBE "activarse" en la barrera contra fuegos el fichero del conjunto de reglas de la política de seguridad. Si fracasa la autenticación, DEBE rechazarse el conjunto de reglas de política.

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 de acuerdo con lo definido por 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 contiene el fichero del conjunto de reglas de política, en formato TFTP URL. Una vez actualizado el objeto cabhSecFwPolicyFileURL DEBE activar la descarga del fichero. El PS DEBE utilizar un cliente TFTP que cumpla [RFC 1350] para descargar el fichero de configuración de la barrera contra fuegos.
- **cabhSecFwPolicyFileHash** – Define el compendio SHA-1 para el correspondiente fichero del conjunto de reglas.
- **cabhSecFwPolicyFileOperStatus** – InProgress(1) indica que esta descargándose un fichero de conjunto de reglas, ya sea como resultado de una discordancia de la versión proporcionada o como resultado de una petición upgradeFromMgt. CompleteFromProvisioning(2) indica que la última actualización del fichero del conjunto de reglas se efectuó como resultado de una discordancia de la versión proporcionada. CompleteFromMgt(3) indica que la última actualización del fichero del conjunto de reglas fue el resultado de otorgar al objeto FirewallPolicyFileAdminStatus el valor upgradeFromMgt. Failed(4) indica que el último intento de descarga fue fallido, lo que normalmente se debe al agotamiento del límite temporal TFTP.
- **cabhSecFwPolicyFileCurrentVersion** – Versión del fichero del conjunto de reglas que está funcionando actualmente en el elemento PS. Este objeto debe tener la sintaxis utilizada por el fabricante en cuestión para identificar las versiones de ficheros de conjuntos de reglas. Cualquier elemento PS DEBE devolver una cadena que describa la carga actual del fichero del conjunto de reglas. Si esto no fuera aplicable, 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 la política activa de la barrera contra fuegos o a los parámetros de configuración de la barrera contra fuegos.

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 11.3.5.2.

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. Este campo de prioridad de eventos DEBE tener prioridad 6 para los eventos de la barrera contra fuegos tipos 1, 2 y 3. 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 días). 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 días 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.
- **cabhSecFwEventType2Enable** – Activa o desactiva el registro histórico de los mensajes de eventos de la barrera contra fuegos del tipo 2.
- **cabhSecFwEventType3Enable** – Activa o desactiva el registro histórico de los mensajes de eventos de la barrera contra fuegos del tipo 3.
- **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 con el nivel de prioridad 4.
- **cabhSecFwEventAttackAlertPeriod** – Indica el periodo a utilizar en días anteriores para el objeto cabhSecFwEventAttackAlertThreshold.

11.3.6 Las MIB

El PS DEBE soportar las siguientes MIB de soporte a la descarga de soporte lógico definidas en la [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 DEBE soportar las MIB de soporte a la descarga de soporte lógico definidas en la Rec. UIT-T J.112, anexo B.O:

- **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 [RSA1].
  - **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 DEBE soportar la siguiente MIB de soporte de descarga de configuración:

- **cabhPsDevProvConfigHash** – Troceado SHA-1 de todo el contenido del fichero de configuración, considerado como una cadena de bytes.

11.3.7 Descarga segura de soporte lógico

El elemento PS de un dispositivo DEBE poder descargar remotamente una imagen de soporte lógico por la red. 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 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.
  - 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 Recomendación 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 o PS) 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 como se define en 11.3.7.2.1.1 y en 11.3.7.3 respectivamente.

– (Opcional): El elemento PS DEBERÍA poder actualizar la clave pública CA de raíz CVC almacenada 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.

La descarga opcional de la clave pública CA de raíz CVC, del certificado CA CVC y/o del certificado CA del fabricante como parte del fichero de código permite la discriminación sin lugar a dudas de la imagen de código respecto de otros parámetros del fichero de descarga de código. Permite también modificar la clave pública CVC de raíz, el certificado CA CVC, los certificados CA del fabricante y los parámetros SignedData del fichero de descarga de código sin perturbar ni modificar la imagen de código que el elemento PS ha de recibir. Esto hace posible que el elemento PS verifique que no se ha alterando la imagen de código aunque el fichero de descarga de código se haya modificado por motivo del cambio de la clave publica CA de la raíz CVC, del certificado CA CVC, de los certificados CA del fabricante o de los parámetros SignedData.

11.3.7.1 Descarga de soporte lógico en los elementos PS

Como el elemento PS está integrado en el módem de cable, la imagen PS/CM DEBE ser una única imagen y la descarga de soporte lógico DEBE ser efectuada únicamente por el módem de cable.

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 PKCS#7 que se haya definido en un formato específico para ser utilizado con los elementos PS. El fichero de código DEBE cumplir [PKCS#7] y DEBE estar codificado en DER. El fichero de código DEBE ajustarse a la estructura que muestra el cuadro 45.

Cuando se descarga la clave pública CA de raíz CVC y/o los certificados CA (por ejemplo, un certificado CA CVC y/o un certificado CA del fabricante) como parte del fichero de código, los certificados PUEDEN estar contenidos en el campo RootCAPublicKey y/o en los campos CACerts respectivamente como indica el cuadro 45, separados de la imagen de código real contenida en el campo CodeImage.

Cuadro 45/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 CVC que cumplen CVS y X.509
} fin de la firma digital PKCS#7	
SignedContent {	
DownloadParameters {	Formato TLV obligatorio (Tipo 28). (De longitud cero si no hay subTLV.)

Cuadro 45/J.191 – Estructura del fichero de código

Fichero de código	Descripción
RootCAPublicKey ()	TLV opcional para la clave pública CA de raíz CVC CL formateada de acuerdo con el formato RSA-Public-Key (Tipo 4).
CACerts ()	TLV opcional para uno o varios certificados CA codificados DER formateados de acuerdo con el formato TLV de certificado CA (Tipo 17).
}	
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 PKCS#7 como se muestra en el cuadro 46. Aun manteniendo la conformidad con [PKCS#7], 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 PKCS#7 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 PKCS#7 si los datos firmados PKCS#7 no concuerdan con la estructura codificada en DER.

Cuadro 46/J.191 – Datos firmados PKCS#7

Campo PKCS#7	Descripción
Datos firmados	
version	version = 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))
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	version = 1
issuerAndSerialNumber	
issuerName	
CountryName	US
organizationName	CableLabs
CommonName	CableLabs CVC Root CA

Cuadro 46/J.191 – Datos firmados PKCS#7

Campo PKCS#7	Descripción
certificateSerialNumber	<número de serie CVC del fabricante >
digestAlgorithm	SHA-1
AuthenticatedAttributes	
contentType	data (contentType de signedContent)
signing Time	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	version = 1
issuerandserialnumber	
issuername	
CountryName	US
organizationName	CableLabs
CommonName	CA raíz CVC CableLabs
certificateSerialNumber	<número de serie CVC CoSigner >
digestAlgorithm	SHA-1
AuthenticatedAttributes	
contentType	Data (contentType de signedContent)
signing Time	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 – una clave pública CA de raíz CVC y certificados CA (por ejemplo, un certificado CA CVC 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, la clave pública CA de raíz CVC se destina a sustituir la clave pública CA de raíz CVC 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 clave pública CA de raíz CVC actualmente almacenada por la clave pública CA de raíz CVC recibida en el campo de contenido firmado. Esta nueva clave pública CA de raíz CVC se utilizará para la verificación CVC subsiguiente.

Si se incluyen en el campo de contenido firmado, los certificados CA se destinan a sustituir a los certificados CA almacenados hasta dicho momento en el elemento PS. Por ejemplo, si concluye con éxito la descarga e instalación de código y el CACert contenía un certificado CA de fabricante, el elemento PS DEBE sustituir los certificados de fabricante almacenados hasta dicho instante por los certificados de fabricante recibidos en el campo de contenido firmado.

11.3.7.2.1.3 Claves de firma de código

La firma digital PKCS#7 utiliza el algoritmo de criptación RSA con SHA-1 [FIPS 186]. El módulo de la clave RSA para la firma de código tiene una longitud de 2048 bits. El elemento PS DEBE poder verificar las firmas del fichero de código que se efectúan utilizando este tamaño de módulo. El exponente público es F4 (65537 decimal).

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 47 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 47.

Cuadro 47/J.191 – Certificado de verificación de código que cumple X.509

Certificado X.509	Descripción
Certificate {	
version	2 (o sea, X.509 versión 3)
serialNumber	Entero de 8 octetos (es decir un número único asignado por la CA de raíz)
signature	RSA SHA-1, parámetros nulos
issuer	
countryName	US
organizationName	CableLabs
commonName	CableLabs CVC Root CA
validity	
notBefore	utcTime (GMT), YYMMDDhhmmssZ (es decir, instante de emisión)
notAfter	utcTime (GMT), YYMMDDhhmmssZ
subject	
countryName	<Nombre del país>
organizationName	<Nombre de la empresa>

Cuadro 47/J.191 – Certificado de verificación de código que cumple X.509

Certificado X.509	Descripción
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
signature Value	<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 Recomendación.

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.

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 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 cofirmante 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 PS 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 que figura en el elemento PS.

4) Validar la firma CA del CVC utilizando la clave pública CA del CVC 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.

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 ub 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 que figura en el elemento PS.

4) Validar la firma del expedidor del CVC utilizando la clave pública CA del CVC 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. todos los parámetros del certificado EXCEPTO el instante de comienzo de la validez ya no son necesarios y DEBERÍAN rechazarse.

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. El CVC DEBE ajustarse exactamente a lo especificado en 11.3.7.3. La CA del CVC NO DEBE firmar ningún CVC salvo que sea idéntico al formato especificado en dicha cláusula. Antes de firmar un CVC, la CA del CVC DEBE verificar que la solicitud del certificado es auténtica.

La CA del CVC 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 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.

Para conservar espacio de almacenamiento, el elemento PS PUEDE representar internamente el nombre del cofirmante de código en un formato alternativo siempre que la información se mantenga y que el formato original pueda reconstruirse; por ejemplo, como un entero no nulo de 32 bits, con un valor entero de 0 para representar 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. 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. 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.

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 aplicación 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 prestación, 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.

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 docsDevOperStatus;
- 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:

- 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.
- docsDevSwServer PUEDE ser la dirección del servidor TFTP que contiene el soporte lógico que actualmente funciona en el dispositivo.
- 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 del elemento PS. A su vez, la clave pública CA del CVC raíz del elemento PS valida la firma del certificado CA de CVC. 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. Una vez establecida la confianza en la CVK del fabricante, los restantes parámetros del certificado EXCEPTO el instante de comienzo de la validez ya no resultan necesarios y DEBERÍAN rechazarse.

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 que figura en el elemento PS. A su vez, la firma del certificado CA del CVC se valida por parte de la clave pública CA de raíz CVC 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. Una vez establecida la confianza en la CVK del cofirmante, los restantes parámetros del certificado

EXCEPTO el instante de comienzo de la validez ya no son necesarios y DEBERÍAN descartarse;

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 actualizará 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 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 aplicación 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 [FIPS-140-2]. Concretamente, los elementos 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.

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:
  - prueba de la velocidad de la conexión remota;
  - prueba ping remota.
- 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 Recomendación 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 prueba de velocidad de conexión remota y para la prueba ping remota, descritas en 6.4.3.1 y 6.4.3.2 respectivamente.

12.2.1.1 Prueba de velocidad de conexión remota

La prueba de velocidad de conexión remota 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 (véase la figura 28).

- El sistema de gestión de red (NMS, *network management system*) 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.

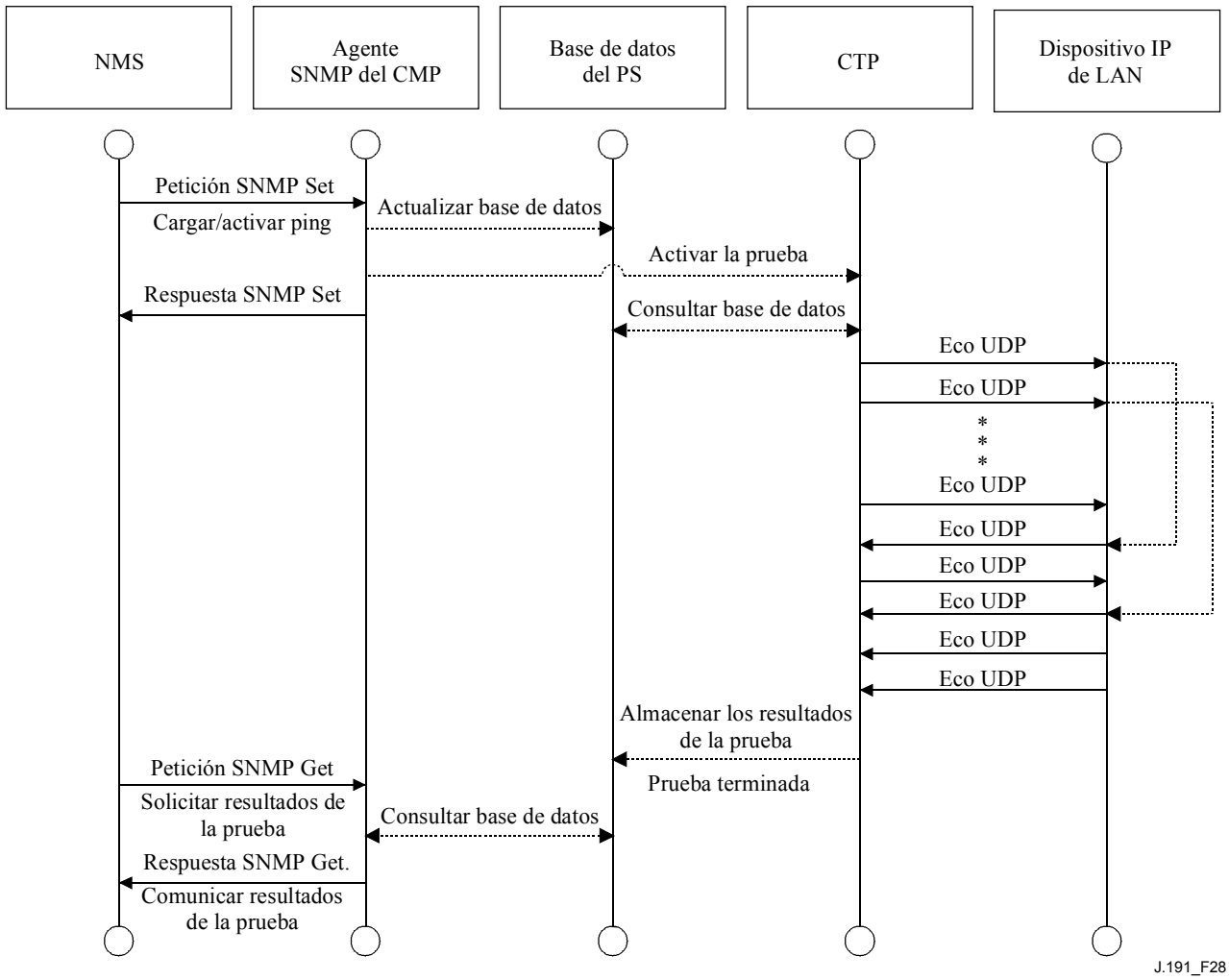


Figura 28/J.191 – Diagrama secuencial de la prueba de la velocidad de conexión

12.2.1.2 Prueba ping remota

La prueba ping remota puede servir para validar el estado de la conectividad, los niveles de la calidad de funcionamiento e identificar posibles errores de configuración (véase la figura 29).

- 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.

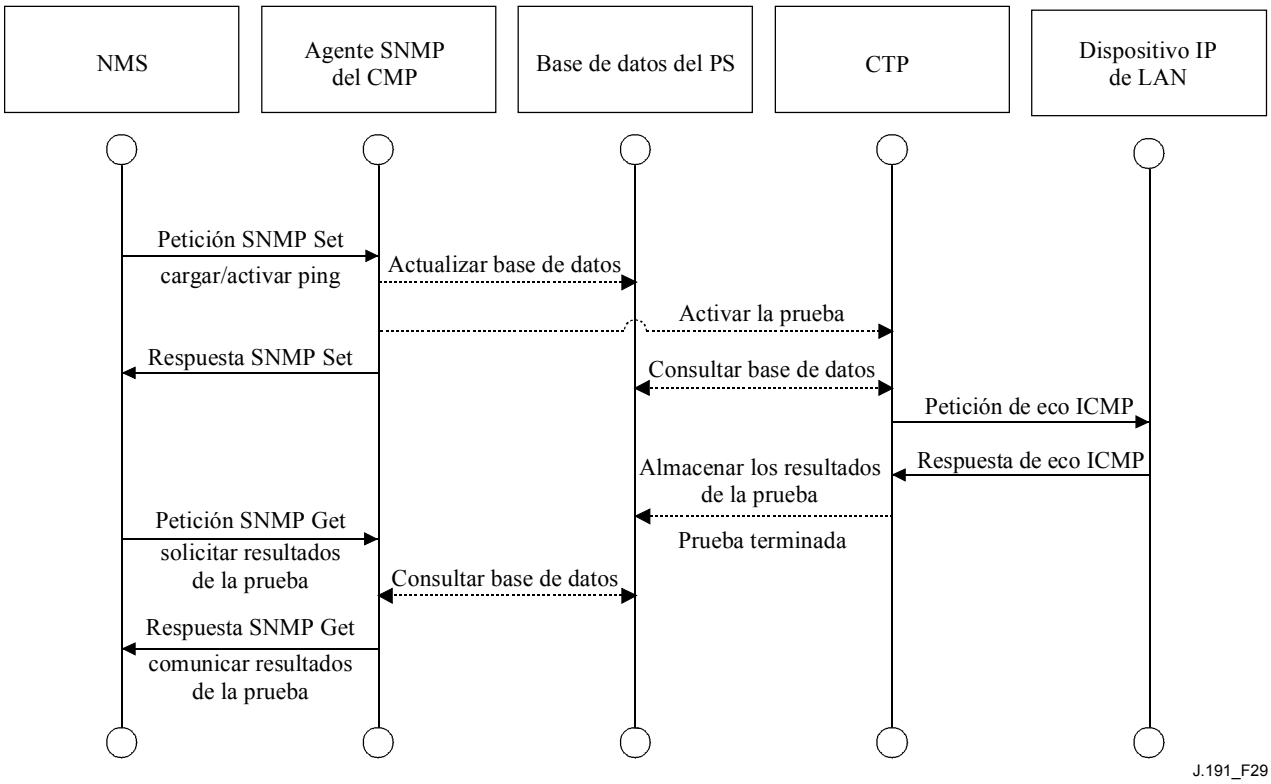


Figura 29/J.191 – Diagrama secuencial de la prueba de ping remoto

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 pruebas de velocidad de la conexión y del ping remoto) 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 30 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.

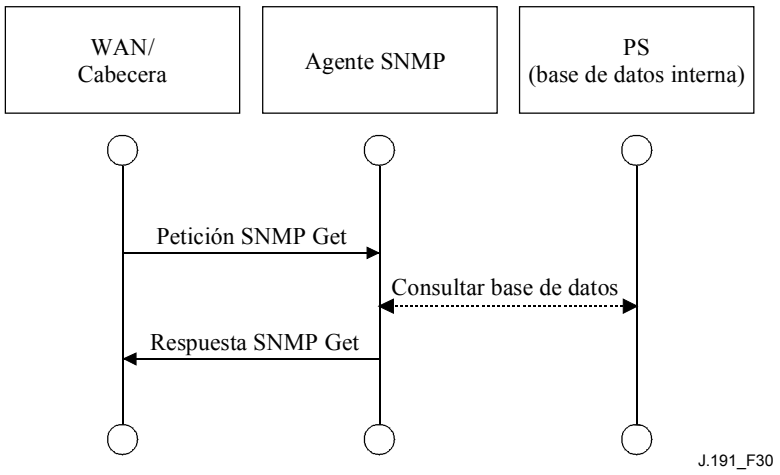


Figura 30/J.191 – Diagrama secuencial del acceso a la base de datos del PS desde la interfaz WAN-Man del PS

12.3.2 Reconfiguración

12.3.2.1 Descarga de soporte lógico del PS

El ejemplo siguiente en la figura 31 ilustra el proceso de descarga de soporte lógico y de microprogramas con destino a un PS en el modo de prestación 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.

