EXHIBIT A

Home Member Login Broadband Supplier Login Contact Us Site Map

CableLabs®
...Revolutionizing Cable Technology®

Search

About CableLabs | Members' Area | Current Projects | Certification & Qualification | Join CableLabs | News Room | Conferences | CableNET®

Cable Modem/DOCSIS® | CableHome™ | PacketCable™ | OpenCable™ | Go2Broadband℠ | VOD Metadata

CableHome™

Specifications

Specifications Archive

Participant Login

- Project Home
- Specifications
- Documents
- Certification Testing
- News & Events
- How to Participate
- FAQ
- Glossary
- Careers
- Contact CableHome

Specifications

DESIG-NATION	DATE	STATUS CODE	AUDIENCE LEVEL	TITLE
CH-SP-CH1.1-I04-040409	04/09/04	Issued (04)	Public	CableHome 1.1 Specification
CH-SP-MIB-QOS-I03-040129	01/29/04	Issued (03)	Public	CableHome™ QOS MIB Specification
CH-SP-CH1.0-I05-030801	08/01/03	Issued (05)	Public	CableHome 1.0 Specification
CH-SP-MIB-CAP-I05-040129	01/29/04	Issued (05)	Public	CableHome CAP MIB Specification
CH-SP-MIB-CDP-I06-040409	04/09/04	Issued (06)	Public	CableHome CDP MIB Specification
CH-SP-MIB-CTP-I06-040409	04/09/04	Issued (06)	Public	CableHome CTP MIB Specification
CH-SP-MIB-PSDEV-I05-040129	01/29/04	Issued (05)	Public	CableHome PSDEV MIB Specification
CH-SP-MIB-SEC-I06-040409	04/09/04	Issued (06)	Public	CableHome Security MIB Specification
CH-SP-CO-CSA-I01-040324	03/24/04	Issued (01)	Public	CableOffice Commercial Services Annex 1.0 Specification
CH-SP-CO-MIB-CSA-I01-040324	03/24/04	Issued (01)	Public	CableOffice Commercial Services Annex 1.0 MIB Specification
CL-SP-MIB-CLABDEF-I03-040113	01/13/04	Issued (03)	Public	CableLabs Definition MIB Specification

Technical Reports

DESIG-NATION	DATE	STATUS CODE	AUDIENCE LEVEL	TITLE
CH-TR-ARCH-I01-010716	7/16/01	Interim (01)	Public	CableHome Architecture Framework Technical Report

EXHIBIT A

Acceptance Test Plans

DESIG-NATION	DATE	STATUS CODE	AUDIENCE LEVEL	TITLE
CH-ATP-CH1.1-I03-040423	04/23/04	Issued (03)	Public	CableHome 1.1 Acceptance Test Plan
TP-CH-ATPv1.0-I06-040302	03/02/04	Issued (06)	Public	CableHome 1.0 Acceptance Test Plan

Copyright | Privacy Policy | Site Map | Contact

EXHIBIT A

http://web.archive.org/web/20040609072138/http://www.cablelabs.com/projects/cablehome/downloads/specs/CH-SP-CH1.1-I04-040409.pdf

EXHIBIT A

CableHome 1.1 Specification

CH-SP-CH1.1-I04-040409

ISSUED SPECIFICATION

Notice

This CableHome specification is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (CableLabs®) for the benefit of the cable industry. Neither CableLabs, nor any other entity participating in the creation of this document, is responsible for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document by any party. This document is furnished on an AS-IS basis and neither CableLabs, nor other participating entity, provides any representation or warranty, express or implied, regarding its accuracy, completeness, or fitness for a particular purpose.

EXHIBIT A

Document Status Sheet

Document Control Number:	CH-SP-CH1.1-I04-040409
Document Title:	CableHome 1.1 Specification
Revision History:	I01 Released April 18, 2003 I02 Released August 1, 2003 I03 Released January 29, 2004 I04 Released April 9, 2004
Date:	April 9, 2004
Status:	~~Work in Progress~~ ~~Draft~~ Issued ~~Closed~~
Distribution Restrictions:	~~Author Only~~ ~~CL/Member~~ ~~CL/ Member/ Vendor~~ Public

Key to Document Status Codes:

Work in Progress An incomplete document, designed to guide discussion and generate feedback, that may include several alternative requirements for consideration.

Draft A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.

Issued A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.

Closed A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks:

DOCSIS®, eDOCSIS™, PacketCable™, CableHome™, CableOffice™, OpenCable™, CableCARD™, and CableLabs® are trademarks of Cable Television Laboratories, Inc.

EXHIBIT A

Contents

EXHIBIT A

EXHIBIT A

EXHIBIT A

EXHIBIT A

Figures

EXHIBIT A

EXHIBIT A

Tables

EXHIBIT A

EXHIBIT A

EXHIBIT A

This page intentionally left blank.

EXHIBIT A

1 CABLEHOME OVERVIEW

The CableLabs' CableHome project has developed this specification to describe the CableHome 1.1 architecture and operation that enables interoperability for devices built to the CableHome 1.1 specification. The CableHome 1.0 [CH6] specification concentrated on a residential gateway device called the Home Access device (HA) as the single entry point into the home. CableHome 1.1 expands this scope to specify additional features for the residential gateway and to standardize Quality of Service (QoS) and LAN messaging features for IP host devices connected to home LANs.