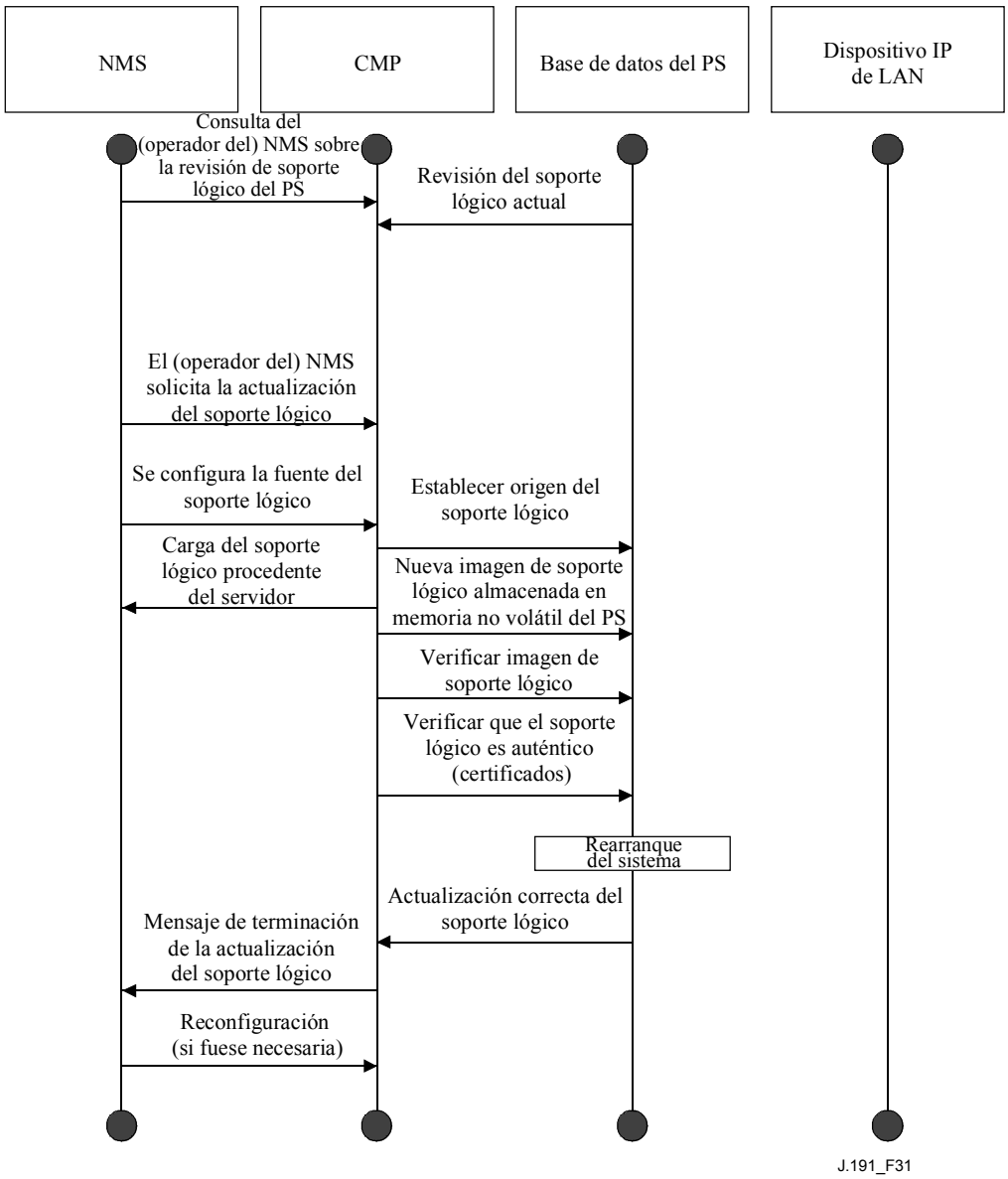


Figura 31/J.191 – Diagrama secuencial de la descarga de soporte lógico del PS

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.

12.3.2.2 Descarga del fichero de configuración del PS

El ejemplo siguiente en la figura 32 ilustra la reconfiguración de un PS en el modo de prestación SNMP, mediante la descarga de un fichero de 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 de configuración, graba el número de tuplas TLV procesadas y omitidas de los objetos correspondientes de la MIB.

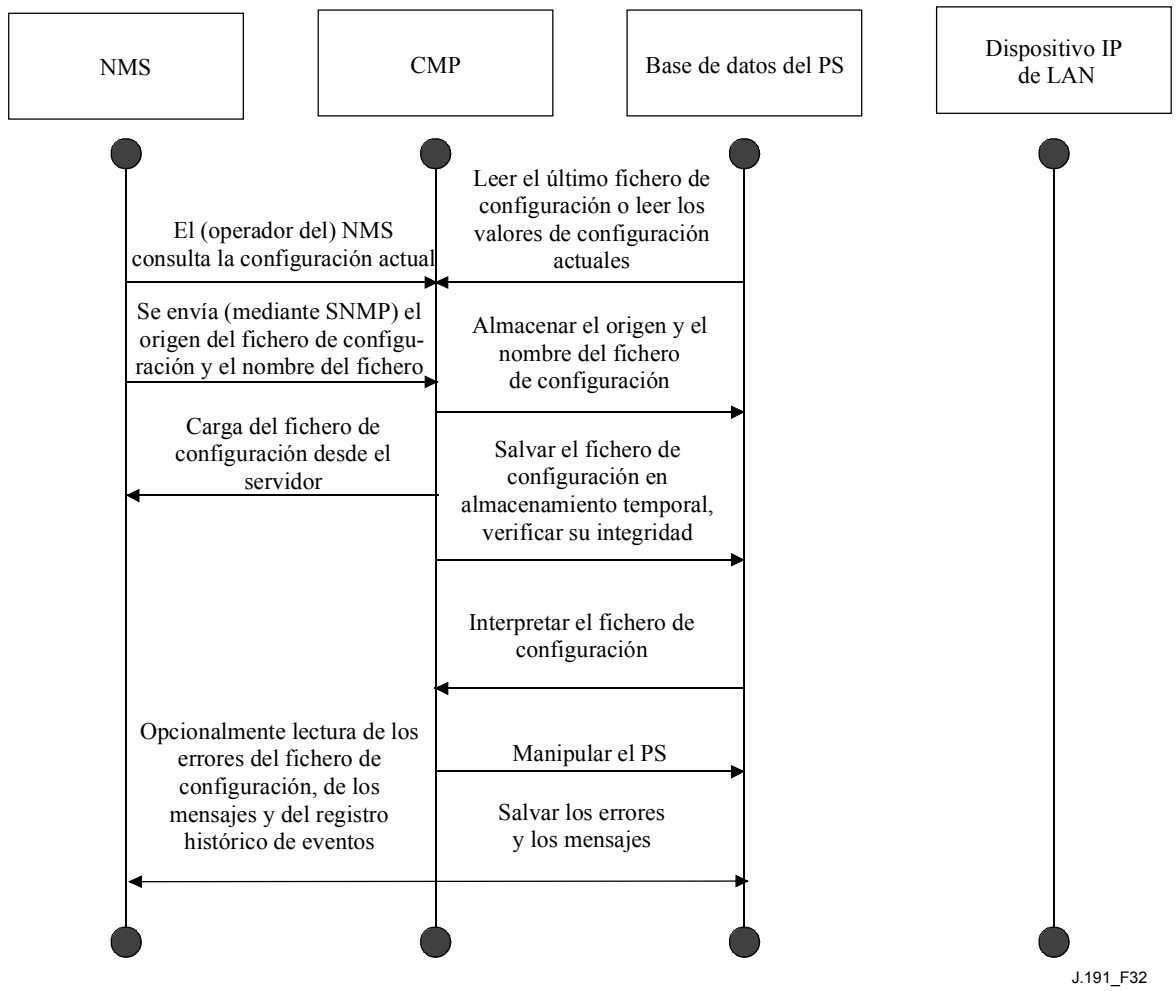


Figura 32/J.191 – Diagrama secuencial de la reconfiguración del PS (descarga del fichero de configuración)

12.4 Acceso a la MIB

12.4.1 Configuración del VACM

El operador de cable controla el dominio de gestión. Se muestra un ejemplo de configuración de los parámetros del VACM, en la figura 33.

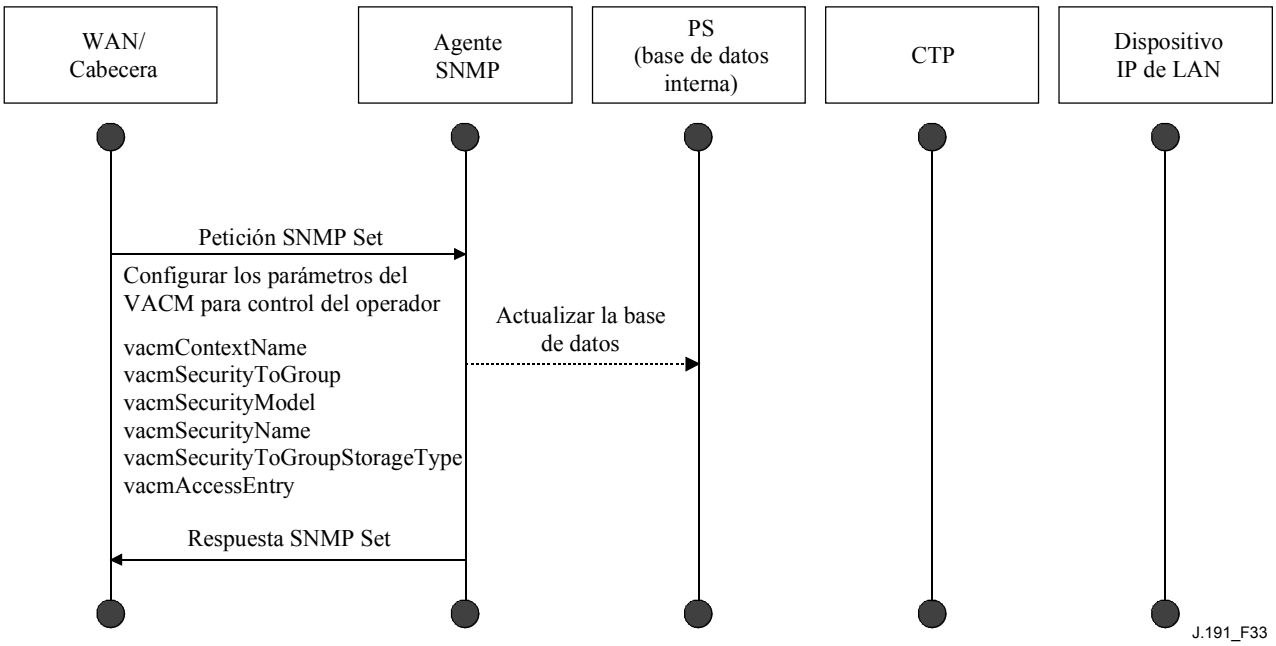


Figura 33/J.191 – Secuencia de configuración del PS (parámetros del VACM)

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.

El siguiente ejemplo en la figura 34 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.

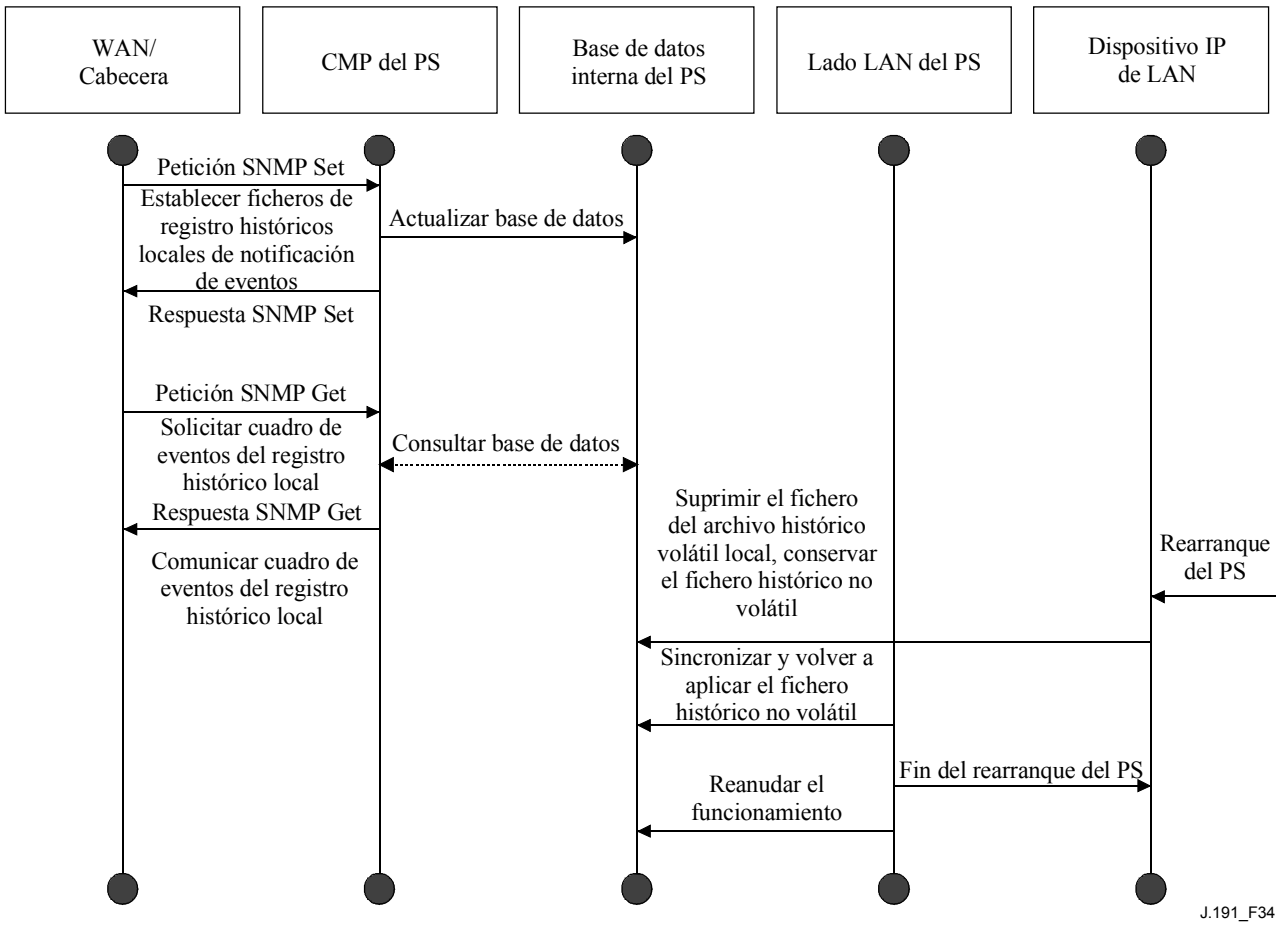


Figura 34/J.191 – Secuencia de la configuración del PS (control de eventos)

El siguiente caso en la figura 35 ilustra la descarga de un fichero de configuración para un PS que se encuentra en el modo de prestación 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.

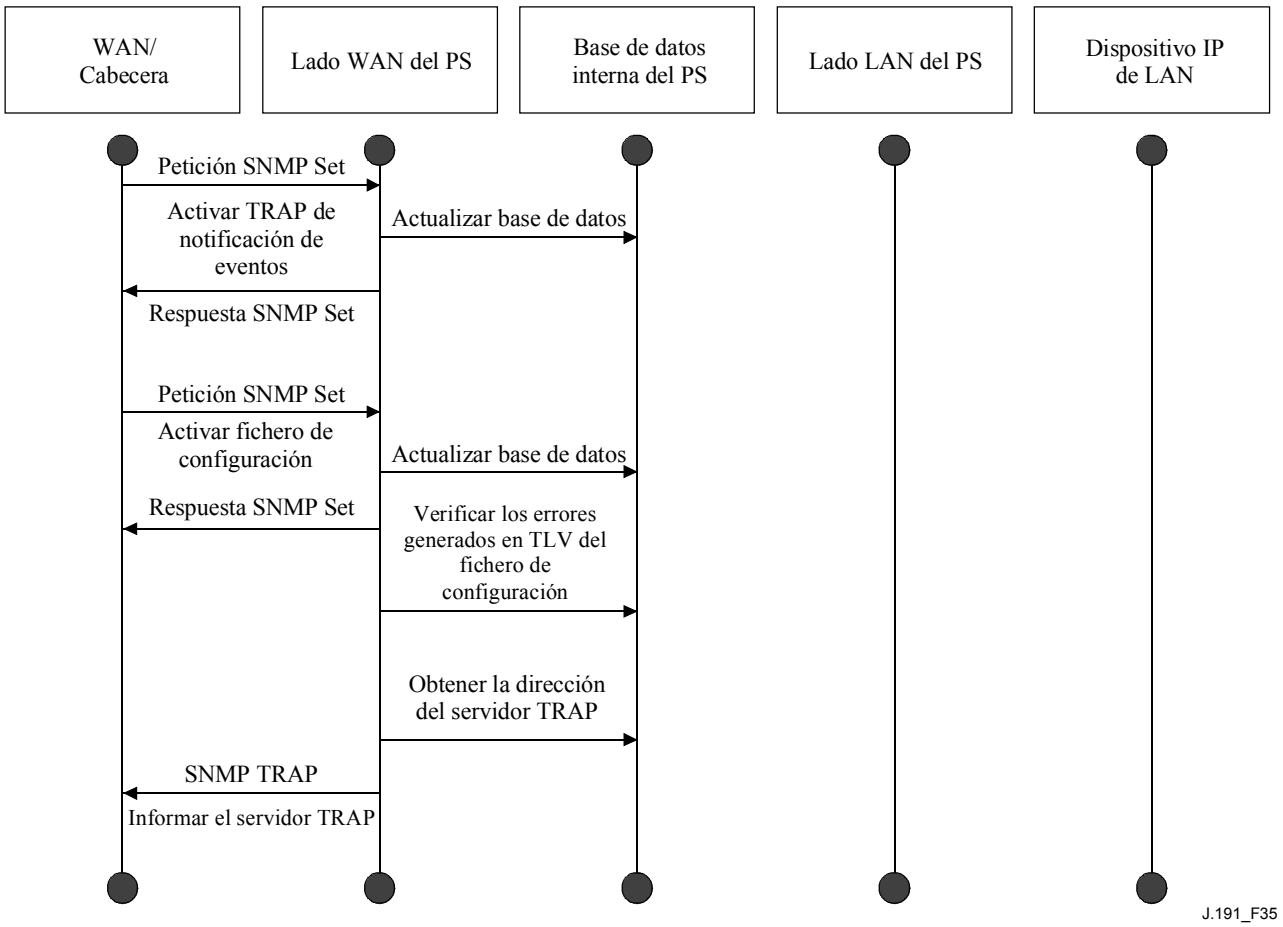


Figura 35/J.191 – Secuencia de descarga del fichero de configuración del PS (con TLV no válidos)

En el siguiente caso (figura 36) 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.

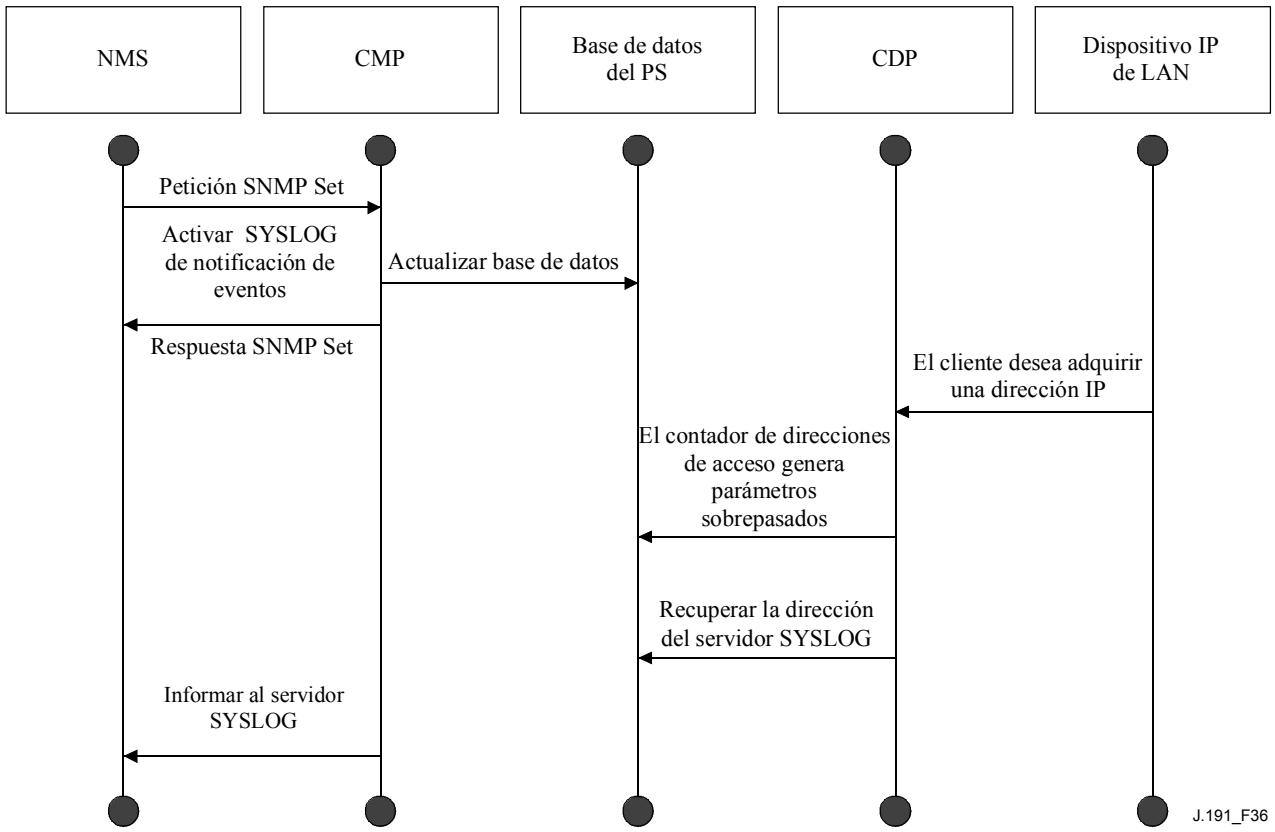


Figura 36/J.191 – Secuencia de adquisición de direcciones del dispositivo IP de LAN (la petición sobrepasa el contador suministrado)

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. La figura 37 contiene una descripción del mecanismo de estrangulamiento y limitación de eventos del CMP.

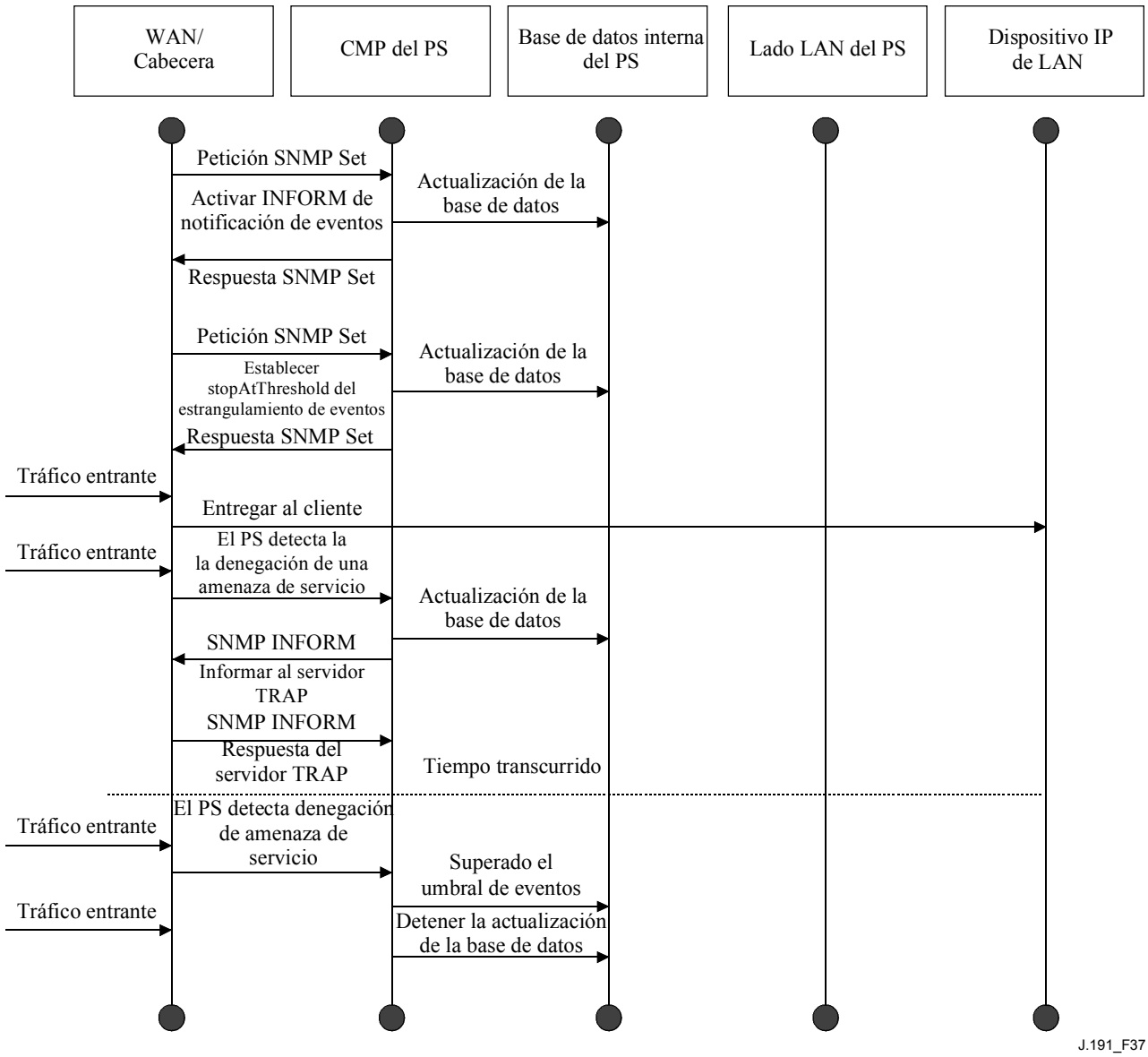


Figura 37/J.191 – Operación de estrangulamiento y limitación de eventos del CMP

El ejemplo en la figura 37 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.

13 Procesos de prestación

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 de la funcionalidad de módem de cable es independiente y distinta de la prestación del PS y ajena al objeto de la presente Recomendación. Se remite al lector a las especificaciones DOCSIS que describen la prestación del módem de cable.

Los elementos funcionales con los que interactúa el elemento PS durante los procesos de prestación enumerados anteriormente se identifican en la figura 38. El elemento funcional centro de distribución de claves (KDC) se muestra con un perfil discontinuo ya que se utiliza en el modo de prestación SNMP aunque no en el modo de prestación DHCP. Los demás elementos funcionales se utilizan en ambos modos de prestación.

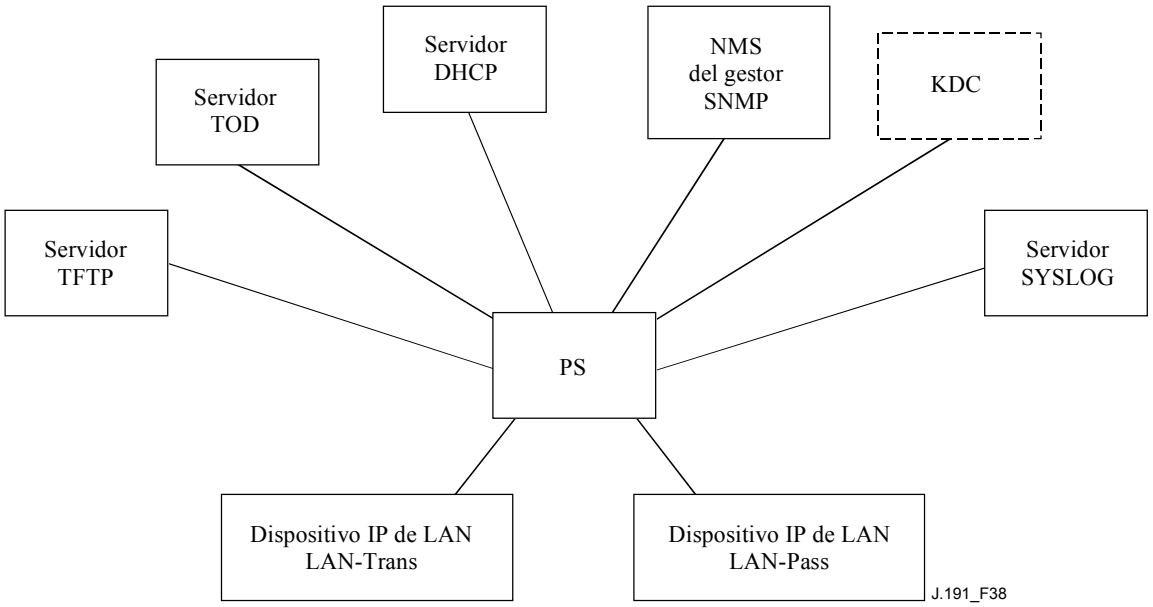


Figura 38/J.191 – Elementos funcionales de la prestación

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, *time of day*) 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, *dynamic host configuration protocol*) 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 2571], [RFC 2572], [RFC 2574], y [RFC 2575]. 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 prestación

Las cláusulas 5.7 y 7.1.1 introducen dos modos de prestación soportados por el elemento de servicio de portal: el modo de prestación DHCP y el modo de prestación SNMP. Esta cláusula expone con más detalle dichos modos. La figura 39 ilustra un posible flujo de eventos de los dos modos de prestación. El punto clave de la figura 39 es la disyuntiva utilizada por el PS para determinar el modo de prestación en el que operar.

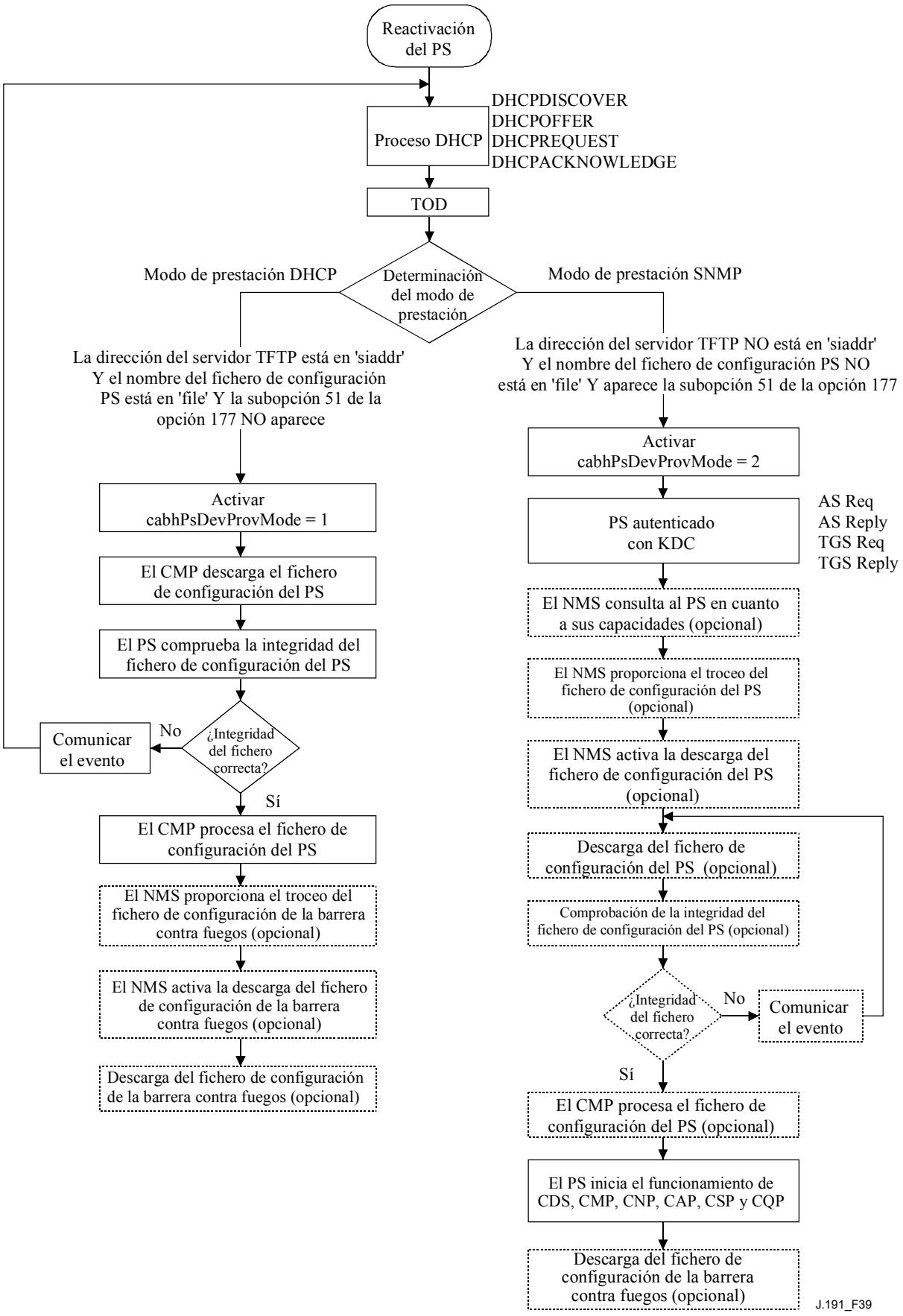


Figura 39/J.191 – Modos de prestación

El PS funciona en el modo de prestación 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 prestación DHCP tiene por objeto permitir que el PS funcione en una infraestructura que no incluya características IPCablecom avanzadas.

El modo de prestación 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 prestación SNMP tiene por objeto permitir que el PS aproveche las características avanzadas de la infraestructura IPCablecom.

13.2 Proceso de prestación de la gestión del PS: modo de prestación 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 prestación bajo el que va a funcionar (véase 7.2.3.3). La cláusula 7.2.2.2.1 describe dos 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 prestación 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 prestación DHCP pero es opcional para el PS cuando funciona en el modo de prestación SNMP. Tras la descarga inicial del fichero de configuración del PS activada por los campos de mensaje DHCP, el NMS puede iniciar la configuración posterior a la prestación emitiendo una petición SNMP Set a los objetos de la MIB cabhPsDevProvConfigHash y cabhPsDevProvConfigFile conforme a lo descrito en 7.3.

En el modo de prestación 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.

La figura 40 y el cuadro 48 describen la secuencia de mensajes necesaria para inicializar el funcionamiento del PS en el modo de prestación DHCP. La prestación del PS NO DEBE tener lugar antes del proceso de prestación del módem de cable.

El proceso opcional de descarga del fichero de configuración de la barrera contra fuegos se muestra sombreado en la figura 40.

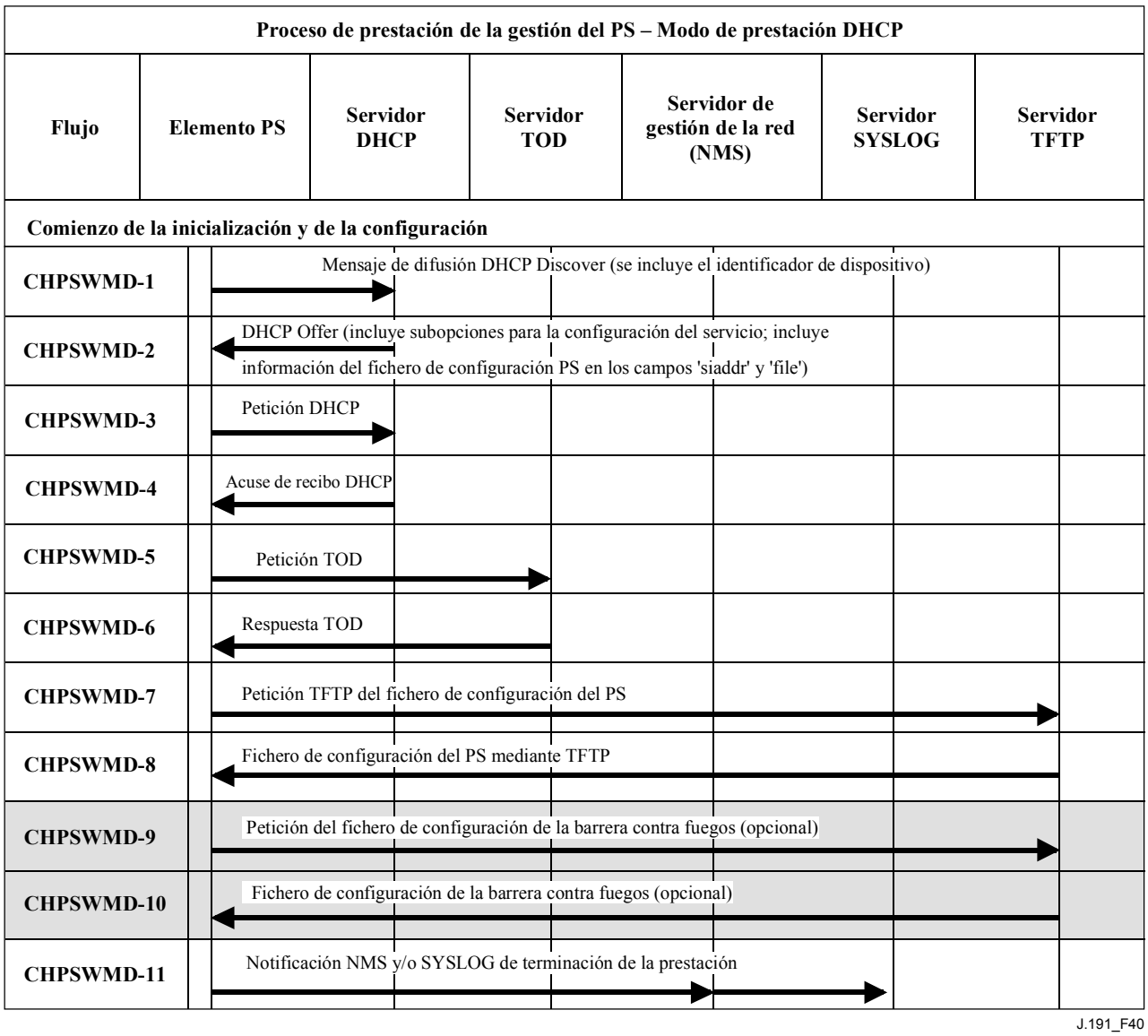


Figura 40/J.191 – Proceso de prestación de la gestión del PS – Modo de prestación DHCP

El cuadro 48 describe los mensajes CHPSWMD-1 a CHPSWMD-11 mostrados en la figura 40.

Cuadro 48/J.191 – Descripciones del flujo del proceso de prestación PS WAN-Man en el modo de prestación 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) DEBE enviar un mensaje de difusión DHCP DISCOVER. El mensaje de difusión DHCP DISCOVER enviado por el CDP (CDC) DEBE incluir las opciones obligatorias que recoge el cuadro 21. 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). Tras cinco reintentos 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 177 con la subopción 51 Y debe incluir información del fichero de configuración del PS en los campos 'siaddr' y 'file' del mensaje DHCP. El PS modifica cabhPsDevProvMode en base a la información recibida en el DHCP OFFER (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 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.