The CableHome architecture provides a defined set of requirements that support a wide range of services that can be delivered over cable. In order to ensure wide adoption and ease of use of this specification, CableHome closely aligns its technical specifications with well known industry standards, as well as other CableLabs projects. CableHome allows efficient use of the existing cable operators' system infrastructure, but also provides a clear transition path for the deployment of CableHome over older systems. The CableHome architecture provides support for existing and future IP-based services into the home.

In general, cable-based services are defined as application services that are delivered via a hybrid fiber/coax (HFC)/cable infrastructure. Cable operators currently offer a wide variety of cable-based services; additional service opportunities are enabled by the advent of home networks. Examples include high-speed data, streaming audio and video, packetized telephony, network management, home security, environmental monitoring, medical monitoring, gaming, interactive television, and video conferencing.

CableHome specifications are intended to provide Internet Protocol (IP) - based architecture for managed home- networked services on the cable network through a DOCSIS cable modem. The CableHome architecture accommodates any physical and link layer home network technology that supports the transport of IP packets. This layer 1 and 2 independent architecture enables cable operators to provide services to a wide range of home networking environments.

1.1 CableHome Motivation

The technology and service evolution in the cable industry is providing a direction for service providers and cable operators to have the ability to offer customers a wide range of services through a home networked system. The timing of emerging home networking technologies is a perfect fit to meet the evolving needs of the cable industry. With these two industries working together, under the direction of the CableLabs CableHome project, a best-of-breed technology, CableHome-specific architectural solution is brought to the cable industry to enable, at a minimum, a core set of services.

CableHome's major focus is to enable core DOCSIS and PacketCable functionality on home networks, with an additional focus on home network management capabilities. The CableHome infrastructure is designed to be complementary to those of DOCSIS and PacketCable, but distinct and operational in the absence of PacketCable deployment. DOCSIS 1.1, the advanced two-way data communication cable modem (CM) lends itself to be the ideal foundation for many business opportunities including CableHome, however if a cable operator is running a DOCSIS 1.0 system, CableHome allows the operator to deploy CableHome with a transition path to run a full CableHome system in the future.

1.2 Business Objectives

The CableHome project seeks to establish a common infrastructure that will allow the creation and interoperability of home networking equipment for use over a cable operator's system. Other considerations for CableHome include:

- Time to market

EXHIBIT A

- Existing Cable Infrastructure
- Cost-effective technology
- Leverage existing protocol standards
- Easily upgradeable to next generation services and equipment
- Enable vendor innovation
- Encourage vendor competition
- Independent home networking physical layer environment
- Provide a scalable CableHome system
- Enable existing home networking products for a plug and play environment
- Define an architecture that allows multiple vendors to rapidly develop low-cost interoperable solutions
- Create a specification to enable as many services as possible

Benefits to cable operators and consumers from this specifications should be: 1) lower installation costs by simplifying the home networking installation process with equipment that needs little or no configuration; 2) lower equipment costs to consumers through multiple suppliers enabled by CableHome's open specification process; and 3) lower operating costs by providing cable operators with tools that facilitate remote troubleshooting of consumer problems.

1.3 Business Design Guidelines

The CableHome project focuses on capabilities of networks within the home, and the cable infrastructure needed to support these capabilities. This specification describes a technical architecture to support the business requirements for CableHome 1.1. The following is a list of business requirements for CableHome 1.1.

- Auto provisioning for address acquisition and device configuration
- Network address management enabling managed network address and port translation
- Non-NAT addressing supported, to preserve existing service offerings
- Direct IP Communication between Network Management Systems (NMS) and LAN hosts
- Resolve LAN host names enabling the consumer to refer to devices by intuitive names
- Conservation of IP addresses
- Preserves cable network source-based routing architectures
- Remote configuration of residential gateway features
- Secure network management messaging between the NMS and the residential gateway
- Visibility from the NMS to all connected IP devices in the home
- Remote testing of connectivity between the residential gateway and LAN host devices
- Enable Quality of Service between LAN host devices
- Residential gateway device authentication
- Standardized remote firewall configuration
- Minimum set of firewall functionality
- Protect HFC from home traffic
- Proper functioning of home devices during HFC outage
- Secure software download
- Virtual Private Networking support
- Enable static port mapping

EXHIBIT A

- Support for DOCSIS 1.0 and DOCSIS 1.1 protocols
- Support for PacketCable protocols
- Independent physical and data link layer architecture in the home network
- Interoperability with non-compliant CableHome equipment

1.4 Assumptions

In addressing cable operators' business models, the CableHome advanced system and technical designs include a wide variety of assumptions that complete an operational environment to provide managed services for home networks. CableHome assumes the following:

- Residential Gateways can be either "stand alone" or embedded with a DOCSIS cable modem.
- Specific services being delivered over home networks is outside the scope of this project.
- The cable operator understands the trade-offs between the DOCSIS 1.0, DOCSIS 1.1, and DOCSIS 2.0 systems for CableHome functionality and performance.
- CableHome-compliant devices implement the Internet Protocol (IP) suite of protocols.
- References to required documents must be strictly adhered to unless explicit exceptions are noted.
- The format of any field referred to in another document is not to be changed when the field is used in a CableHome compliant product, unless the format is explicitly described in the CableHome specification.
- All references to cable modems mean DOCSIS 1.0-, 1.1-, or 2.0-compliant cable modems.
- The residential gateway will include a firewall.
- The residential gateway, if manufactured as a standalone unit without an embedded cable modem, will have one port to connect to a cable modem as well as any other ports necessary to support the home network.
- The residential gateway will have its own MAC address, independent of the cable modem, even in the embedded case.