Cuadro 48/J.191 – Descripciones del flujo del proceso de prestación PS WAN-Man en el modo de prestación 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 DEBE emitir 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 prestación DHCP DEBE enviar 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.

Cuadro 48/J.191 – Descripciones del flujo del proceso de prestación PS WAN-Man en el modo de prestación DHCP

Fase	Prestación WAN-Man del PS: modo de prestación DHCP	Secuencia normal	Secuencia de fallo
CHPSWMD-8	*El servidor TFTP envía el fichero de configuración del PS* Tras la recepción del fichero de configuración del PS, se calcula el troceo del fichero de configuración y se compara con el valor añadido al nombre del fichero de configuración del PS (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/FQDN del servidor TFTP del fichero de configuración de la barrera contra fuegos, en nombre del fichero de configuración de la barrera contra fuegos, el troceo del fichero de configuración de la barrera contra fuegos y la clave de criptación (suponiendo criptado el fichero de configuración) 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.	CHPSWM-8 DEBE tener lugar una vez completada CHPSWM-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 48/J.191 – Descripciones del flujo del proceso de prestación PS WAN-Man en el modo de prestación 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 prestación DHCP) DEBE saltarse las fases CHPSWMD-9 y CHPSMWD-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. Si el fichero está criptado se descripta. 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 48/J.191 – Descripciones del flujo del proceso de prestación PS WAN-Man en el modo de prestación 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 48/J.191 – Descripciones del flujo del proceso de prestación PS WAN-Man en el modo de prestación 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 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 fallida (cabhPsDevInitRetryTrap) al receptor de trampas. 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'.		

El temporizador de prestación del PS NO DEBE reinicializarse al valor de comienzo de cabhPsDevProvTimer mientras no expire el temporizador de prestación del PS Y el valor de cabhPsDevProvState siga siendo inProgress (2) O se reactive el PS.

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 7.2.3.3, el PS determina que ha de operar en el modo de prestación 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 prestación 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 41 ilustra los flujos de mensajes que han de utilizarse para la prestación del PS cuando funciona en el modo de prestación SNMP.

El proceso de prestación para la interfaz WAN-Man de un PS que funciona en el modo de prestación SNMP DEBE tener lugar de acuerdo con la secuencia descrita en la figura 41 y definida en detalle en el cuadro 49. Los pasos opcionales se muestran sombreados en la figura 41. Estos pasos opcionales pueden tener lugar inmediatamente después de la fase CHPSWMS-15 con posterioridad a ésta o no tener lugar en absoluto.

El cuadro 49 describe las fases del proceso de prestación mostrado en la figura 41.

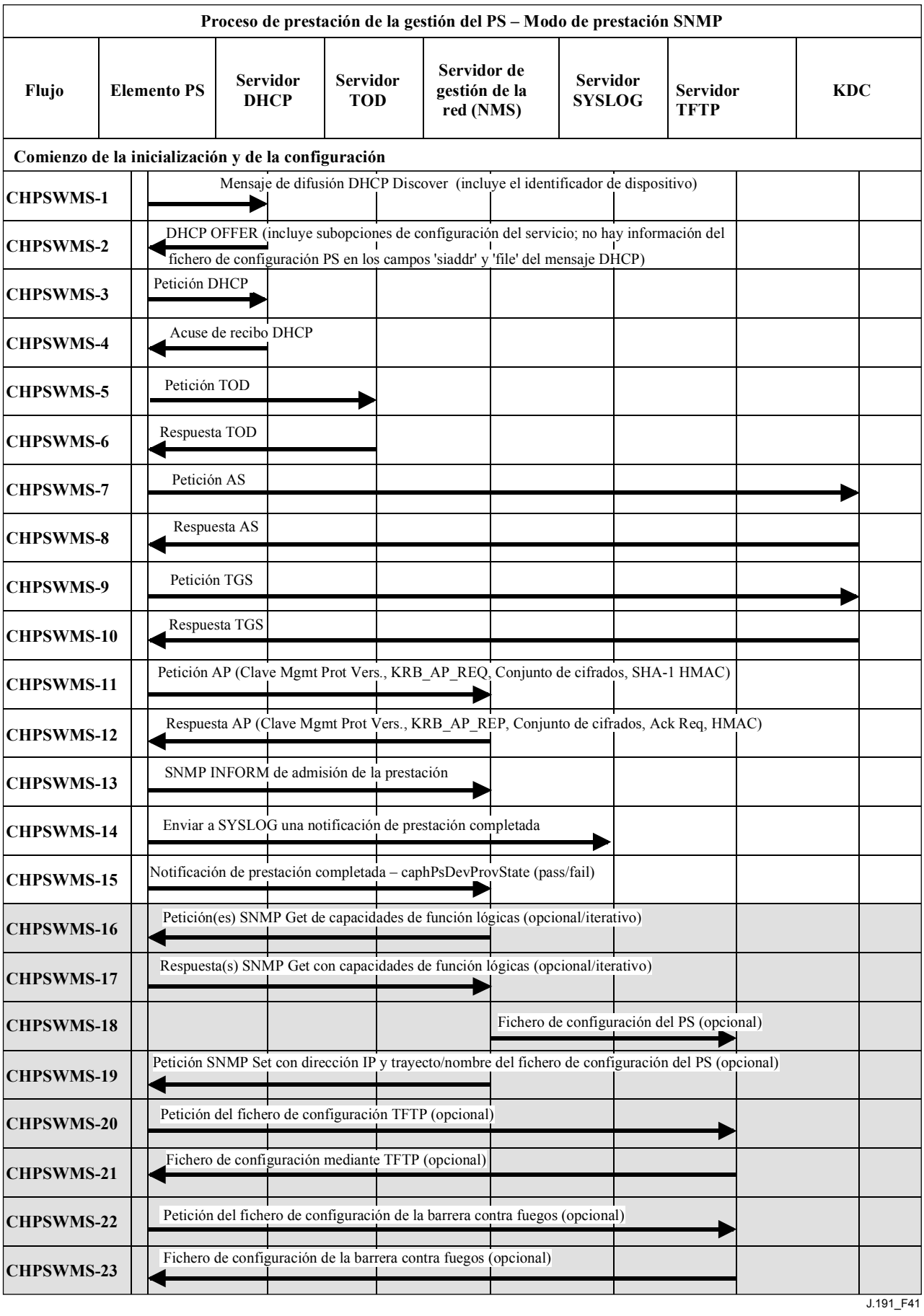


Figura 41/J.191 – Proceso de prestación de la gestión del PS – Modo de prestación SNMP

Cuadro 49/J.191 – Descripciones del flujo del proceso de prestación WAN-Man del PS en el modo de prestación SNMP

Fase	Prestación WAN-Man del PS: Modo de prestación SNMP	Secuencia ordinaria	Secuencia de fallo
CHPSWMS-1	*Mensaje de difusión DHCP Discover* El CDP (CDC) DEBE enviar un mensaje de difusión DHCP DISCOVER. El mensaje de difusión DHCP DISCOVER enviado por el CDP (CDC) DEBE incluir las opciones obligatorias que recoge el cuadro 21. El PS DEBE iniciar el temporizador de prestación utilizando el valor de comienzo accesible a través de cabhPsDevProvTimer Y otorgando a cabhPsDevProvState el estado 'inProgress' (2) cuando el CDC envía un mensaje de difusión DHCP DISCOVER.	Comenzar la secuencia de prestación.	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). Tras cinco reintentos el PS inicia la operación del CDS especificado 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 la subopción 51 Y no debe figurar información del fichero de configuración del PS en los campos siaddr y file del mensaje DHCP. El PS modifica cabhPsDevProvMode en base a la información recibida en el mensaje DHCP OFFER (véase 7.2.3.3).	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 CDP DEBE enviar 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 CDP un mensaje DHCP ACK que contiene la dirección IPv4 del PS. 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 49/J.191 – Descripciones del flujo del proceso de prestación WAN-Man del PS en el modo de prestación SNMP

Fase	Prestación WAN-Man del PS: Modo de prestación 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 a la dirección almacenada en cabhPsDevServerTime conforme a lo dispuesto en 7.4.2.	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*[a)] El PS DEBE enviar el mensaje de petición AS al operador KDC para solicitar un tique Kerberos	CHPSWMS-7 DEBE tener lugar tras completarse CHPSWMS-5. CHPSWMS-7 PUEDE tener lugar antes de completarse CHPSWMS-6.	Volver a CHPSWMS-1.
CHPSWMS-8	*Respuesta AS* El mensaje de respuesta AS se recibe procedente del operador KDC con el tique Kerberos	CHPSWMS-8 DEBE tener lugar tras completarse CHPSWMS-7.	Volver a CHPSWMS-1.
CHPSWMS-9	*Petición TGS* Si el PS obtiene el tique de concesión de tique (TGT, *ticket granting ticket*) en la fase CHPSWMS-10 del proceso de prestación de la interfaz WAN-Man del PS, DEBE enviarse al operador KDC el mensaje de petición TGS.	CHPSWMS-9 DEBE tener lugar tras completarse CHPSWMS-8.	Volver a CHPSWMS-1.
CHPSWMS-10	*Respuesta TGS* 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.

Cuadro 49/J.191 – Descripciones del flujo del proceso de prestación WAN-Man del PS en el modo de prestación SNMP

Fase	Prestación WAN-Man del PS: Modo de prestación SNMP	Secuencia ordinaria	Secuencia de fallo
CHPSWMS-11	*Petición AP* El mensaje de petición AP DEBE enviarse al servidor de prestación para solidar la información de claves para SNMPv3.	CHPSWMS-11 DEBE tener lugar tras completarse CHPSWMS-10.	Volver a CHPSWMS-1.
CHPSWMS-12	*Respuesta AP* Se recibe el mensaje de respuesta AP procedente del servidor de prestación con la información de claves para SNMPv3. NOTA – DEBEN establecerse las claves SNMPv3 y rellenarse los cuadros SNMPv3 asociados antes de la siguiente fase. Las claves y los cuadros se establecen con la información de la respuesta AP.	CHPSWMS-12 DEBE tener lugar tras completarse CHPSWMS-11.	Volver a CHPSWMS-1.
CHPSWMS-13	*SNMP Inform* El PS DEBE enviar al NMS un SNMPv3 INFORM (cabhPsDevProvEnrollTrap) solicitando la admisión. La dirección IP de esta PROVISIONING SNMP ENTITY se encuentra en el mensaje DHCP OFFER.	CHPSWMS-13 DEBE tener lugar tras completarse CHPSWMS-12.	Volver a CHPSWMS-1.
CHPSWMS-14	*Notificación de SYSLOG* Si el PS recibió una dirección de servidor SYSLOG en el DHCP OFFER, el PS DEBE enviar al SYSLOG una notificación de "prestación completada". Esta notificación incluirá el resultado pass-fail de la operación de prestación. El formato genérico de esta notificación corresponde a la definición de 6.5.1.	CHPSWMS-14 DEBE tener lugar tras completarse CHPSWMS-13.	

Cuadro 49/J.191 – Descripciones del flujo del proceso de prestación WAN-Man del PS en el modo de prestación SNMP

Fase	Prestación WAN-Man del PS: Modo de prestación SNMP	Secuencia ordinaria	Secuencia de fallo
CHPSWMS-15	*SNMP Inform* El PS DEBE enviar al NMS un SNMP INFORM (cabhPsDevInitTrap) con una notificación "prestación completada". Se presenta FAIL cuando fracasa el proceso del fichero de configuración. De lo contrario el estado de prestación es PASS. El PS DEBE actualizar el valor cabhPsDevProvState con el estado 'pass' (1) cuando las fases de prestación CHPSWMS-1 a CHPSWMS-23 se completan con éxito. El PS DEBE actualizar el valor de cabhPsDevProvState con el estado 'fail' (3) Y comunicar un evento indicando el fallo del proceso de prestación si el temporizador de prestación del PS expira antes de la actualización del valor de cabhPsDevProvState con el estado 'pass'.	CHPSWMS-15 DEBE tener lugar tras completarse CHPSWMS-14.	Si falla el SNMP Inform, el servidor de prestación puede desconocer que se ha completado el proceso de prestación salvo que consulte el objeto cabhPsProvisioning State.
Fases opcionales			
CHPSWMS-16	*SNMP Get*[b)] Si el sistema de prestación necesita capacidades adicionales de dispositivo, la solicita al PS mediante peticiones SNMPv3 Get. (Iterativo) El NMS envía peticiones SNMPv3 GET del PS para obtener la información necesaria sobre capacidad del PS. La aplicación de prestación puede utilizar una petición GETBulk para obtener varias informaciones en un único mensaje.	CHPSWMS-16 no debe tener lugar antes de completarse CHPSWMS- 15.	Volver a CHPSWMS-1.

Cuadro 49/J.191 – Descripciones del flujo del proceso de prestación WAN-Man del PS en el modo de prestación SNMP

Fase	Prestación WAN-Man del PS: Modo de prestación SNMP	Secuencia ordinaria	Secuencia de fallo
CHPSWMS-17	*Respuesta SNMP Get* (Iterativo) El PS DEBE responder al NMS los mensajes de petición Get Request o Get Bulk con una respuesta Get para cada una de las peticiones Get. Una vez terminados todos los Get y los GetBulk, el NMS envía el dato solicitado a la aplicación de prestación.	CHPSWMS-17 DEBE tener lugar tras completarse CHPSWMS-16.	N/A
CHPSWMS-18	*Creación del fichero de configuración* (Opcional) El sistema de prestación utiliza información de las fases de prestación del PS CHPSWMS-14 y CHPSWMS-15 para crear un fichero de configuración PS. El sistema de prestación efectúa un troceo sobre el contenido del fichero de configuración PS. Dicho troceo se envía al PS en la fase siguiente.	CHPSWMS-18 DEBE tener lugar tras completarse CHPSWMS-17.	N/A

Cuadro 49/J.191 – Descripciones del flujo del proceso de prestación WAN-Man del PS en el modo de prestación SNMP

Fase	Prestación WAN-Man del PS: Modo de prestación SNMP	Secuencia ordinaria	Secuencia de fallo
CHPSWMS-19	*SNMP Set* El sistema de prestación 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 prestación 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, el troceo del fichero de configuración de la barrera contra fuegos y la clave de criptación (si se cripta el 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.	CHPSWMS-19 DEBE tener lugar tras completarse CHPSWMS-18.	Volver a CHPSWMS-1 si se refirió el Set pero tuvo lugar un error de proceso.
CHPSWMS- 20	*Petición TFTP* Si el NMS activa la descarga por parte del PS del fichero de configuración del PS descrito en 7.3.3.2, el PS DEBE enviar al servidor TFTP una petición TFTP Get para solicitar el fichero de configuración del PS especificado.	CHPSWMS-20 DEBE tener lugar tras completarse CHPSWMS-19.	Continuar en CHPSWMS-21.

Cuadro 49/J.191 – Descripciones del flujo del proceso de prestación WAN-Man del PS en el modo de prestación SNMP

Fase	Prestación WAN-Man del PS: Modo de prestación SNMP	Secuencia ordinaria	Secuencia de fallo
CHPSWMS-21	*El servidor TFTP envía el fichero de configuración* 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-19. 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/FQDN del servidor TFTP del fichero de configuración de la barrera contra fuegos, el nombre del fichero de configuración de la barrera contra fuegos, el troceo del fichero de configuración de la barrera contra fuegos y la clave de criptación (de criptarse el 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.	CHPSWMS-21 DEBE tener lugar tras completarse CHPSWMS-20.	Si falla la descarga TFTP, comunicar el error, continuar en CHPSWMS-23, y continuar reintentando CHPSWMS-20 (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-22	*TFTP Request – 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-22 tiene lugar, DEBE tener lugar tras completarse CHPSWMS-21.	Volver a CHPSWMS-1.

Cuadro 49/J.191 – Descripciones del flujo del proceso de prestación WAN-Man del PS en el modo de prestación SNMP

Fase	Prestación WAN-Man del PS: Modo de prestación SNMP	Secuencia ordinaria	Secuencia de fallo
CHPSWMS-23	*El servidor TFTP envía el fichero de configuración de la barrera contra fuegos* El servidor TFTP envía al PS una respuesta TFTP con el fichero solicitado. Una vez recibe el PS el fichero de configuración de la barrera contra fuegos, calcula el troceo de éste y lo compara con el valor recibido en la fase CHPSWMS-21. Si el fichero está criptado se descripta. A continuación se procesa el fichero. Consúltese en 7.3.3 la descripción del contenido del fichero de configuración del PS.	CHPSWMS-23 DEBE tener lugar tras completarse CHPSWMS-22.	Si falla la descarga TFTP, continuar el funcionamiento del PS pero comunicar el error y continuar reintentando CHPSWMS-22. Si el procesamiento del fichero de configuración de la barrera contra fuegos provoca un error, continuar y comunicar el error como evento.
a) Los pasos CHPSWMS-7 a CHIPSWMS-10 son opcionales en ciertos casos. Puede consultarse los detalles en la cláusula 11. b) Las operaciones SNMP Get y subsiguientes operaciones de respuesta SNMP Get son opcionales, dependiendo de la necesidad de información adicional para formar el fichero de configuración del PS, y también de la necesidad del fichero de configuración del PS.			

13.3.1 Descarga del fichero de configuración WAN-Man del PS

El PS funcionando en el modo de prestación 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 prestación SNMP, PUEDE descargarse del fichero de configuración del PS para que la prestación 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 prestación del PS

Se proporciona un temporizador de prestación para que el PS continúe los ciclos del proceso de prestación cuando queda incompleta alguna operación. El objeto temporizador, cabhPsDevProvTimer, tiene un valor de inicialización por defecto de 5 minutos.

Modo de prestación DHCP

El temporizador de prestación DEBE comenzar a correr al comenzar la fase CHPSWMD-1. Si el temporizador de prestación del PS expira antes de ejecutar la fase CHPSWMD-12, el CDC DEBE otorgar a cabhPsDevProvState el estado '3' (fallo), el proceso de prestación DEBE volver a la fase CHPSWMD-1, Y el PS debe generar el evento adecuado y restaurar el temporizador de prestación del PS al valor de cabhPsDevProvTimer.

Modo de prestación SNMP

El temporizador de prestación DEBE comenzar a correr cuando comienza la fase CHPSWMS-1. Si el temporizador de prestación del PS expira antes de ejecutar la fase CHPSWMS-23 el CDC DEBE otorgar a cabhPsDevProvState el estado '3' (fallo), el proceso de prestación DEBE volver a la fase CHPSWMD-1, el PS DEBE comunicar el oportuno evento Y el PS DEBE restaurar el temporizador de prestación del PS al valor de cabhPsDevProvTimer.

13.3.3 Informe de terminación de la admisión a prestación y de la prestación

Sólo para el PS funcionando en el modo de prestación SNMP, el informe de admisión de prestación, definido en el anexo B permite que el servidor de prestación determine si el PS está preparado para el fichero de configuración del PS.

Tanto en el modo de prestación DHCP como en el modo de prestación SNMP, la trampa de terminación de la prestación (cabhPsDevInitTrap), definida en el anexo B, indica si se ha completado o no la secuencia de prestación.

13.4 Prestación 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.

13.4.1 Estado de prestación y comunicación de errores

Como indican los cuadros 48 y 49, el fallo de las fases del proceso de prestación se suele traducir en la repetición del proceso desde la primera fase, CHPSWMD-1 o CHPSWMS-1.

13.5 Proceso de prestación 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 prestación DHCP y SNMP.

Los siguientes diagramas ilustran el flujo de mensajes que ha de utilizarse para la prestación de direcciones WAN-Data del PS.

Si tiene lugar el proceso de prestación de direcciones WAN-Data del PS, DEBE seguir la secuencia que muestra la figura 42 y describe el cuadro 50 detalladamente.

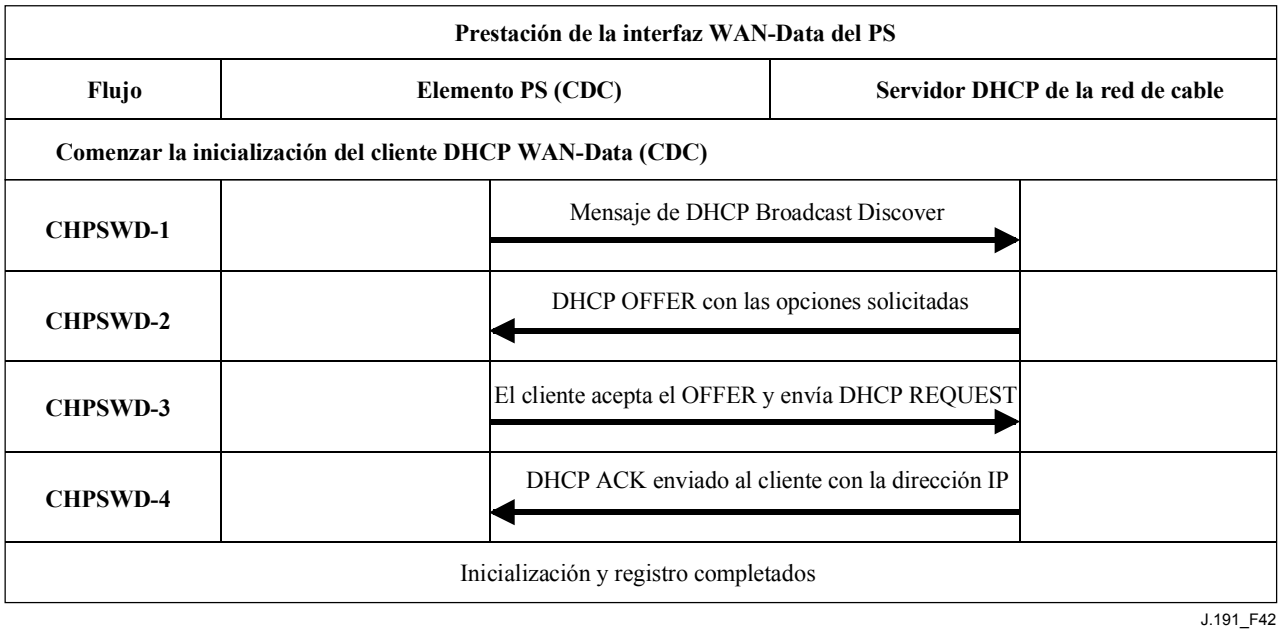


Figura 42/J.191 – Proceso de prestación WAN-Data del PS

Cuadro 50/J.191 – Descripción del flujo de la prestación WAN-Data del PS

Fase	Prestación de dirección WAN-Data del PS	Secuencia ordinaria	Secuencia de fallo
CHPSWD-1	*Mensaje de difusión DHCP Discover* El PS DEBE enviar un mensaje de difusión DHCP DISCOVER con las opciones obligatorias que figuran en el cuadro 21.	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 DEBE enviar al servidor DHCP adecuado un mensaje DHCP REQUEST 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 prestación termina al completarse CHPSWD-4.	Si falla en virtud del protocolo DHCP volver a CHPSWD-1.

13.6 Proceso de prestación: 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 prestación asignados por el NMS de la red de cable (véase 7.2.3.2).

Esta cláusula describe el proceso de prestación 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 prestación de los dispositivos IP del sector LAN-Trans en los modos de prestación DHCP y SNMP.

El flujo de mensajes del proceso de prestación para un dispositivo IP de LAN del sector LAN-Trans se describe en la figura 43. El cuadro 51 proporciona detalles adicionales de dicho proceso.

El proceso de prestación correspondiente a los dispositivos IP de LAN del sector LAN-Trans DEBE tener lugar de acuerdo con la secuencia representada en la figura 43 y descrita en más detalle en el cuadro 51.

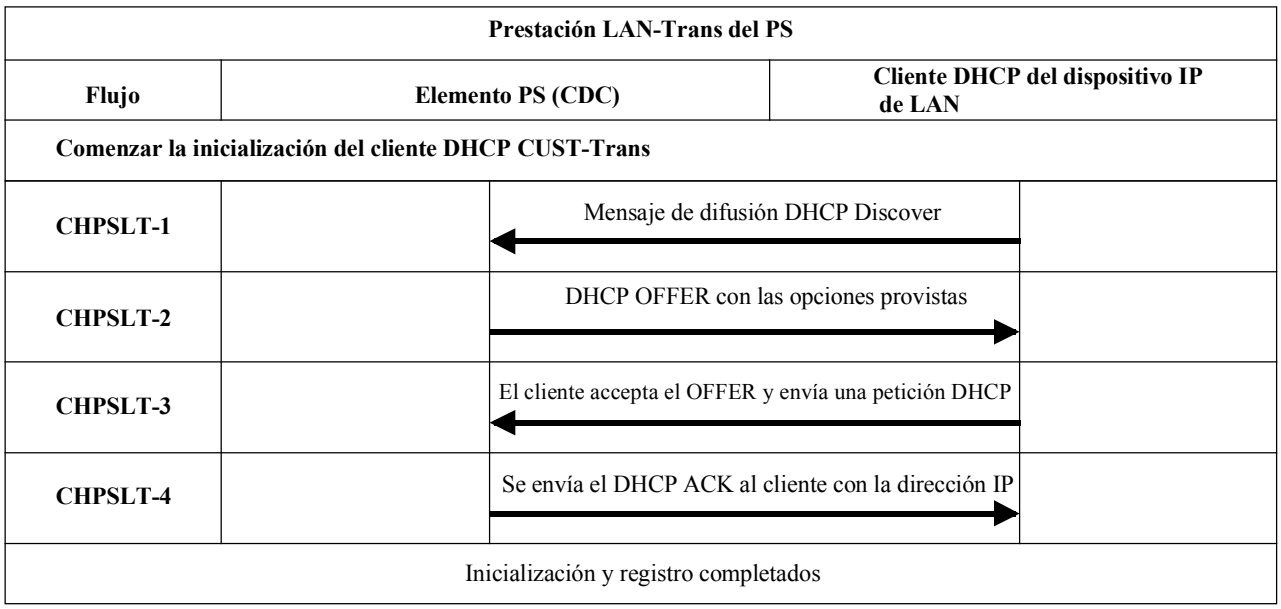


Figura 43/J.191 – Proceso de prestación de un dispositivo IP de LAN en el sector LAN-Trans

Cuadro 51/J.191 – Descripción del flujo del proceso de prestación LAN-Trans del PS

Fase	Prestación de dirección LAN-Trans del cliente	Secuencia ordinaria	Secuencia de fallo
CHPSLT-1	*Mensaje de difusión DHCP Discover* El Cliente[a)] envía un mensaje de difusión DHCP DISCOVER por su LAN[b)] 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 CHPSWD-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 broadcast[c)] específico del enlace.	Continuar en CHPSLT-4.	Si falla, el cliente cancelará el temporizador del protocolo DHCP y se repetirá CHPSWD-1.

Cuadro 51/J.191 – Descripción del flujo del proceso de prestación LAN-Trans del PS

Fase	Prestación de dirección LAN-Trans del cliente	Secuencia ordinaria	Secuencia de fallo
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).	Prestación completada	Si falla, el cliente cancelará el temporizador del protocolo DHCP y se repetirá CHPSWD-1.

a) Si el cliente conociera la dirección IP anterior (por ejemplo, tras un rearranque), podría omitir el DHCP DISCOVER y continuar en la fase 3.

b) Si el cliente se encuentra en una red que no es de difusión se espera que envíe el mensaje al servidor DHCP en unidifusión.

c) Si el cliente se encuentra en una red que no es de multidifusión se espera que envíe el mensaje al PS en unidifusión.

13.6.1 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 18.

13.7 Proceso de prestación: Cliente DHCP en el sector LAN-Pass

Algunas aplicaciones del cliente 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 44 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 prestación para el dispositivo IP de LAN del sector LAN-Pass DEBE realizarse de acuerdo con la secuencia descrita en la figura 44 y expuesta en detalle en el cuadro 52.

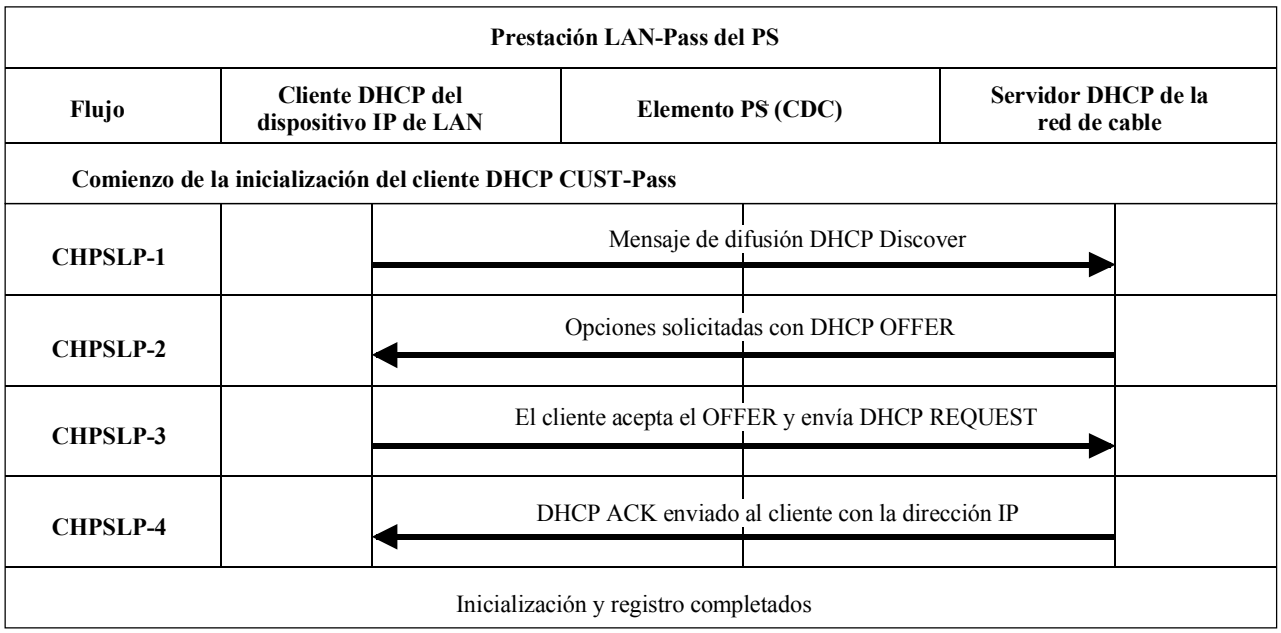


Figura 44/J.191 – Proceso de prestación para dispositivo IP de LAN en el sector LAN-Pass

Cuadro 52/J.191 – Descripción del flujo del proceso de prestación LAN-Pass

Fase	Prestación 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[a)] 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.

Cuadro 52/J.191 – Descripción del flujo del proceso de prestación LAN-Pass

Fase	Prestación de dirección transferencia del cliente	Secuencia ordinaria	Secuencia de fallo
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.	Prestación completada.	Si falla, el dispositivo IP de LAN cancelará el temporizador del protocolo DHCP y se repetirá CHPSLP-1.
a) 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

MIB Objects

Este anexo contiene la relación de todos los objetos de la MIB necesarios, indicados en 6.3.7.

MIB NOMBRE/Parámetro	**Acceso máximo**	**Se conserva**
mib-2		
system		
sysDescr	sólo lectura	Sí
sysObjectID	sólo lectura	Sí
sysUpTime	sólo lectura	No
sysContact	sólo lectura	Sí
sysName	sólo lectura	Sí
sysLocation	sólo lectura	Sí
sysServices	sólo lectura	Sí
interfaces [RFC 2863]		
ifNumber	sólo lectura	No
ifTable/ifEntry		
ifIndex	sólo lectura	No
ifDescr	sólo lectura	No
ifType	sólo lectura	No
ifMtu	sólo lectura	No

ifSpeed	sólo lectura	No
ifPhysAddress	sólo lectura	No
ifAdminStatus	lectura-escritura	No
ifOperStatus	sólo lectura	No
ifLastChange	sólo lectura	No
ifInOctets	sólo lectura	No
ifInUcastPkts	sólo lectura	No
ifInNUcastPkts	sólo lectura	No
ifInDiscards	sólo lectura	No
ifInErrors	sólo lectura	No
ifInUnknownProtos	sólo lectura	No
ifOutOctets	sólo lectura	No
ifOutUcastPkts	sólo lectura	No
ifOutNUcastPkts	sólo lectura	No
ifOutDiscards	sólo lectura	No
ifOutErrors	sólo lectura	No
ifOutQLen	sólo lectura	No
ifSpecifc	sólo lectura	No
ip [RFC 2011]		
ipForwarding	lectura-escritura	No
ipDefaultTTL	lectura-escritura	No
ipInReceives	sólo lectura	No
ipInHdrErrors	sólo lectura	No
ipInAddrErrors	sólo lectura	No
ipForwDatagrams	sólo lectura	No
ipInUnknownProtos	sólo lectura	No
ipInDiscards	sólo lectura	No
ipInDelivers	sólo lectura	No
ipOutRequests	sólo lectura	No
ipOutDiscards	sólo lectura	No
ipOutNoRoutes	sólo lectura	No
ipReasmTimeout	sólo lectura	No
ipReasmReqds	sólo lectura	No
ipReasmOKs	sólo lectura	No
ipReasmFails	sólo lectura	No
ipFragOKs	sólo lectura	No
ipFragFails	sólo lectura	No
ipFragCreates	sólo lectura	No
ipNetToMediaTable/ipNetToMediaEntry		
ipNetToMediaIfIndex	lectura-creación	No
ipNetToMediaPhyAddress	lectura-creación	No
ipNetToMediaNetAddress	lectura-creación	No
ipNetToMediaType	lectura-creación	No

icmp		
icmpInMsgs	sólo lectura	No
icmpInErrors	sólo lectura	No
icmpInDestUnreachs	sólo lectura	No
icmpInTimeExcds	sólo lectura	No
icmpInParmProbs	sólo lectura	No
icmpInSrcQuenchs	sólo lectura	No
icmpInRedirects	sólo lectura	No
icmpInEchos	sólo lectura	No
icmpInEchosReps	sólo lectura	No
icmpInTimestamps	sólo lectura	No
icmpInTimestampsReps	sólo lectura	No
icmpInAddrMasks	sólo lectura	No
icmpInAddrMaskReps	sólo lectura	No
icmpOutMsgs	sólo lectura	No
icmpOutErrors	sólo lectura	No
icmpOutDestUnreachs	sólo lectura	No
icmpOutTimeExcds	sólo lectura	No
icmpOutParmProbs	sólo lectura	No
icmpOutSrcQuenchs	sólo lectura	No
icmpOutRedirects	sólo lectura	No
icmpOutEchos	sólo lectura	No
icmpOutEchosReps	sólo lectura	No
icmpOutTimestamps	sólo lectura	No
icmpOutTimestampReps	sólo lectura	No
icmpOutAddrMasks	sólo lectura	No
icmpOutAddrMaskReps	sólo lectura	No
udp [RFC 2013]		
udpInDatagrams	sólo lectura	No
udpNoPorts	sólo lectura	No
udpInErrors	sólo lectura	No
udpOutDatagrams	sólo lectura	No
udpTable/udpEntry		
udpLocalAddress	sólo lectura	No
udpLocalPort	sólo lectura	No
transmission [RFC draft-ietf-ipcdn-bpiplus-mib-06.txt]		
docsIfMib		
docsBpi2MIB		
docsBpi2MIBObjects		
docsBpi2CmObjects		
docsBpi2CmCertObjects		
docsBpi2CmDeviceCertTable/docsBpi2CmDeviceCertEntry		
docsBpi2CmDeviceCmCert	lectura-escritura	Sí

docsBpi2CmDeviceManufCert	sólo lectura	Sí
docsBpi2CodeDownloadControl		
docsBpi2CodeDownloadStatusCode	sólo lectura	Sí
docsBpi2CodeDownloadStatusString	sólo lectura	Sí
docsBpi2CodeMfgOrgName	sólo lectura	Sí
docsBpi2CodeMfgCodeAccessStart	sólo lectura	Sí
docsBpi2CodeMfgCvcAccessStart	sólo lectura	Sí
docsBpi2CodeCoSignerOrgName	sólo lectura	Sí
docsBpi2CodeCoSignerCodeAccessStart	sólo lectura	Sí
docsBpi2CodeCoSignerCvcAccessStart	sólo lectura	Sí
docsBpi2CodeCvcUpdate	lectura-escritura	Sí
snmp [RFC 1907]		
snmpInPkts	sólo lectura	No
snmpOutPkts	sólo lectura	No
snmpInBadVersions	sólo lectura	No
snmpInBadCommunityNames	sólo lectura	No
snmpInBadCommunityUses	sólo lectura	No
snmpInASNParseErrs	sólo lectura	No
snmpInTooBigs	sólo lectura	No
snmpInNoSuchNames	sólo lectura	No
snmpInBadValues	sólo lectura	No
snmpInReadOnlys	sólo lectura	No
snmpInGenErrs	sólo lectura	No
snmpInTotalReqVars	sólo lectura	No
snmpInTotalSetVars	sólo lectura	No
snmpInGetRequests	sólo lectura	No
snmpInGetNexts	sólo lectura	No
snmpInSetRequests	sólo lectura	No
snmpInGetResponses	sólo lectura	No
snmpInTraps	sólo lectura	No
snmpOutTooBigs	sólo lectura	No
snmpOutNoSuchNames	sólo lectura	No
snmpOutBadValues	sólo lectura	No
snmpOutGenErrs	sólo lectura	No
snmpOutGetRequests	sólo lectura	No
snmpOutGetNexts	sólo lectura	No
snmpOutSetRequests	sólo lectura	No
snmpOutGetResponses	sólo lectura	No
snmpOutTraps	sólo lectura	No
snmpEnableAuthenTraps	lectura-escritura	No
snmpSilentDrops	sólo lectura	No
snmpProxyDrops	sólo lectura	No
ifMIB [RFC 2863]		

ifMIBOjects		
ifXTable/ifXEntry		
ifName	sólo lectura	No
ifInMulticastPkts	sólo lectura	No
ifInBroadcastPkts	sólo lectura	No
ifOutMulticastPkts	sólo lectura	No
ifOutBroadcastPkts	sólo lectura	No
ifHCInOctets	sólo lectura	No
ifHCInUcastPkts	sólo lectura	No
ifHCInMulticastPkts	sólo lectura	No
ifHCInBroadcastPkts	sólo lectura	No
ifHCOutOctets	sólo lectura	No
ifHCOutUcastPkts	sólo lectura	No
ifHCOutMulticastPkts	sólo lectura	No
ifHCOutBroadcastPkts	sólo lectura	No
ifLinkUpDownTrapEnable	lectura-escritura	No
ifHighSpeed	sólo lectura	No
ifPromiscuousMode	lectura-escritura	No
ifConnectorPresent	sólo lectura	No
ifAlias	lectura-escritura	No
ifCounterDiscontinuitityTime	sólo lectura	No
docsDev [RFC 2669]		
docsDevMIBObjects		
docsDevNmAccessTable/docsDevNmAccessEntry		
docsDevNmAccessIndex	inaccesible	No
docsDevNmAccessIp	lectura-creación	No
docsDevNmAccessIpMask	lectura-creación	No
docsDevNmAccessCommunity	lectura-creación	No
docsDevNmAccessControl	lectura-creación	No
docsDevNmAccessInterfaces	lectura-creación	No
docsDevNmAccessStatus	lectura-creación	No
docsDevSoftware		
docsDevSwServer	lectura-escritura	Sí
docsDevSwFilename	lectura-escritura	Sí
docsDevSwAdminStatus	lectura-escritura	Sí
docsDevSwOperStatus	sólo lectura	Sí
docsDevSwCurrentVers	sólo lectura	Sí
docsDevEvent		
docsDevEvControl	lectura-escritura	No
docsDevEvSyslog	lectura-escritura	No
docsDevEvThrottleAdminStatus	lectura-escritura	No
docsDevEvThrottleInhibited	sólo lectura	No
docsDevEvThrottleThreshold	lectura-escritura	No