1.5 Purpose of document

The goal of this specification is to create an architecture that enables vendors to develop interoperable products for the benefit of the cable operator and its subscribers. The CableHome 1.1 specification describes the requirements and architecture for development of interoperable CableHome-compliant devices to enable the core set of functionalities.

This specification provides information about management and provisioning protocols, initialization and configuration processes, manageable parameters, prioritized QoS, security, and Network Address Translation (NAT) for CableHome-compliant devices. The CableHome Management Information Base (MIB) is described in a separate set of documents.

EXHIBIT A

1.6 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"	This word or the adjective "REQUIRED" means that the item is an absolute requirement of this specification.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this specification
"SHOULD"	This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

EXHIBIT A

2 REFERENCES

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

2.1 References (normative)[1]

[CableLabs2] CableLabs Definition MIB Specification, CL-SP-MIB-CLABDEF-I03-040113

[CH1] CableHome Security MIB Specification, CH-SP-MIB-SEC-I06-040409

[CH2] CableHome CAP MIB Specification, CH-SP-MIB-CAP-I05-040129

[CH3] CableHome CDP MIB Specification, CH-SP-MIB-CDP-I06-040409

[CH4] CableHome CTP MIB Specification, CH-SP-MIB-CTP-I06-040409

[CH5] CableHome PSDEV MIB Specification, CH-SP-MIB-PSDEV-I05-040129

[CH6] CableHome 1.0 Specification, CH-SP-CH1.0-I05-030801

[CH7] CableHome QoS MIB Specification, CH-SP-MIB-QOS-I03-040129

[DIX] The Ethernet: A Local Area Network, Data Link Layer and Physical Layer Specification, Version 2.0, Digital Equipment Corporation, Intel Corporation, and Xerox Corporation, DEC document No.AA-K759B-TK, November 1982.

[DOCSIS1] Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premises Equipment Interface Specification, SP-CMCI-I09-030730.

[DOCSIS5] Data-Over-Cable Service Interface Specifications, Operations Support System Interface Specification, SP-OSSIv2.0-I05-040407.

[DOCSIS8] Data-Over-Cable Service Interface Specifications, Baseline Privacy Plus Interface Specification, SP-BPI+-I11-040407.

[DOCSIS9] Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification v1.1, SP-RFIv1.1-I10-030730.

[DOCSIS11] Data-Over-Cable Service Interface Specifications, Operations Support System Interface Specification v.1.1, SP-OSSIv1.1-I07-030730.

[FIPS 140-2] Security Requirements for Cryptographic Modules, Department of Commerce, NIST, FIPS 140-2, May 25, 2001.

[FIPS 180-1] Secure Hash Algorithm, Department of Commerce, NIST, FIPS 180-1, April, 1995

[IANA1] IANA Port Numbers, http://www.iana.org/assignments/port-numbers

[IANAType] IANAifType MIB Definitions, http://www.iana.org/assignments/ianaiftype-mib

[ISO8025] ISO 8025 (December 1987) – Information processing systems - Open Systems Interconnection - Specification of the Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).

[ISO/IEC8802-2] ISO/IEC 8802-2 (ANSI/IEEE Std 802.2): 1994, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 2: Logical link control.

[1] Revised normative list per ECNs CH1.1-N-03060 and CH1.1-N-03070 by GO, 10/28/03 and 11/13/03.

EXHIBIT A

[ISO/IEC10038] ISO/IEC 10038 (ANSI/IEEE Std 802.1D): 1993, Information technology - Telecommunications and information exchange between systems - Local area networks - Media access control (MAC) bridges.

[ITU-T X.509] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1977.

[PKCS #1] RSA Laboratories, PKCS #1, v2.0: RSA Cryptography Standard, October 1, 1999.

[PKCS #7] RSA Laboratories, PKCS #7, Cryptographic Message Syntax Standard, An RSA Laboratories Technical Note, Version 1.5, Revised November 1, 1993.

[PKT-ASP] PacketCable Specifications, Audio Server Protocol Specification, PKT-SP-ASP-I02-010620.

[PKT-CMSS] PacketCable Specifications, Call Management Server Signaling, PKT-SP-CMSS-I03-040402.

[PKT-CODEC] PacketCable Specifications, Audio/Video Codecs Specification, PKT-SP-CODEC-I04-021018.

[PKT-DQOS] PacketCable Specifications, Dynamic Quality of Service Specification, PKT-SP-DQOS-I09-040402.

[PKT-MEM] PacketCable Specifications, Management Event Mechanism, PKT-SP-MEM-I01-001128.

[PKT-MGCP] PacketCable Specifications, Network-Based Call Signaling Protocol Specification, PKT-SP-EC-MGCP-I10-040402.

[PKT-PROV] PacketCable Specifications, MTA Device Provisioning Specification, PKT-SP-PROV-I09-040402.

[PKT-SEC] PacketCable Specifications, Security, PKT-SP-SEC-I10-040113.

[RFC 347] Postel, J., Echo Process, IETF RFC-0347, May 1972.

[RFC 768] Postel, J., User Datagram Protocol (UDP), IETF RFC-0768, August 1980.

[RFC 791] Postel, J., Internet Protocol, IETF RFC-0791 (MIL STD 1777), September, 1981.