docsDevEvThrottleInterval	lectura-escritura	No
docsDevEvControlTable/docsDevEvControlEntry		
docsDevEvPriority	inaccesible	No
docsDevEvReporting	lectura-escritura	No
docsDevEventTable/docsDevEventEntry		
docsDevEvIndex	inaccesible	Sí
docsDevEvFirstTime	sólo lectura	Sí
docsDevEvLastTime	sólo lectura	Sí
docsDevEvCounts	sólo lectura	Sí
docsDevEvLevel	sólo lectura	Sí
docsDevEvId	sólo lectura	Sí
docsDevEvText	sólo lectura	Sí
private		
enterprises		
cableLabs		
clabProject		
clabProjCableHome		
cabhPsDevMib		
cabhPsDevBase		
cabhPsDevDateTime	lectura-escritura	No
cabhPsDevResetNow	lectura-escritura	No
cabhPsDevSerialNumber	sólo lectura	Sí
cabhPsDevHardwareVersion	sólo lectura	Sí
cabhPsdevMacAddress	sólo lectura	Sí
cabhPsDevTypeIdentifier	sólo lectura	Sí
cabhPsDevResetDefaults	lectura-escritura	No
cabhPsDevWanManClientId	lectura-escritura	Sí
cabhPsDevTodSyncStatus	sólo lectura	No
cabhPsDevProvMode	sólo lectura	No
cabhPsDevDwnldMode	sólo lectura	No
cabhPsDevProv		
cabhPsDevProvisioningTimer	lectura-escritura	Sí
cabhPsDevProvConfigFile	lectura-escritura	No
cabhPsDevProvConfigHash	lectura-escritura	No
cabhPsDevProvConfigFileSize	sólo lectura	No
cabhPsDevProvConfigTLVProcessed	sólo lectura	No
cabhPsDevProvConfigTLVRejected	sólo lectura	No
cabhPsDevProvSolicitedKeyTimeout	lectura-escritura	Sí
cabhPsDevProvState	sólo lectura	No
cabhPsDevProvAuthState	sólo lectura	No
cabhPsDevProvCorrelationId	sólo lectura	No
cabhPsDevServerType	sólo lectura	No
cabhPsDevServerTime	sólo lectura	No

cabhSecMib		
cabhSecFwObjects		
cabhSecFwBase		
cabhSecFwPolicyFileEnable	lectura-escritura	Sí
cabhSecFwPolicyFileURL	lectura-escritura	No
cabhSecFwPolicyFileHash	lectura-escritura	No
cabhSecFwPolicyFileOperStatus	sólo escritura	No
cabhSecFwPolicyFileCurrentVersion	lectura-escritura	Sí
cabhSecFwLogCtl		
cabhSecFwEventType1Enable	lectura-escritura	Sí
cabhSecFwEventType2Enable	lectura-escritura	Sí
cabhSecFwEventType3Enable	lectura-escritura	Sí
cabhSecFwEventAttachAlertThreshold	lectura-escritura	Sí
cabhSecFwEventAttackAlertPeriod	lectura-escritura	Sí
cabhCapMib		
cabhCapObjects		
cabhCapBase		
cabhCapTcpTimeWait	lectura-escritura	Sí
cabhCapUdpTimeWait	lectura-escritura	Sí
cabhCapIcmpTimeWait	lectura-escritura	Sí
cabhCapPrimaryMode	lectura-escritura	Sí
cabhCapSetToFactory	lectura-escritura	No
cabhCapMap		
cabhCapMappingTable/cabhCapMappingEntry		
cabhCapMappingWanAddrType	inaccesible	Sí[1]
cabhCapMappingWanAddrType	inaccesible	Sí[1]
cabhCapMappingWanPort	inaccesible	Sí[1]
cabhCapMappingLanAddrType	inaccesible	Sí[1]
cabhCapMappingLanAddrType	inaccesible	Sí[1]
cabhCapMappingLanPort	inaccesible	Sí[1]
cabhCapMappingMode	sólo lectura	Sí[1]
cabhCapMappingMethod	sólo lectura	Sí[1]
cabhCapMappingProtocol	sólo lectura	Sí[1]
cabhCapPassthroughTable/cabhCapPassthroughEntry		
cabhCapPassthroughMACAddr	inaccesible	Sí
cabhCapPassthroughRowStatus	lectura-creación	No
cabhCdpMib		
cabhCdpObjects		
cabhCdpBase		
cabhCdpSetToFactory	lectura-escritura	No

[1] Los objetos cabhCapMappingEntry se mantienen si los ha provisto el NMS y no se mantienen si se han creado dinámicamente en base el tráfico saliente. Consúltese 8.3.2.2.

cabhCdpLanTransCurCount	sólo lectura	No
cabhCdpLanTransThreshold	lectura-escritura	Sí
cabhCdpLanTransAction	lectura-escritura	Sí
cabhCdpAddr		
cabhCdpLanAddrTable/cabhCdpLanAddrEntry		
cabhCdpLanAddrIpType	inaccesible	Sí
cabhCdpLanAddrIp	inaccesible	Sí
cabhCdpLanAddrClientID	sólo lectura	Sí
cabhCdpLanAddrCreateTime	sólo lectura	Sí
cabhCdpLanAddrExpireTime	sólo lectura	Sí
cabhCdpLanAddrMethod	sólo lectura	Sí
cabhCdpLanAddrHostName	sólo lectura	Sí
cabhCdpLanAddrRowStatus	lectura-creación	No
cabhCdpWanDataAddrTable/cabhCdpWanDataAddrEntry		
cabhCdpWanDataAddrIndex	inaccesible	Sí
cabhCdpWanDataAddrClientId	lectura-creación	Sí
cabhCdpWanDataAddrIpType	lectura-creación	No
cabhCdpWanDataAddrIp	lectura-creación	No
cabhCdpWanDataAddrAddrRenewalTime	lectura-creación	No
cabhCdpWanDataAddrRowStatus	lectura-creación	No
cabhCdpWanDataAddrServerTable/cabhCdpWanDataAddrServerEntry		
cabhCdpWanDataAddrDnsIpType	inaccesible	No
cabhCdpWanDataAddrDnsIp	inaccesible	No
cabhCdpWanDataAddrDnsRowStatus	lectura-creación	No
cabhCdpServer		
cabhCdpLanPoolStartType	lectura-escritura	Sí
cabhCdpLanPoolStart	lectura-escritura	Sí
cabhCdpLanPoolEndType	lectura-escritura	Sí
cabhCdpLanPoolEnd	lectura-escritura	Sí
cabhCdpServerSubnetMaskType	lectura-escritura	Sí
cabhCdpServerSubnetMask	lectura-escritura	Sí
cabhCdpServerTimeOffset	lectura-escritura	Sí
cabhCdpServerRouterType	lectura-escritura	Sí
cabhCdpServerRouter	lectura-escritura	Sí
cabhCdpServerDnsAddressType	lectura-escritura	Sí
cabhCdpServerDnsAddress	lectura-escritura	Sí
cabhCdpServerSyslogAddressType	lectura-escritura	Sí
cabhCdpServerSyslogAddress	lectura-escritura	Sí
cabhCdpServerDomainName	lectura-escritura	Sí
cabhCdpServerTTL	lectura-escritura	Sí
cabhCdpServerInterfaceMTU	lectura-escritura	Sí
cabhCdpServerVendorSpecific	lectura-escritura	Sí
cabhCdpServerLeaseTime	lectura-escritura	Sí

cabhCdpServerDhcpAddressType	lectura-escritura	Sí
cabhCdpServerDhcpAddress	lectura-escritura	Sí
cabhCtpMib		
cabhCtpObjects		
cabhCtpBase		
cabhCtpReset	lectura-escritura	No
cabpCtpConnSpeed		
cabhCtpConnSrcIpType	lectura-escritura	No
cabhCtpConnSrcIp	lectura-escritura	No
cabhCtpConnDestIpType	lectura-escritura	No
cabhCtpConnDestIp	lectura-escritura	No
cabhCtpConnProto	lectura-escritura	No
cabhCtpConnPort	lectura-escritura	No
cabhCtpConnNumPkts	lectura-escritura	No
cabhCtpConnPktSize	lectura-escritura	No
cabhCtpConnTimeOut	lectura-escritura	No
cabhCtpConnControl	lectura-escritura	No
cabhCtpConnStatus	lectura-sólo	No
cabhCtpConnPktsSent	lectura-sólo	No
cabhCtpConnPktsRecv	lectura-sólo	No
cabhCtpConnAvgRTT	lectura-sólo	No
cabhCtpConnMaxRTT	lectura-sólo	No
cabhCtpConnMinRTT	lectura-sólo	No
cabhCtpConnNumIcmpError	lectura-sólo	No
cabhCtpConnIcmpError	lectura-sólo	No
cabhCtpPing		
cabhCtpPingSrcIpType	lectura-escritura	No
cabhCtpPingSrcIp	lectura-escritura	No
cabhCtpPingDestIpType	lectura-escritura	No
cabhCtpPingDestIp	lectura-escritura	No
cabhCtpPingProto	lectura-escritura	No
cabhCtpPingNumPkts	lectura-escritura	No
cabhCtpPingPktSize	lectura-escritura	No
cabhCtpPingTimeBetween	lectura-escritura	No
cabhCtpPingTimeOut	lectura-escritura	No
cabhCtpPingControl	lectura-escritura	No
cabhCtpPingStatus	sólo lectura	No
cabhCtpPingNumSent	sólo lectura	No
cabhCtpPingNumRecv	sólo lectura	No
experimental		
snmpUSMDHObjectsMIB [RFC 2786]		
usmDHKeyObjects		
usmDHPublicObjects		

usmDHPParameters	lectura-escritura	No
usmDHUserKeyTable/usmDHUserKeyEntry		
usmDHUserAuthKeyChange	lectura-creación	No
usmDHUserOwnAuthKeyChange	lectura-creación	No
usmDHUserPrivKeyChange	lectura-creación	No
usmDHUserOwnPrivKeyChange	lectura-creación	No
usmDHKickstartGroup		
usmDHKickstartTable/usmDHKickstartEntry		
usmDHKickstartIndex	inaccesible	No
usmDHKickstartMyPublic	sólo lectura	No
usmDHKickstartMgrPublic	sólo lectura	No
usmDHKickstartSecurityName	sólo lectura	No
snmpV2		
snmpModules		
snmpMIB		
snmpMIBObjects		
snmpSet		
snmpSetSerialNo	lectura-escritura	No
snmpFrameworkMIB [RFC 2571]		
snmpEngine		
snmpEngineID	sólo lectura	Sí
snmpEngineBoots	sólo lectura	Sí
snmpEngineTime	sólo lectura	No
snmpEngineMaxMessageSize	sólo lectura	Sí
snmpMPDMIB [RFC 2572]		
snmpMPDObjects		
snmpMPDStats		
snmpUnknownSecurityModels	sólo lectura	No
snmpInvalidMsgs	sólo lectura	No
snmpUnknownPDUHandlers	sólo lectura	No
snmpTargetMIB [RFC 2573]		
snmpTargetObjects		
snmpTargetSpinLock	lectura-escritura	No
snmpTargetAddrTable/snmpTargetAddrEntry		
snmpTargetAddrName	inaccesible	No
snmpTargetAddrTDomain	lectura-creación	No
snmpTargetAddrTAddress	lectura-creación	No
snmpTargetAddrTimeout	lectura-creación	No
snmpTargetAddrRetryCount	lectura-creación	No
snmpTargetAddrTagList	lectura-creación	No
snmpTargetAddrParams	lectura-creación	No
snmpTargetAddrStorageType	lectura-creación	No
snmpTargetAddrRowStatus	lectura-creación	No

snmpTargetParamsTable/snmpTargetParamsEntry		
snmpTargetParamsName	inaccesible	No
snmpTargetParamsMPModel	lectura-creación	No
snmpTargetParamsSecurityModel	lectura-creación	No
snmpTargetParamsSecurityName	lectura-creación	No
snmpTargetParamsSecurityLevel	lectura-creación	No
snmpTargetParamsStorageType	lectura-creación	No
snmpTargetParamsRowStatus	lectura-creación	No
snmpUnavailableContexts	sólo lectura	No
snmpUnknownContexts	sólo lectura	No
snmpNotificationMIB [RFC 2573]		
snmpNotifyObjects		
snmpNotifyTable/snmpNotifyEntry		
snmpNotifyName	inaccesible	No
snmpNotifyTag	lectura-creación	No
snmpNotifyType	lectura-creación	No
snmpNotifyStorageType	lectura-creación	No
snmpNotifyRowStatus	lectura-creación	No
snmpNotifyFilterProfileTable/snmpNotifyFilterProfileEntry		
snmpNotifyFilterProfileName	lectura-creación	No
snmpNotifyFilterProfileStorType	lectura-creación	No
snmpNotifyFilterProfileRowStatus	lectura-creación	No
snmpNotifyFilterTable/snmpNotifyFilterEntry		
snmpNotifyFilterSubtree	inaccesible	No
snmpNotifyFilterMask	lectura-creación	No
snmpNotifyFilterType	lectura-creación	No
snmpNotifyFilterStorageType	lectura-creación	No
snmpNotifyFilterRowStatus	lectura-creación	No
snmpUsmMIB [RFC 2574]		
usmStats		
usmStatsUnsupportedSecLevels	sólo lectura	No
usmStatsNotInTimeWindows	sólo lectura	No
usmStatsUnknownUserNames	sólo lectura	No
usmStatsUnknownEngineIDs	sólo lectura	No
usmStatsWrongDigests	sólo lectura	No
usmStatsDecryptionErrors	sólo lectura	No
usmUser		
usmUserSpinLock	lectura-escritura	No
usmUserTable/usmUserEntry		
usmUserEngineID	inaccesible	No
usmUserName	inaccesible	No
usmUserSecurityName	sólo lectura	No
usmUserCloneFrom	lectura-creación	No

usmUserAuthProtocol	lectura-creación	No
usmUserAuthKeyChange	lectura-creación	No
usmUserOwnAuthKeyChange	lectura-creación	No
usmUserPrivProtocol	lectura-creación	No
usmUserPrivKeyChange	lectura-creación	No
usmUserOwnPrivKeyChange	lectura-creación	No
usmUserPublic	lectura-creación	No
usmUserStorageType	lectura-creación	No
usmUserStatus	lectura-creación	No
SNMP-VIEW-BASED-ACM-MIB [RFC 2575]		
snmpVacmMIB		
vacmMIBObjects		
vacmContextTable/vacmContextEntry		
vacmContextName	sólo lectura	No
vacmSecurityToGroupTable/vacmSecurityToGroupEntry		
vacmSecurityModel	inaccesible	No
vacmSecurityName	inaccesible	No
vacmGroupName	lectura-creación	No
vacmSecurityToGroupStorageType	lectura-creación	No
vacmSecurityToGroupStatus	lectura-creación	No
vacmAccessTable/vacmAccessEntry		
vacmAccessContextPrefix	inaccesible	No
vacmAccessSecurityModel	inaccesible	No
vacmAccessSecurityLevel	inaccesible	No
vacmAccessContextMatch	lectura-creación	No
vacmAccessReadViewName	lectura-creación	No
vacmAccessWriteViewName	lectura-creación	No
vacmAccessNotifyViewName	lectura-creación	No
vacmAccessStorageType	lectura-creación	No
vacmAccessStatus	lectura-creación	No
vacmMIBViews		
vacmViewSpinLock	lectura-escritura	No
vacmViewTreeFamilyTable/vacmViewTreeFamilyEntry		
vacmViewTreeFamilyViewName	inaccesible	No
vacmViewTreeFamilySubtree	inaccesible	No
vacmViewTreeFamilyMask	lectura-creación	No
vacmViewTreeFamilyType	lectura-creación	No
vacmViewTreeFamilyStorageType	lectura-creación	No
vacmViewTreeFamilyStatus	lectura-creación	No
snmpCommunityMIB [RFC 2576]		
snmpCommunityMIBObjects		
snmpCommunityTable/snmpCommunityEntry		
snmpCommunityIndex	inaccesible	No

snmpCommunityName	lectura-creación	No
snmpCommunitySecurityName	lectura-creación	No
snmpCommunityContextEngineID	lectura-creación	No
snmpCommunityContextName	lectura-creación	No
snmpCommunityTransportTag	lectura-creación	No
snmpCommunityStorageType	lectura-creación	No
snmpCommunityStatus	lectura-creación	No
snmpTargetAddrExtTable/snmpTargetAddrExtEntry		
snmpTargetAddrTMask	lectura-creación	No
snmpTargetAddrMMS	lectura-creación	No
snmpTrapAddress	accesible para notificación	No
snmpTrapCommunity	accesible para notificación	No

Anexo B

Formato y contenido de los eventos, SYSLOG y Trap SNMP

El cuadro B.1 resume el formato y el contenido de las anotaciones históricas de eventos, de los mensajes SYSLOG y SNMP trap.

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 SNMP trap 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 B.1 se expresan en formato decimal.