[RFC 792] Postel, J., Internet Control Message Protocol (ICMP), IETF RFC-0792, September 1981.

[RFC 793] Information Sciences Institute, University of Southern California, Transmission Control Protocol, IETF RFC-0793, September 1981.

[RFC 868] Harrenstien, K., and Postel, J., Time Protocol, IETF RFC-0868, May 1983.

[RFC 919] J.C. Mogul, Broadcasting Internet Datagrams, Oct-01-1984.

[RFC 922] J.C. Mogul, Broadcasting Internet datagrams in the presence of subnets, Oct-01-1984.

[RFC 1034] Mockapetris, P., Domain Names - Concepts and Facilities, IETF RFC-1034, November 1987.

[RFC 1035] Mockapetris, P., Domain Names - Implementation and Specification, IETF RFC-1035, November 1987.

[RFC 1122] Braden, R., ed., Requirements for Internet Hosts -- Communication Layers, IETF RFC-1122, October 1989.

[RFC 1123] Braden, R., Requirements for Internet Hosts – Application and Support, IETF RFC-1123, October 1989.

[RFC 1213] McCloghrie, K. and Rose, M., ed., Management Information Base for Network Management of TCP/IP-based Internets, IETF RFC-1213, March 1991.

EXHIBIT A

[RFC 1157] Schoffstall, M., Fedor, M., Davin, J. and Case, J., A Simple Network Management Protocol (SNMP), IETF RFC-1157, May, 1990.

[RFC 1350] Sollins, K., The TFTP Protocol (Revision 2), IETF RFC-1350, July, 1992.

[RFC 1510] J. Kohl, C. Neuman, The Kerberos Network Authentication Service (V5) September, 1993.

[RFC 1812] Baker, F., Requirements for IP Version 4 Routers, IETF RFC-1812, June, 1995.

[RFC 1889] Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V., RTP: A Transport Protocol for Real-Time Applications, IETF RFC-1889, January 1996.

[RFC 1901] Case, J., McCloghrie, K., Rose, M., Waldbusser, S., Introduction to Community-based SNMPv2, IETF RFC-1901, January 1996.

[RFC 2011] McCloghrie, K., ed., SNMPv2 Management Information Base for the Internet Protocol using SMIv2, IETF RFC-2011, November 1996.

[RFC 2013] McCloghrie, K., ed., SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2, November 1996.

[RFC 2104] Krawczyk, H., Bellare, M., and Canetti, R., HMAC: Keyed-Hashing for Message Authentication, IETF RFC-2104, February 1997.

[RFC 2131] Droms, R., Dynamic Host Configuration Protocol, IETF RFC-2131, March 1997.

[RFC 2132] Alexander, S., and Droms, R., DHCP Options and BOOTP Vendor Extensions, IETF RFC-2132, March 1997.

[RFC 2233] McCloghrie, K. and Kastenholz, F., The Interfaces Group MIB using SMIv2, IETF RFC-2233, November 1997.

[RFC 2236] Fenner, W., Internet Group Management Protocol, Version 2, IETF RFC-2236, November 1997.

[RFC 2246] Dierks, T. and Allen, C., The TLS Protocol Version 1.0, IETF RFC-2246, January 1999.

[RFC 2349] Malkin, G. and Harkin, A., TFTP Timeout Interval and Transfer Size Options, IETF RFC-2349, May 1998.

[RFC 2401] Kent, S. and Atkinson, R, Security Architecture for the Internet Protocol, IETF RFC-2401, November 1998

[RFC 2402] Kent, S. and Atkinson, R, IP Authentication Header , November 1998

[RFC 2406] Kent, S. and Atkinson, IP Encapsulating Security Payload (ESP), November 1998

[RFC 2409] Harkins, D. and Carrel, D., The Intenet Key Exchange (IKE), IETF RFC-2409, November 1998

[RFC 2474] K. Nichols, S. Blake, F. Baker, D. Black, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998.

[RFC 2576] Frye, R., Levi, D., Routhier, S., and Wijnen, B., Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework, IETF RFC-2576, March 2000.

[RFC 2578] K. McCloghrie, D. Perkins, J. Schoenwaelder, Structure of Management Information Version 2 (SMIv2), April 1999.

[RFC 2579] K. McCloghrie, D. Perkins, J. Schoenwaelder, Textual Conventions for SMIv2, April 1999.

[RFC 2580] K. McCloghrie, D. Perkins, J. Schoenwaelder, Conformance Statements for SMIv2, April 1999.

[RFC 2616] Fielding, R, et. al, Hypertext Transfer Protocol -- HTTP/1.1, IETF RFC-2616, June 1999.

EXHIBIT A

[RFC 2663] Srisuresh, P. and Holdrege, M., IP Network Address Translator (NAT) Terminology and Considerations, IETF RFC-2663, August 1999.

[RFC 2669] St. Johns, M., DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems, IETF RFC-2669, August 1999.

[RFC 2670] St. Johns, M., Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces , August 1999.

[RFC 2786] St. Johns, M., Diffie-Hellman USM Key Management Information Base and Textual Convention, IETF RFC-2786, March, 2000.

[RFC 2863] McCloghrie, K. and Kastenholz, F., The Interfaces Group MIB, IETF RFC-2863, June 2000.

[RFC 3022] Srisuresh, P. and Egevang, K., Traditional IP Network Address Translator (Traditional NAT). IETF RFC-3022, January 2001.