Para ilustrar más adecuadamente el cuadro B.1, 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

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 prestación							
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	Falló DHCP – La respuesta no contiene todos los campos válidos descritos en la Recomendación		D03.1	68000301	
Errores de TOD antes de completar la prestación							
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 prestación							
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	

Cuadro B.1/J.191 – Eventos definidos

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	Crítica	Fichero TFTP completo – pero falló la verificación de integridad del mensaje (MIC)	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							
Inicialización	TFTP	Notificación	TFTP conseguido		D10.0	68001000	
Análisis sintáctico TLV							
Inicialización	TLV parsing	Notificación	TLV-28 – OID no reconocida		I401.0	73040100	cabhPsDevInitTLVUnknownTrap
Inicialización	TLV parsing	Notificación	TLV desconocida <P1>	Únicamente para SYSLOG: <P1> = el TLV completo en hexadecimal	I401.1	73040101	cabhPsDevInitTLVUnknownTrap
Inicialización	TLV parsing	Notificación	Formato o contenido TLV no válido <P1>	Únicamente para SYSLOG: <P1> = el TLV completo en hexadecimal	I401.2	73040102	
Prestación							
Inicialización	SNMP Inform	Notificación	SNMP Inform enviado para indicar que se ha completado la prestación (pass/fail)	Únicamente para SYSLOG, añadir dirección MAC: <P1>. P1 = dirección MAC del PS	I11.0	73001100	cabhPsDevInitTrap
Inicialización	Retransmisión de SNMP Inform	Crítica	SNMP Inform enviado para indicar que se ha completado la prestación (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	cabhPsDevInitRetryTrap

Cuadro B.1/J.191 – Eventos definidos

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 de actualización del SW							
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
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							
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

Cuadro B.1/J.191 – Eventos definidos

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 – 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
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

Cuadro B.1/J.191 – Eventos definidos

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 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

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							
Actualización del SW	Éxito de la actualización del SW	Notificación	Éxito del software 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 software 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 prestación					D100.0	68010000	
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

Cuadro B.1/J.191 – Eventos definidos

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
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 prestación							
TOD	TOD	Alarma	Petición TOD enviada – no se recibe respuesta		D04.3	68000403	cabhPsDev TODFailTrap
TOD	TOD	Alarma	Respuesta TOD recibida – formato de datos no válido		D04.4	68000404	cabhPsDev TODFailTrap
Verificación del fichero de código					E200		
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

Cuadro B.1/J.191 – Eventos definidos

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 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
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

Cuadro B.1/J.191 – Eventos definidos

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	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					P		
CDP	CDS	Notificación	Intento de asignar más direcciones IP LAN-Trans de las permitidas		P01.0	80000100	cabhPsDev CDPTrap
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

Cuadro B.1/J.191 – Eventos definidos

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	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
Eventos CAP							
CAP	C-NAT	Notificación	CAP incapaz de establecer la correspondencia C-NAT. No hay direcciones IP WAN-Data disponibles		P201.0	800201.00	cabhPsDev CAPTrap
CAP	C-NAPT	Notificación	CAP incapaz de establecer la correspondencia C-NAPT. No hay direcciones IP WAN disponibles		P250.0	800250.00	cabhPsDev CAPTrap

B.1 Descripción de las trampas

```
cabhPsDevInitTLVUnknownTrap NOTIFICATION-TYPE
      OBJECTS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress }
      STATUS current
      DESCRIPTION
            "Evento provocado por la detección de un TLV desconocido durante el
            proceso de análisis sintáctico del TLV. Los valores de
            docsDevEvLevel, docsDevId y DocsDevEvText proceden de la anotación
            histórica de dicho evento en el docsDevEventTable. El valor
            ifPhysAddress es la dirección MAC del PS. Esta parte de información
            es uniforme en todas las trampas PS."
      := { cabhPsDevTraps 1 }

cabhPsDevInitTrap NOTIFICATION-TYPE
      OBJECTS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevServerConfigFile,
                  number of TLVs,
                  number of skipped TLVs }
      STATUS current
      DESCRIPTION
            "Evento para comunicar que se ha completado el proceso de
            inicialización detectado en el PS.
            Los valores de docsDevEvLevel, docsDevId y docsDevEvText proceden de
            la anotación histórica de este evento en el docsDevEventTable. El
            valor de ifPhysAddress indica la dirección MAC del PS.
```

```
            DocsDevServerConfigFile es el nombre del fichero de configuración
            utilizado. Éste, el número de TLV del fichero de configuración y el
            número de TLV ignorados, deberán ponerse a 'none' si no se utiliza
            fichero de configuración alguno.
            Esta parte de la información es uniforme en todas las trampas PS."
      ::= { cabhPsDevTraps 2 }

cabhPsDevInitRetryTrap NOTIFICATION-TYPE
      OBJECTS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress }
      STATUS current
      DESCRIPTION
            "Evento para comunicar el fallo que ha tenido lugar durante el
            proceso de inicialización detectado en el PS.
            Los valores de docsDevEvLevel, docsDevId y docsDevEvText proceden de
            la anotación histórica de este evento en el docsDevEventTable. El
            valor de ifPhysAddress indica la dirección MAC del PS.
            Esta parte de la información es uniforme en todas las trampas PS."
      ::= { cabhPsDevTraps 3 }
cabhPsDevDHCPFailTrap NOTIFICATION-TYPE

      OBJECTS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevServerDhcp }
      STATUS current
      DESCRIPTION
            "Evento para comunicar el fallo de un servidor DHCP. El valor de
            docsDevServerDhcp es la dirección IP del servidor DHCP."
      ::= { cabhPsDevTraps 4 }

cabhPsDevSwUpgradeInitTrap NOTIFICATION-TYPE
      OBJECTS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevSwFilename,
                  docsDevSwServer }
      STATUS current
      DESCRIPTION
            "Evento para comunicar el inicio de una actualización de soporte
            lógico. Los valores de docsDevSwFilename y docsDevSwServer indican
            el nombre de la imagen de soporte lógico y la dirección IP del
            servidor del que procede la imagen."
      ::= { cabhPsDevTraps 5 }

cabhPsDevSwUpgradeFailTrap NOTIFICATION-TYPE
      OBJECTS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevSwFilename,
                  docsDevSwServer }
      STATUS current
      DESCRIPTION
            "Evento para comunicar el fallo del intento de actualización de
            soporte lógico. Los valores de docsDevSwFilename y docsDevSwServer
            indican el nombre de la imagen de soporte lógico y la dirección IP
            del servidor del que procede la imagen."
      ::= { cabhPsDevTraps 6 }
```

```
cabhPsDevSwUpgradeSuccessTrap NOTIFICATION-TYPE
      OBJECTS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevSwFilename,
                  docsDevSwServer }
      STATUS current
      DESCRIPTION
            "Evento para comunicar que se ha conseguido actualizar el soporte
            lógico. Los valores de docsDevSwFilename y docsDevSwServer indican
            el nombre de la imagen de soporte lógico  y la dirección IP del
            servidor del que procede la imagen."
      ::= { cabhPsDevTraps 7 }

cabhPsDevSwUpgradeCVCFailTrap NOTIFICATION-TYPE
      OBJECTS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress }
      STATUS current
      DESCRIPTION
            "Evento para comunicar el fallo de la verificación del fichero de
            código durante el intento de actualización segura de soporte
            lógico."
      ::= { cabhPsDevTraps 8 }

cabhPsDevTODFailTrap NOTIFICATION-TYPE
      OBJECTS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevServerTime }
      STATUS current
      DESCRIPTION
            "Evento para comunicar el fallo del servidor de hora del día. El
            valor de docsDevServerTime indica la dirección IP del servidor."
      ::= { cabhPsDevTraps 9 }

cabhPsDevCDPTrap NOTIFICATION-TYPE
      OBJECTS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  addressThreshold }
      STATUS current
      DESCRIPTION
            "Para comunicar un evento con el portal DHCP."
      ::= { cabhPsDevTraps 10 }

cabhPsDevCSPTrap   NOTIFICATION-TYPE
      OBJECTS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress }
      STATUS current
      DESCRIPTION
            "Para comunicar un evento con el portal de seguridad."
      ::= { cabhPsDevTraps 11 }

cabhPsDevCAPTrap   NOTIFICATION-TYPE
      OBJECTS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
```

```
                ifPhysAddress }
    STATUS current
    DESCRIPTION
          "Para comunicar un evento con el portal de seguridad."
    ::= { cabhPsDevTraps 12 }
```

Anexo C

Amenazas de seguridad y medidas preventivas

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 para abonados y operadores que se han advertido son las siguientes:

– **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 del hogar 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 el hogar.

  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.

– **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.

– **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.

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:

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.

– **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.

– **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.

– **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 aplicaciones domésticas, las barreras contra fuegos se suelen ubicar en los dispositivos domésticos de pasarela que conectan la red HFC al hogar.

  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.

– **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. Esta lista NO supone ninguna prioridad específica.

1) FTP.

2) Aplicaciones par-a-par (es decir, Gnutella, LimeWire, BearShare, Morpheus, etc.).

3) IPsec.

4) IGMP e IP Multicast.

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 multimedios (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.

Anexo E

MIB

E.1 MIB del servicio de portal (PS)

La MIB 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,
     DisplayString,
     PhysAddress,
     DateAndTime,
     TEXTUAL-CONVENTION
                                        FROM SNMPv2-TC
     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
                       FROM CABH-CDP-MIB

     clabProjCableHome
                                        FROM CLAB-DEF-MIB;
```

```
--============================================================================
--
--   History:
--============================================================================

cabhPsDevMib MODULE-IDENTITY
     LAST-UPDATED  "0112190000Z" -- December 19, 2001
     ORGANIZATION  "Cable    NMP Group"
     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 describe general PS Device attributes and
       behavior characteristics. Most the PS Device MIB is needed for
       configuration download.

-- Textual conventions
     X509Certificate ::= TEXTUAL-CONVENTION
       STATUS current
       DESCRIPTION
          "An X.509 digital certificate encoded as an ASN.1 DER object."
       SYNTAX OCTET STRING (SIZE (0..4096))

--
-- assumes SNMPv3
-- load management is per DOCSIS 1.1 only
--

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 time zone information."
     ::= { cabhPsDevBase 1 }

cabhPsDevResetNow OBJECT-TYPE
     SYNTAX        TruthValue
     MAX-ACCESS    read-write
     STATUS        current
     DESCRIPTION
       "Setting this object to true(1) causes the device to reset.
       Reading this object always returns false(2). When cabhPsDevResetNow is
       set to true, the following actions occur:
       1) Clear all statistics in PS.
       2) Clear trace logs.
       3) Clear all security associations.
       4) Initialize all configuration parameters
```

```
        5) Delete all address translations
        6) Delete all FQDN to IP mappings
        7) Delete all stored ARP translations
        8) The provisioning flow is started at step PS - 1."
      ::= { cabhPsDevBase 2 }

cabhPsDevSerialNumber OBJECT-TYPE
      SYNTAX        DisplayString (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        DisplayString (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 }

cabhPsDevMacAddress OBJECT-TYPE
      SYNTAX        PhysAddress
      MAX-ACCESS    read-only
      STATUS        current
      DESCRIPTION
        "The PS WAN-MAN MAC address. Typically, the PS WAN-MAN and PS
        WAN-DATA addresses will be identical. The client identifiers
        will not be the same so that each may be assigned a different
        IP address."
      ::= { cabhPsDevBase 5 }

cabhPsDevTypeIdentifier OBJECT-TYPE
      SYNTAX        DisplayString
      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 6 }

cabhPsDevResetDefaults OBJECT-TYPE
      SYNTAX        TruthValue
      MAX-ACCESS    read-write
      STATUS        current
      DESCRIPTION
        "Setting this object to True sets all PS parameters to the
        factory defaults"
      ::= { cabhPsDevBase 7 }

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 8 }

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."
    REFERENCE
      " "
    DEFVAL { false }
    ::= { cabhPsDevBase 9 }

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 receives PS Configuration File information (server
      address and file name) in the DHCP message issued by the DHCP server in
      the cable network, the PS sets this object to DHCPmode(1). If the PS
      receives DHCP option 177 sub-option 51 AND does not receive PS
      Configuration File information in the DHCP message the PS
      receives from the DHCP server in the cable network, the PS
      sets this object to SNMPmode(2)."
    ::= { cabhPsDevBase 10 }

cabhPsDevDwnldMode OBJECT-TYPE
    SYNTAX   INTEGER
    {
      standard    (1),
      enhanced    (2)
    }
    MAX-ACCESS    read-only
    STATUS        current
    DESCRIPTION
      "This is the download mode that the PS will used."
      ::= { 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
      time-out 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        DisplayString(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 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 }

cabhPsDevProvConfigTLVProcessed OBJECT-TYPE
     SYNTAX        INTEGER (0..16383)
     MAX-ACCESS    read-only
     STATUS        current
     DESCRIPTION
       "Number of TLVs processed in config file."
     ::={ cabhPsDevProv 5 }

cabhPsDevProvConfigTLVRejected OBJECT-TYPE
     SYNTAX        INTEGER (0..16383)
     MAX-ACCESS    read-only
     STATUS        current
     DESCRIPTION
       "Number of TLVs rejected in config file."
     ::={ cabhPsDevProv 6 }

cabhPsDevProvSolicitedKeyTimeout OBJECT-TYPE
     SYNTAX        Integer32 (15..600)
     UNITS         "seconds"
     MAX-ACCESS    read-write
     STATUS        current
     DESCRIPTION
       "This time-out 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 7 }

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 ompletion of the initialization
       flow. InProgress occurs from PS initialization start to PS
       initialization end."
       ::= { cabhPsDevProv 8 }

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 9 }

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 10 }

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 11 }

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 12 }

--
--   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,
       cabhPsDevMacAddress
     }
     STATUS current
     DESCRIPTION
       "Event due to detection of unknown TLV during the TLV parsing process.
       The values of docsDevEvLevel, docsDevId, and docsDevEvText are from the
       entry which logs this event in the docsDevEventTable. The value of
       cabhPsDevMacAddressindicates the 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,
       cabhPsDevMacAddress,
       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,
     cabhPsDevMacAddress
     }
     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,
       cabhPsDevMacAddress,
       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,
      cabhPsDevMacAddress,
      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,
      cabhPsDevMacAddress,
      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,
      cabhPsDevMacAddress,
      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,
      cabhPsDevMacAddress
    }
    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
    }
```

```
    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
    }
    STATUS    current
    DESCRIPTION
      "An event to report the failure of PS to obtain all needed WAN-Data
      IP Addresses.
      cabhCdpWanDataAddrClientId indicates the ClientId for which the failure
      occurred."
    ::= { cabhPsNotification 10 }

cabhPsDevCdpThresholdTrap NOTIFICATION-TYPE
    OBJECTS {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
      cabhPsDevMacAddress,
      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,
      cabhPsDevMacAddress
    }
    STATUS    current
    DESCRIPTION
      "To report an event with the Cable Security Portal."
    ::= { cabhPsNotification 12 }

cabhPsDevCapTrap NOTIFICATION-TYPE
    OBJECTS {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
      cabhPsDevMacAddress
    }
    STATUS    current
    DESCRIPTION
      "To report an event with the Cable Address Portal."
    ::= { cabhPsNotification 13 }

cabhPsDevProvEnrollTrap NOTIFICATION-TYPE
    OBJECTS {
      cabhPsDevHardwareVersion,
      docsDevSwCurrentVers,
      cabhPsDevTypeIdentifier,
      cabhPsDevMacAddress,
```

```
      cabhPsDevProvCorrelationId
    }
    STATUS    current
    DESCRIPTION
      "This inform is issued to initiate the process provisioning."
    REFERENCE
      "Inform as defined in RFC 1902."
    ::= { cabhPsNotification 14 }

-- 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 3 }

cabhPsGroup OBJECT-GROUP
    OBJECTS {
      cabhPsDevDateTime,
      cabhPsDevResetNow,
      cabhPsDevSerialNumber,
      cabhPsDevHardwareVersion,
      cabhPsDevMacAddress,
      cabhPsDevTypeIdentifier,
         cabhPsDevResetDefaults,
         cabhPsDevWanManClientId,
         cabhPsDevTodSyncStatus,
      cabhPsDevProvMode,
      cabhPsDevDwnldMode,

      cabhPsDevProvisioningTimer,
         cabhPsDevProvConfigFile,
         cabhPsDevProvConfigHash,
         cabhPsDevProvConfigFileSize,
         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, 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 CTP 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:
--
--============================================================================

cabhCtpMib MODULE-IDENTITY
     LAST-UPDATED  "0112190000Z" -- December 19, 2001
     ORGANIZATION       "Cable NMP Group"
     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 CableHome Testing Portal (CTP).
       Acknowledgements:
       "
     ::= { clabProjCableHome 5 }

-- Textual conventions

--
-- assumes SNMPv3
```

```
-- SW load management is per DOCSIS 1.1 only
--

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.
--

cabhCtpReset OBJECT-TYPE
       SYNTAX      TruthValue
       MAX-ACCESS  read-write
     STATUS        current
     DESCRIPTION
       "Setting this object to true(1) causes all testing to be
       terminated. Reading this object always returns false(2).
       When cabhCtpReset is set to true, the following actions occur:
       1) Terminate any diagnostic tests in progress.
       2) Clear all diagnostic statistics."
     ::= { 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.
       Typically the address with be the value in cabhCdpServerRouter. The
       default address is 192.168.0.1."
       REFERENCE
          "Specification Section 6.4.3.2"
       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 used as the destination address for the Connection
       Speed Test."
       ::= { 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 }

cabhCtpConnPort OBJECT-TYPE
        SYNTAX      INTEGER (1..65535)
        MAX-ACCESS  read-write
      STATUS        current
      DESCRIPTION
        "The port used for the Connection Speed Test."
      DEFVAL {7}
      ::= { cabhCtpConnSpeed 6 }

cabhCtpConnNumPkts OBJECT-TYPE
      SYNTAX        INTEGER (1..255)
      MAX-ACCESS    read-write
      STATUS        current
      DESCRIPTION
        "The number of packets to send."
        DEFVAL {1}
        ::= { cabhCtpConnSpeed 7 }

cabhCtpConnPktSize OBJECT-TYPE
        SYNTAX      INTEGER (64..1518)
        MAX-ACCESS  read-write
      STATUS        current
      DESCRIPTION
        "The size of the test frames."
        REFERENCE
        ""
        ::= { cabhCtpConnSpeed 8 }

cabhCtpConnTimeOut OBJECT-TYPE
        SYNTAX      INTEGER (0..600000)          -- Max 10 minutes
        UNITS       "milliseconds"
        MAX-ACCESS  read-write
      STATUS        current
      DESCRIPTION
        "The time-out value for the response. A value of zero indicates
        no time out and can be used for TCP only."
        DEFVAL {600000}
      ::= { cabhCtpConnSpeed 9 }

cabhCtpConnControl OBJECT-TYPE
          SYNTAX    INTEGER {
                        notRun        (1),
                        start         (2),
                        abort         (3)
                        }
```

```
      MAX-ACCESS  read-write
     STATUS        current
     DESCRIPTION
       "The control for Connection Speed Test. The value notRun
       is used to indicate never executed. This parameter should
       only be set via SNMP."
       DEFVAL { notRun(1) }
     ::= { cabhCtpConnSpeed 10 }

cabhCtpConnStatus OBJECT-TYPE
       SYNTAX      INTEGER {
                        running       (1),
                        complete      (2),
                        aborted       (3)
                   }
       MAX-ACCESS  read-only
     STATUS        current
     DESCRIPTION
       "The Status of the currently/last executed test."
       DEFVAL { complete(2) }
       ::= { cabhCtpConnSpeed 11 }

cabhCtpConnPktsSent OBJECT-TYPE
       SYNTAX      INTEGER (0..255)
     MAX-ACCESS    read-only
     STATUS        current
     DESCRIPTION
       "The number of packets sent."
       ::= { cabhCtpConnSpeed 12 }

cabhCtpConnPktsRecv OBJECT-TYPE
       SYNTAX      INTEGER (0..255)
       MAX-ACCESS  read-only
     STATUS        current
     DESCRIPTION
       "The number for packet received."
     ::= { cabhCtpConnSpeed 13 }

cabhCtpConnAvgRTT OBJECT-TYPE
     SYNTAX        INTEGER (0..600000)
     UNITS         "milliseconds"
     MAX-ACCESS    read-only
     STATUS        current
     DESCRIPTION
       "The resulting average of round-trip times for
       acknowledged packets."
       ::= { cabhCtpConnSpeed 14 }

cabhCtpConnMaxRTT OBJECT-TYPE
       SYNTAX      INTEGER (0..600000)
       UNITS       "milliseconds"
       MAX-ACCESS  read-only
     STATUS        current
     DESCRIPTION
       "The resulting maximum of round-trip times for
       acknowledged packets."
       ::= { cabhCtpConnSpeed 15 }

cabhCtpConnMinRTT OBJECT-TYPE
       SYNTAX      INTEGER (0..600000)
       UNITS       "milliseconds"
       MAX-ACCESS  read-only
     STATUS        current
     DESCRIPTION
```

```
       "The resulting minimum of round-trip times for
       acknowledged packets."
       ::= { cabhCtpConnSpeed 16 }

cabhCtpConnNumIcmpError OBJECT-TYPE
       SYNTAX      INTEGER (0..255)
       MAX-ACCESS  read-only
     STATUS        current
     DESCRIPTION
       "Number of ICMP errors."
       ::= { cabhCtpConnSpeed 17 }

cabhCtpConnIcmpError OBJECT-TYPE
       SYNTAX      INTEGER (0..255)
       MAX-ACCESS  read-only
     STATUS        current
     DESCRIPTION
       "The last ICMP error."
     ::= { cabhCtpConnSpeed 18 }

--
--   Parameters and Results for Ping Command
--

cabhCtpPingSrcIpType OBJECT-TYPE
       SYNTAX      InetAddressType
       MAX-ACCESS  read-write
     STATUS        current
     DESCRIPTION
       "The IP Address Type used as the source address for the Ping Test."
       ::= { 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. Typically the address will be the value of
       PS WanMan IP address. The address 192.168.0.x is used."
       ::= { cabhCtpPing 2 }

cabhCtpPingDestIpType OBJECT-TYPE
       SYNTAX      InetAddressType
       MAX-ACCESS  read-write
     STATUS        current
     DESCRIPTION
       "The Destination IP Address Type used as the destination address for
       the Ping Test."
       ::= { 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 }

cabhCtpPingProto OBJECT-TYPE
       SYNTAX      INTEGER {
                        icmp (1),
                        }
```