[RFC 3046] Patrick, M., DHCP Relay Agent Information Option, IETF RFC-3046, January 2001.

[RFC 3280] Housley, Polk, Ford and Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF RFC-3280, April 2002.

[RFC 3291] Danielle, M., Haberman, B., Routhier, S., and J. Schoenwaelder, Textual Conventions for Internet Network Addresses, IETF RFC-3291, May 2002.

[RFC 3396] Lemon, T. and Cheshire, S., Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4), IETF RFC-3396, November 2002.[2]

[RFC 3410] Case, J., Mundy, R., Partain, D., and Stewart, B. Introduction and Applicability Statements for Internet-Standard Management Framework. IETF RFC-3410, December 2002.

[RFC 3411] Harrington, D., Presuhn, R., and Wijnen, B., An Architecture for Describing SNMP Management Frameworks, IETF RFC-3411, December 2002.

[RFC 3412] Case, J., Harrington, D., Presuhn, R., and Wijnen, B., Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), IETF RFC-3412, December 2002.

[RFC 3413] Levi, D., Meyer, P., and Stewart, B., SNMP Applications, IETF RFC-3413, December 2002.

[RFC 3414] Blumenthal, U. and Wijnen, B., User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), IETF RFC-3414, December 2002.

[RFC 3415] Wijnen, B., Presuhn, R., and McCloghrie, K. View-based Access Control Model (VACM) for the Simple Network Control Model (SNMP), IETF RFC-3415, December 2002.

[RFC 3416] Presuhn, R., ed.,. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), IETF RFC-3416, December 2002.

[RFC 3417] Presuhn, R., ed., Transport Mappings for the Simple Network Management Protocol (SNMP), IETF-RFC 3417, December 2002.

[RFC 3418] Presuhn, R., ed., Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), December 2002.

[SCTE1] SCTE 22-1 2002, DOCSIS 1.0, Radio Frequency Interface Standard.

[SHA] NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995.

[SOAP] SOAP Version 1.2, W3C Working Draft, World Wide Web Consortium (W3C), December 19, 2002, http://www.w3.org/2000/xp/Group/#drafts.

[2] Added this item to the normative list per ECN CH1.1-N-03.0112-1 by KB on 4/5/04.

EXHIBIT A

[XML1] XML Protocol (XMLP) Requirements, W3C Working Draft, World Wide Web Consortium (W3C), June 26, 2002, http://www.w3.org/TR/2002/WD-xmlp-reqs-20020626.

2.2 References (informative)[3]

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

[FIPS 186] Federal Information Processing Standards Publications (FIPS PUB) 186, Digital Signature Standard, 18 May 1994

[RFC 2644] Senie, D., Changing the Default for Directed Broadcasts in Routers, IETF RFC-2644, August 1999.

[RFC 3164] C. Lonvick, The BSD Syslog Protocol, August 2001.

[RFC 3235] Senie, D., Network Address Translator (NAT)-Friendly Application Design Guidelines, IETF RFC-3235, January 2002.

[RFC 3435] F. Andreasen, B. Foster, Media Gateway Control Protocol (MGCP) Version 1.0, January 2003

[3] Revised informative list per ECNs CH1.1-N-03070 and CH1.1-N-03.0099-3 by GO on 11/13/03 and 12/10/03.

EXHIBIT A

3 GLOSSARY

Address Realms	A network domain in which the network addresses are uniquely assigned to entities such that datagrams can be routed to them.
Asymmetric Key	An encryption key or a decryption key used in public key cryptography, where encryption and decryption keys are always distinct.
Authentication	The process of verifying the claimed identity of an entity to another entity.
Authenticity	The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity that claims to have given the information.
Authorization	The act of giving access to a service or device if one has permission to have the access.
CableHome	The CableLabs home networking technology standardization initiative.
CableHome Security Portal (CSP)	A functional element that provides security management and translation functions between the HFC and Home network.
Certificate Authority (CA)	A trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates.
Cipher	An algorithm that transforms data between plaintext and ciphertext.
Ciphersuite	A set which must contain both an encryption algorithm and a message authentication algorithm (e.g., a MAC or an HMAC). In general, it may also contain a key-management algorithm, which does not apply in the context of PacketCable.
Ciphertext	The (encrypted) message output from a cryptographic algorithm that is in a format that is unintelligible.
Cleartext	The original (unencrypted) state of a message or data. Also called plaintext.
Call Management Server (CMS)	Controls the audio connections. Also called a Call Agent in MGCP/SGCP terminology.
Co-existence Mode	a method described by [RFC 2576] for enabling any of the three versions (version 1, version 2, or version 3) of SNMP to be supported.
Confidentiality	A way to ensure that information is not disclosed to anyone other then the intended parties. Information is encrypted to provide confidentiality. Also known as privacy.
Cryptanalysis	The process of recovering the plaintext of a message or the encryption key without access to the key.
Cryptographic algorithm	An algorithm used to transfer text between plaintext and ciphertext.
Decipherment	A procedure applied to ciphertext to translate it into plaintext.
Decryption	A procedure applied to ciphertext to translate it into plaintext.
Decryption key	The key in the cryptographic algorithm to translate the ciphertext to plaintext.
DHCP Provisioning Mode	DHCP driven PS configuration file download.
Digital certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a public key certificate.

EXHIBIT A

Digital signature	A data value generated by a public-key algorithm based on the contents of a block of data and a private key, yielding an individualized cryptographic checksum.
Downstream	The direction from the Headend toward the subscriber location.
Dynamic Host Configuration Protocol (DHCP)	An Internet protocol used for assigning network layer (Internet Protocol) addresses.
Dynamic Quality-of-Service (DQoS)	[PacketCable] Assigned on the fly for each communication depending on the QoS requested.
Embedded Multimedia Terminal Adapter (E-MTA)	[PacketCable] A single node that contains both an MTA and a cable modem.
Embedded PS	A Portal Services element that does not use a standalone interface as defined in the DOCSIS CMCI specification to connect to a CM.
Encipherment	A method used to translate plaintext into ciphertext.
Encryption	A method used to translate plaintext into ciphertext.
Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Firewall	An application that blocks unauthorized access from one network segment to another.
Firewall Rule Set	A set of rules used to configure a Firewall's security policy.
Hash	A number generated from a string of text using a formula in such a way that it is extremely unlikely that some other text will produce the same hash value (ref.: Webopedia).
Home Access (HA) Device	A grouping of logical elements used to achieve HFC access for CableHome network(s).
Home Bridge (HB) Device	A group of logical elements used to bridge CableHome networks together.
Home Client (HC) Device	A group of logical elements used to provide functionality to client applications.
Headend	The extent of the cable operator's network that includes the CMTS and the servers that serve the PS and the cable modem to which it is connected.
Internet Protocol Security (IPSec)	A collection of Internet standards for protecting IP packets with encryption and authentication.
Jitter	Variability in the delay of a stream of incoming packets making up a flow such as a voice communication.
Kerberos	A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.
Key	A mathematical value input into the selected cryptographic algorithm.
Key Exchange	The swapping of public keys between entities to be used to encrypt communication between the entities.
Key Management	The process of distributing shared symmetric keys needed to run a security protocol.
Key Pair	An associated public and private key where the correspondence between the two are mathematically related, but it is computationally infeasible to derive the private key from the public key.

EXHIBIT A

Keying Material	A set of cryptographic keys and their associated parameters, normally associated with a particular run of a security protocol.
Keyspace	The range of all possible values of the key for a particular cryptographic algorithm.
Kickstart	A method described by DOCSIS 1.1 specifications for establishing trust between two networked elements for the purpose of secure communication.
LAN IP Device	A LAN IP Device is representative of a typical IP device expected to reside on home networks, and is assumed to contain a TCP/IP stack as well as a DHCP client.
Latency	The time, expressed in quantity of symbols, taken for a signal element to pass through a device.
Link Encryption	Cryptography applied to data as it travels on data links between the network devices.
Media Access Control (MAC)	It is a sublayer of the Data Link Layer. It normally runs directly over the physical layer.
Media Gateway Control Protocol (MGCP)	Protocol follow-on to SGCP. Refer to [RFC 3435].
Multicast	To transmit a single message to a select group of recipients.
Network Management OSS	The functions related to the management of data link layer and physical layer resources and their stations across the data network supported by the hybrid fiber/coax system.
NmAccess Mode	SNMPv1/v2 management mode to support DOCSIS 1.0 infrastructure.
Nonce	A random value used only once that is sent in a communications protocol exchange to prevent replay attacks.
Non-Repudiation	The ability to prevent a sender from denying later that he or she sent a message or performed an action.
One-way Hash	A hash function that has an insignificant number of collisions upon output.
PacketCable	CableLabs specification of packetized service delivery system.
PacketCable Dynamic Quality-of Service	(See Dynamic Quality of Service [DQoS]).
Passthrough	A sub-function of the CAP, the Passthrough function bridges packets on the WAN-Data side of the CAP to the LAN-Pass side unchanged.
Plaintext	The original (unencrypted) state of a message or data. Also called cleartext.
Policy	Combination of a Ruleset, General Firewall Behavior, and the implementation-specific capabilities of the filtering function.[4]
Portal Services (PS)	A functional element that provides management and translation functions between the HFC and Home network.
Pre-shared Key	A shared secret key passed to both parties in a communication flow, using an unspecified manual or out-of-band mechanism.
Privacy	A way to ensure that information is not disclosed to any one other then the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality.
Private Key	The key used in public key cryptography that belongs to an individual entity and must be kept secret.

[4] Added this term to the Glossary per ECN CH1.1-N-03.0097-5 by GO on 12/9/03.

EXHIBIT A

Provisioning Application	A software utility or set of software utilities that coordinate various tasks responsible for initializing and establishing service for elements connected to a network.
Proxy	A facility that indirectly provides some service or acts as a representative in delivering information, thereby eliminating the need for a host to support the service.
PS Database	A conceptual entity representing a store of PS function (CAP, CDP, CMP, etc.) information.
Public Key	The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.
Public Key Certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.
Public Key Cryptography	A procedure that uses a pair of keys, a public key and a private key, for encryption and decryption, also known as an asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A user's private key is kept secret and is the only key that can decrypt messages sent encrypted by the user's public key.
Public-Key Infrastructure	A process for issuing public key certificates, which includes standards, Certification Authorities, communication between authorities and protocols for managing certification processes.
Public-Key Cryptography for Initial Authentication (PKINIT)	The extension to the Kerberos protocol that provides a method for using public-key cryptography during initial authentication.
Real-time Transport Protocol (RTP)	A protocol for encapsulating encoded voice and video streams. Refer to [RFC 1889].
Request for Comments (RFC)	Technical policy documents approved by the IETF which are available on the World Wide Web at http://www.ietf.cnri.reston.va.us/rfc.html.
Rivest, Shamir, Adlemen (RSA)	A public-key, or asymmetric, cryptographic algorithm used to provide authentication and encryption services. RSA stands for the three inventors of the algorithm, Rivest, Shamir, Adlemen.
RSA Key Pair	A public/private key pair created for use with the RSA cryptographic algorithm.
Root Private Key	The private signing key of the highest-level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.
Root Public Key	The public key of the highest level Certification Authority, normally used to verify digital signatures generated with the corresponding root private key.
Rule	A specific filter defined as an exception to the General Firewall Behavior and is an element of a Ruleset.[5]