```
      MAX-ACCESS  read-write
     STATUS        current
     DESCRIPTION
       "The protocol used to gather topology info."
       DEFVAL { icmp }
     ::= { cabhCtpPing 5 }

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 6 }

cabhCtpPingPktSize OBJECT-TYPE
       SYNTAX      INTEGER (64..1518)
       MAX-ACCESS  read-write
     STATUS        current
     DESCRIPTION
       "The size of the test frames."
       DEFVAL {64}
       ::= { cabhCtpPing 7 }

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 8 }

cabhCtpPingTimeOut OBJECT-TYPE
       SYNTAX      INTEGER (0..600000)
       UNITS       "milliseconds"
       MAX-ACCESS  read-write
       STATUS      current
     DESCRIPTION
       "The time-out for ping response of sending a single ping."
       DEFVAL { 5000 }  -- 5 seconds
       ::= { cabhCtpPing 9 }

cabhCtpPingControl OBJECT-TYPE
       SYNTAX      INTEGER {
                        notRun        (1),
                        start         (2),
                        abort         (3)
                        }
       MAX-ACCESS  read-write
     STATUS        current
     DESCRIPTION
       "The control for Ping Test. The value notRun
       is used to indicate never executed."
       DEFVAL { notRun(1) }
       ::= { cabhCtpPing 10 }

cabhCtpPingStatus OBJECT-TYPE
       SYNTAX      INTEGER {
                        running       (1),
                        complete      (2),
```

```
                        aborted       (3)
                        }
      MAX-ACCESS  read-only
    STATUS        current
    DESCRIPTION
      "The Status of the currently/last executed test."
      ::= { cabhCtpPing 11 }

cabhCtpPingNumSent OBJECT-TYPE
      SYNTAX      INTEGER (0..255)
      MAX-ACCESS  read-only
    STATUS        current
    DESCRIPTION
      "The number of pings sent."
      DEFVAL { complete(2) }
      ::= { cabhCtpPing 12 }

cabhCtpPingNumRecv OBJECT-TYPE
      SYNTAX      INTEGER (0..255)
      MAX-ACCESS  read-only
    STATUS        current
    DESCRIPTION
      "The number of pings received."
      ::= { cabhCtpPing 13 }

--============================================================================

--
-- 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 {
      cabhCtpReset,
         cabhCtpConnSrcIpType,
         cabhCtpConnSrcIp,
         cabhCtpConnDestIpType,
         cabhCtpConnDestIp,
```

```
        cabhCtpConnProto,
        cabhCtpConnPort,
        cabhCtpConnNumPkts,
        cabhCtpConnPktSize,
        cabhCtpConnTimeOut,
        cabhCtpConnControl,
        cabhCtpConnStatus,
        cabhCtpConnPktsSent,
        cabhCtpConnPktsRecv,
        cabhCtpConnAvgRTT,
        cabhCtpConnMinRTT,
        cabhCtpConnMaxRTT,
        cabhCtpConnNumIcmpError,
        cabhCtpConnIcmpError,

        cabhCtpPingSrcIpType,
        cabhCtpPingSrcIp,
        cabhCtpPingDestIpType,
        cabhCtpPingDestIp,
        cabhCtpPingProto,
        cabhCtpPingNumPkts,
        cabhCtpPingPktSize,
        cabhCtpPingTimeBetween,
        cabhCtpPingTimeOut,
        cabhCtpPingControl,
        cabhCtpPingStatus,
        cabhCtpPingNumSent,
        cabhCtpPingNumRecv
      }
    STATUS    current
    DESCRIPTION
      "Group of objects for Cable 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-BPI2MIB
      clabProjCableHome     FROM CLAB-DEF-MIB;
```

```
--============================================================================
--
--   History:
--
--
--
--============================================================================

cabhSecMib MODULE-IDENTITY
     LAST-UPDATED  "0112200000Z" -- December 20, 2001
     ORGANIZATION       "Cable NMP Group"
     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.

       Acknowledgements:
       "
     ::= { clabProjCableHome 2 }

-- Textual conventions

--
-- assumes SNMPv3
-- SW load management is per DOCSIS 1.1 only
--

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
--   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
       "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 hash length
       160 bits."
     ::= { 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 time-out."

     ::= { cabhSecFwBase 4 }

cabhSecFwPolicyFileCurrentVersion OBJECT-TYPE
     SYNTAX        SnmpAdminString
     -- MAX-ACCESS read-only
     -- Write access added to allow factory configuration
     MAX-ACCESS    read-write
     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
```

```
      "Enables or disables logging of type 1 firewall event messages."
    ::= { cabhSecFwLogCtl 1 }

cabhSecFwEventType2Enable 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 2 firewall event messages."
    ::= { 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."
    ::= { 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."
    ::= { cabhSecFwLogCtl 4 }

cabhSecFwEventAttackAlertPeriod OBJECT-TYPE
    SYNTAX      INTEGER              (0..65535)
    MAX-ACCESS  read-write
    STATUS current
    DESCRIPTION
      "Indicates the period to be used (in days) for the
      cabhSecFwEventAttackAlertThreshold."
    ::= { cabhSecFwLogCtl 5 }
cabhSecCertPsCert OBJECT-TYPE
    SYNTAX      X509Certificate
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
      "The X.509 DER-encoded PS certificate."
    REFERENCE
      "Security Specification Section 11.3.2.2"
    ::= { 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 {
       cabhSecFwGroup
     }

::= { 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 MIB de definición

La MIB de definición DEBE implementarse como se define a continuación.

```
CLAB-DEF-MIB DEFINITIONS ::= BEGIN
IMPORTS
     MODULE-IDENTITY,
     enterprises
                                  FROM SNMPv2-SMI;

cableLabs MODULE-IDENTITY
     LAST-UPDATED  "0201310000Z" -- January 31, 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 }

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,
       DisplayString,
     RowStatus,
     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:
--
--
--
--============================================================================

cabhCdpMib MODULE-IDENTITY
     LAST-UPDATED  "0112190000Z" -- December 19, 2001
     ORGANIZATION  "Cable NMP Group"
     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 CDP and the CAP portions of the PS database.

      Acknowledgements:
      "
    ::= { clabProjCableHome 4 }

-- Textual conventions
CabhCdpLanTransDhcpClientId ::= TEXTUAL-CONVENTION
    STATUS  current
    DESCRIPTION
      "LAN-Trans DHCP option61 information."
    SYNTAX OCTET STRING (SIZE (1..80))

--
-- assumes SNMPv3
-- SW load management is per DOCSIS 1.1 only
--

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 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 and all
      current mappings to use the factory default settings at
      the next lease renewal time. Reading this object always
      returns false(2). When cabhCdpDhcpReset is set to true,
      the following actions occur:
      1) Reset all default CDS DHCP options to the factory
      defaults.
      2) The CDS will offer the factory default DHCP options
      at the next lease renewal time.

      The objects set to factory defaults are:
         cabhCdpLanTransThreshold,
         cabhCdpLanTransAction,

         cabhCdpLanPoolStart,
         cabhCdpLanPoolEnd,
         cabhCdpServerSubnetMask,
         cabhCdpServerTimeOffset,
         cabhCdpServerRouter,
         cabhCdpServerDnsAddress,
         cabhCdpServerSyslogAddress,
         cabhCdpServerDomainName,
         cabhCdpServerTTL,
         cabhCdpServerInterfaceMTU,
         cabhCdpServerVendorSpecific,
         cabhCdpServerLeaseTime,
```

```
          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 WAN side addresses."
        REFERENCE
           ""
      ::= { cabhCdpBase 2 }

cabhCdpLanTransThreshold OBJECT-TYPE
      SYNTAX    INTEGER (1..65533)
      MAX-ACCESS    read-write
      STATUS    current
      DESCRIPTION
        "The threshold number of LAN-Trans IP addresses
        allocated or assigned above which an alarm
        condition MUST be generated. Whenever an attempt
        to allocate an LAN-Trans IP address when
        cabhCdpLanTransCurCount is greater than or equal
        to cabhCdpLanTransThreshold, an event is generated.
        For class C addresses, 253 is used as default. For
        class B addresses, 65533 is used as a default. In
        either case, this setting disables the feature."
        REFERENCE
           ""
        DEFVAL { 65533 }
      ::= { 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 }

--
--   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.
--
--============================================================================

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,
       cabhCdpLanAddrCreateTime   TimeStamp,
       cabhCdpLanAddrExpireTime   TimeStamp,
       cabhCdpLanAddrMethod            INTEGER,
       cabhCdpLanAddrHostName          DisplayString,
       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."
     ::= { 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."
     ::= { cabhCdpLanAddrEntry 2 }

cabhCdpLanAddrClientID OBJECT-TYPE
     SYNTAX        CabhCdpLanTransDhcpClientId
     MAX-ACCESS    read-only
     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."
     ::= { cabhCdpLanAddrEntry 3 }

cabhCdpLanAddrCreateTime 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 set only 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 }

cabhCdpLanAddrExpireTime 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        DisplayString(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 requesting a WAN-Data IP Address
       via DHCP."
     ::= { cabhCdpWanDataAddrEntry 2 }

cabhCdpWanDataAddrIpType OBJECT-TYPE
     SYNTAX        InetAddressType
     MAX-ACCESS    read-create
     STATUS        current
     DESCRIPTION
       "The address type assigned on the WAN-Data side."
     ::= { cabhCdpWanDataAddrEntry 3 }

cabhCdpWanDataAddrIp OBJECT-TYPE
     SYNTAX        InetAddress
     MAX-ACCESS    read-create
     STATUS        current
     DESCRIPTION
       "The address assigned on the WAN-Data side."
     ::= { cabhCdpWanDataAddrEntry 4 }

cabhCdpWanDataAddrRenewalTime OBJECT-TYPE
     SYNTAX        Integer32
     MAX-ACCESS    read-create
     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 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."
       ::= { 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 }

cabhCdpServerSubnetMaskType OBJECT-TYPE
       SYNTAX      InetAddressType
     MAX-ACCESS    read-write
     STATUS        current
     DESCRIPTION
       "Type of LAN-Trans Subnet Mask."
     DEFVAL { ipv4 }
     ::= { cabhCdpServer 5 }

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 6 }

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 7 }

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 8 }

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 9 }

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 10 }

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 11 }

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 12 }

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 13 }

cabhCdpServerDomainName OBJECT-TYPE
        SYNTAX       DisplayString(SIZE(0..128))
      MAX-ACCESS     read-write
      STATUS         current
      DESCRIPTION
        "Option value 15 - Domain name of LAN-Trans address realm."
        DEFVAL {""}
        ::= { cabhCdpServer 14 }

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 15 }

cabhCdpServerInterfaceMTU OBJECT-TYPE
        SYNTAX       INTEGER (68..4096)
        MAX-ACCESS   read-write
      STATUS         current
      DESCRIPTION
        "Option value 26 - LAN-Trans Interface MTU."
        DEFVAL { 1500 }
        ::= { cabhCdpServer 16 }

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 17 }

cabhCdpServerLeaseTime OBJECT-TYPE
        SYNTAX       Unsigned32
        UNITS             "seconds"
        MAX-ACCESS   read-write
      STATUS         current
      DESCRIPTION
        "Option value 51 - LAN-Trans default Lease Time (seconds)."
        DEFVAL { 60 }
        ::= { cabhCdpServer 18 }
```

```
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 19 }

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 20 }

--
-- 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,

          cabhCdpLanAddrIpType,
          cabhCdpLanAddrIp,
          cabhCdpLanAddrClientID,
          cabhCdpLanAddrCreateTime,
          cabhCdpLanAddrExpireTime,
```

```
          cabhCdpLanAddrMethod,
          cabhCdpLanAddrHostName,
          cabhCdpLanAddrRowStatus,

          cabhCdpWanDataAddrIndex,
          cabhCdpWanDataAddrClientId,
          cabhCdpLanAddrIpType,
          cabhCdpWanDataAddrIp,
          cabhCdpWanDataAddrRenewalTime,
          cabhCdpWanDataAddrRowStatus,

          cabhCdpWanDataAddrDnsIpType,
          cabhCdpWanDataAddrDnsIp,
          cabhCdpWanDataAddrDnsRowStatus,

          cabhCdpLanPoolStartType,
          cabhCdpLanPoolStart,
          cabhCdpLanPoolEndType,
          cabhCdpLanPoolEnd,
          cabhCdpServerSubnetMaskType,
          cabhCdpServerSubnetMask,
          cabhCdpServerTimeOffset,
          cabhCdpServerRouterType,
          cabhCdpServerRouterType,
          cabhCdpServerRouter,
          cabhCdpServerDnsAddressType,
          cabhCdpServerDnsAddress,
          cabhCdpServerSyslogAddressType,
          cabhCdpServerSyslogAddress,
          cabhCdpServerDomainName,
          cabhCdpServerTTL,
          cabhCdpServerInterfaceMTU,
          cabhCdpServerVendorSpecific,
          cabhCdpServerLeaseTime,
          cabhCdpServerDhcpAddressType,
          cabhCdpServerDhcpAddress
              }
     STATUS   current
     DESCRIPTION
       "Group of objects for Cable CDB 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:
--
--
--============================================================================

cabhCapMib MODULE-IDENTITY
     LAST-UPDATED  "0112190000Z" -- December 19, 2001
     ORGANIZATION  "Cable NMP Group"
     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 CDP and the CAP portions of the PS database.

       Acknowledgements:
       "
     ::= { 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
                   }

--
-- assumes SNMPv3
-- SW load management is per DOCSIS 1.1 only
--

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
       "The maximum time to wait before assuming TCP
       session is terminated."
       REFERENCE
          ""
       DEFVAL { 240 }        -- 4 minutes
     ::= { cabhCapBase 1 }

cabhCapUdpTimeWait OBJECT-TYPE
     SYNTAX      Unsigned32
       UNITS     "seconds"
     MAX-ACCESS  read-write
     STATUS      current
     DESCRIPTION
       "The maximum time to wait before assuming UDP
       session is terminated."
       REFERENCE
          ""
       DEFVAL { 86400 } -- 1 day
     ::= { cabhCapBase 2 }

cabhCapIcmpTimeWait OBJECT-TYPE
     SYNTAX      Unsigned32
       UNITS     "seconds"
     MAX-ACCESS  read-write
     STATUS      current
     DESCRIPTION
       "The maximum time to wait before assuming Icmp
       session is terminated."
       REFERENCE
          ""
       DEFVAL { 86400 } -- 1 day
     ::= { 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 the all the tables in the CAP
       to be cleared, and all CAP objects with defaults to be reset back to
       their default values."
     ::= { 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 { cabhCapMappingWanAddrType, cabhCapMappingWanAddr,
     cabhCapMappingWanPort,
       cabhCapMappingLanAddrType, cabhCapMappingLanAddr, cabhCapMappingLanPort}
     ::= { cabhCapMappingTable 1 }

CabhCapMappingEntry ::= SEQUENCE {
     cabhCapMappingWanAddrType   InetAddressType,
       cabhCapMappingWanAddr          InetAddress,
       cabhCapMappingWanPort          INTEGER,
       cabhCapMappingLanAddrType      InetAddressType,
       cabhCapMappingLanAddr          InetAddress,
       cabhCapMappingLanPort          INTEGER,
       cabhCapMappingMode         CabhCapPacketMode,
       cabhCapMappingMethod           INTEGER,
       cabhCapMappingProtocol              INTEGER
       }

cabhCapMappingWanAddrType OBJECT-TYPE
     SYNTAX      InetAddressType
     MAX-ACCESS    not-accessible
     STATUS      current
     DESCRIPTION
       "The IP address type assigned on the WAN side. IP version 4
       is typically used."
     ::= { cabhCapMappingEntry 1 }

cabhCapMappingWanAddr OBJECT-TYPE
     SYNTAX      InetAddress
     MAX-ACCESS    not-accessible
     STATUS        current
     DESCRIPTION
       "The IP address assigned on the WAN side. IP version 4
       is typically used."
     ::= { cabhCapMappingEntry 2 }

cabhCapMappingWanPort OBJECT-TYPE
     SYNTAX      INTEGER (1..65535)
     MAX-ACCESS    not-accessible
     STATUS        current
     DESCRIPTION
       "The TCP/UDP port number on the WAN side."
     ::= { cabhCapMappingEntry 3 }

cabhCapMappingLanAddrType OBJECT-TYPE
     SYNTAX        InetAddressType
     MAX-ACCESS    not-accessible
     STATUS        current
     DESCRIPTION
       "The IP address type assigned on the LAN side. IP version 4
```

```
      is typically used."
    ::= { cabhCapMappingEntry 4 }

cabhCapMappingLanAddr OBJECT-TYPE
    SYNTAX        InetAddress
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION
      "The IP address assigned on the LAN side. IP version 4
      is typically used."
    ::= { cabhCapMappingEntry 5 }

cabhCapMappingLanPort OBJECT-TYPE
    SYNTAX        INTEGER (1..65535)
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION
      "The TCP/UDP port number on the LAN side."
    ::= { cabhCapMappingEntry 6 }

cabhCapMappingMode OBJECT-TYPE
    SYNTAX        CabhCapPacketMode
    MAX-ACCESS         read-only
    STATUS        current
    DESCRIPTION
      "The type of packet-handling mode for this mapping. Note that this
      information could be gleaned from the IP address and Port information for
      this mapping."
    ::= { 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-only
    STATUS   current
    DESCRIPTION
      "The protocol for this mapping."
    ::= { cabhCapMappingEntry 9 }

--============================================================================
--
--   cabhCapPassthroughTable (CAP Passthrough Table)
--
--   The cabhCapPassthroughTable contains the MAC Addresses for all LAN-IP
     Devices which will be configured as pass-through.
--
--============================================================================
```

```
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-ACCESS    not-accessible
     STATUS        current
     DESCRIPTION
       "List of MAC addresses for LAN-IP Devices which are configured as
       passthrough mode."
     INDEX {cabhCapPassthroughMACAddr }
     ::= { cabhCapPassthroughTable 1 }

CabhCapPassthroughEntry ::= SEQUENCE {
     cabhCapPassthroughMACAddr        PhysAddress,
     cabhCapPassthroughRowStatus           RowStatus
     }

cabhCapPassthroughMACAddr OBJECT-TYPE
     SYNTAX        PhysAddress
     MAX-ACCESS    not-accessible
     STATUS        current
     DESCRIPTION
       "MAC Address of LAN-IP Device to be configured as passthrough mode."
     ::= {cabhCapPassthroughEntry 1 }

cabhCapPassthroughRowStatus OBJECT-TYPE
     SYNTAX        RowStatus
     MAX-ACCESS    read-create
     STATUS        current
     DESCRIPTION
       "The RowStatus interlock for creation and deletion
       of cabhCapPassthroughTable entry."
     ::= { cabhCapPassthroughEntry 2 }

--
-- 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 3 }

cabhCapGroup OBJECT-GROUP
     OBJECTS {
       cabhCapTcpTimeWait,
       cabhCapUdpTimeWait,
       cabhCapIcmpTimeWait,
       cabhCapPrimaryMode,

--     cabhCapMappingWanAddrType,
--     cabhCapMappingWanAddr,
--     cabhCapMappingWanPort,
--     cabhCapMappingLanAddrType,
--     cabhCapMappingLanAddr,
--     cabhCapMappingLanPort,
       cabhCapMappingMode,
     cabhCapMappingMethod,
       cabhCapMappingProtocol,

--     cabhCapPassthroughMacAddr
       cabhCapPassthroughRowStatus
       }
     STATUS    current
     DESCRIPTION
       "Group of objects for CDB MIB."
     ::= { cabhCapGroups 1 }

END
```

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
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	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
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 y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2003