[5] Added this term to the Glossary per ECN CH1.1-N-03.0097-5 by GO on 12/9/03.

EXHIBIT A

Ruleset	A collection of defined filtering rules. In CableHome, two types of rulesets are defined. These are (1) the Default Ruleset, which is defined in cabhSec2FwFactoryDefaultFilterTable of the CableHome Security MIB [CH1], and (2) the Configured Ruleset, which is defined by the cable operator and configured in the docsDevFilterIpTable [RFC 2669] with required modifications by this specification.[6]
Secret Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a symmetric key.
Secure Hash Algorithm 1 (SHA-1)	A one-way hash algorithm.
Session Key	A cryptographic key intended to encrypt data for a limited period of time, typically between a pair of entities.
Signed and Sealed	An "envelope" of information which has been signed with a digital signature and sealed using encryption.
SNMP Provisioning Mode	SNMP driven PS configuration file download.
SNMP Trap	An event notification message sent to the SNMP management system to identify the occurrence of conditions such as a threshold that exceeds a predetermined value.
Simple Object Access Protocol (SOAP)	A message-based protocol based on XML supporting remote procedure calls and message exchange on IP-based networks.
Standalone Multimedia Terminal Adapter (S-MTA)	a single node that contains an MTA and a non-DOCSIS MAC (e.g. ethernet).
Standalone PS	A Portal Services element that connects to the CM using only a standalone interface as defined in the DOCSIS CMCI specification.
Symmetric Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a secret key.
SYSLOG	System Log. A log file and a protocol for storing event messages reported by networked elements. The protocol is described in [RFC 3164].
Type-Length-Value (TLV)	A tuple within a DOCSIS configuration file.
X.509 certificate	A public key certificate specification developed as part of the ITU-T X.500 standards directory.

[6] Added this term to the Glossary per ECN CH1.1-N-03.0097-5 by GO on 12/9/03.

EXHIBIT A

4 ABBREVIATIONS

A/V	Audio/Video
APP	Application
ASP	Application Specific Proxy
CA	Certificate Authority
CAP	CableHome Address Portal
CAT	CableHome Address Translation
CDC	CableHome DHCP Client
CDP	CableHome DHCP Portal
CDS	CableHome DHCP Server
CH	CableHome Host
CL	CableLabs
CM	DOCSIS Cable Modem
CMP	CableHome Management Portal
CMS	Call Management Server
CMTS	Cable Modem Termination System
C-NAT	CableHome Network Address Translation
C-NAPT	CableHome Network Address and Port Translation
CNP	CableHome Naming Portal
CPU	Central Processing Unit
CQoS	CableHome Quality of Service
CQP	CableHome QoS Portal
CRG	CableHome Residential Gateway
CRL	Certificate Revocation List
CSP	CableHome Security Portal
CTP	CableHome Testing Portal
CVC	Code Verification Certificate
CVS	Code Verification Signature
CxP	CableHome Portal Services Sub-function
DER	Distinguished Encoding Rules
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DOCSIS	Data-Over-Cable Service Interface Specification
DQoS	Dynamic Quality-of-Service (PacketCable)
E-MTA	Embedded Multimedia Terminal Adapter
FTP	File Transfer Protocol
FW	Firewall
GMT	Greenwich Mean Time

EXHIBIT A

HA	Home "Access"
HE	Headend
HEX	Hexidecimal
HFC	Hybrid Fiber Coax
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCDN	IP over Cable Data Network - a working group of the IETF
IPF	Inbound Packet Filter
IPSec	Internet Protocol Security
KDC	Key Distribution Center
LAN	Local Area Network
LAN-Pass	Pass-through Local Area Network address
LAN-Trans	Translated Local Area Network address
MAC	Media Access Control
MCF	Management Client Function
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
MSF	Management Server Function
MSO	Multimedia Systems Operator
MTA	Multimedia Terminal Adapter
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NCS	Network-based Call Signaling
NMS	Network Management System
NS	Authoritative Name Server
OID	Object Identifier
OPF	Outbound Packet Filter
OSI	Open System Interconnection
OSS	Operations Support System
PDU	Protocol Data Unit
PING	Packet Inter-Network Groper
PKI	Public Key Infrastructure
PKINIT	Public-Key Cryptography for Initial Authentication
PS	Portal Services
PS WAN-Man	CableHome Portal Services element WAN management interface
PS WAN-Data	CableHome Portal Services element WAN data interface

EXHIBIT A

QBP	Quality of Service Boundary Point
QCC	Quality of Service Characteristics Client
QCS	Quality of Service Characteristics Server
QFM	Quality of Service Forwarding & Media Access
QoS	Quality of Service
RAM	Random Access Memory
RDN	Relative Distinguished Name
RFC	Request for Comments
ROM	Read Only Memory
RSA	Rivest, Shamir, Adleman (See Glossary)
RSVP	Resource ReSerVation Protocol
RTCP	Real-Time Control Protocol
RTP	Real-Time Transport Protocol
SDP	Session Description Protocol
SHA – 1	Secure Hash Algorithm 1
S-MTA	Standalone Multimedia Terminal Adapter
SNMP	Simple Network Management Protocol
SOA	Start of Authority
SPF	Stateful Packet Filtering
SYSLOG	System Log
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type-Length-Value
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USFS	Upstream Selective Forwarding Switch
USM	User Security Model
UTC	Coordinated Universal Time
VACM	View-based Access Control Model
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WAN-Data	Wide Area Network Data Address Realm
WAN-Man	Wide Area Network Management Address Realm

EXHIBIT A

5 REFERENCE ARCHITECTURE

The goal of CableHome is to enable the delivery of new cable-based services to devices within the home, complementing the DOCSIS and PacketCable infrastructures, and enabling the delivery of these services. Specifically, CableHome provides an infrastructure by specifying a home networking environment, over which PacketCable and other related application services can be delivered, managed, and supported.

The CableHome project supports a myriad of cable operator business models and introduces additional features beyond current proprietary home networking solutions. CableHome 1.1 is a single technical specification that facilitates the development of an interoperable CableHome Residential Gateway (CRG) and CableHome compliant hosts (CH). The goal is the creation of a cable operator-configurable CableHome Residential Gateway-centric environment that will interact meaningfully with IP based home devices (LAN IP Devices), whether or not they are CableHome compliant. CableHome 1.1 brings cable operator-driven management, provisioning, QoS, and Security to the CableHome Residential Gateway. In addition, LAN messaging, prioritized QoS, and simple remote diagnostics for home devices is specified. CableHome 1.1 also defines QoS for applications running on CableHome compliant LAN hosts. A summary of the capabilities provided by the CableHome 1.1 specification follows:

Management, Discovery, and Provisioning

- Remote management and configuration of the CableHome Residential Gateway device
- Simple CableHome Residential Gateway diagnostics proxy for IP based home devices
- Hands-off provisioning for CableHome Residential Gateway devices
- Discovery of IP based home devices and associated applications
- Management of the CableHome Residential Gateway from the LAN

Addressing and Packet Handling

- One-to-many addressing translation for home devices
- One-to-one addressing translation for home devices
- Non-translated addressing for home devices (for translated address phobic applications)
- HFC traffic protection from in-home device intra-communications
- Home addressing support during HFC outage
- Simple DNS server in the CableHome Residential Gateway
- NAT support for IPsec VPN clients
- NAT support for IP based servers in the home using address translation

Quality of Service (QoS)

- CableHome Residential Gateway device transparent bridging functionality for PacketCable QoS messaging from/to PacketCable compliant applications
- Ability to assign traffic priorities (differentiated media access) to specific applications
- Ability to prioritize queuing in the CableHome Residential Gateway device in conjunction with the packet handling functionality.

Security

- CableHome Residential Gateway device authentication
- Secure management messages between the cable data network and the CableHome Residential Gateway
- Secure download of configuration and software files

EXHIBIT A

- Optional configuration file security
- Remote CableHome Residential Gateway firewall management
- Standardized firewall configuration and reporting
- Simple parental control

CableHome communication across the WAN and LAN is IPv4 based, leveraging specific protocols defined throughout the remainder of this document. CableHome compliant devices MUST implement version 4 of the Internet Protocol suite (IPv4) [RFC 791] and [RFC 3280].

The remainder of this section examines the CableHome 1.1 Reference Architecture from six perspectives:

- Logical view (Section 5.1)
- Functional view (Section 5.2)
- Messaging Interface view (Section 5.3)
- Informational view (Section 5.4)
- Operational view (Section 5.5)
- Physical Interface view (Section 5.6)

5.1 Logical Reference Architecture

As shown in Figure 5-1, this section introduces the logical concepts of the CableHome domain, logical elements, and the CableHome devices.

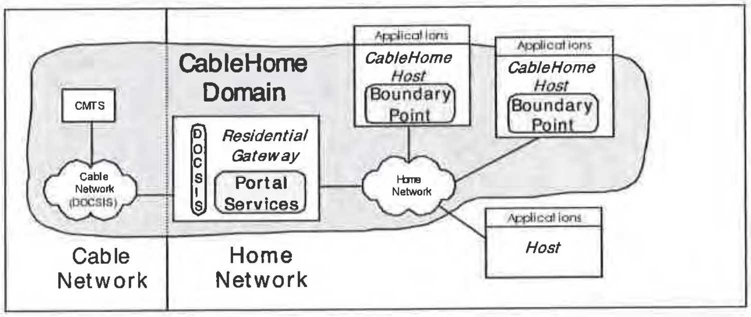


Figure 5-1 — CableHome 1.1 Key Logical Concepts

5.1.1 CableHome Domains

The CableHome domain represents the set of network elements that are compliant with the CableHome specification, and is diagrammatically represented as a shaded region in Figure 5-1. This region serves as a visual tool to clearly identify those elements within the home network that are CableHome compliant. Elements that reside within the CableHome domain (i.e., compliant elements) are directly or indirectly manageable by cable operators.

5.1.2 CableHome Devices

The CableHome architecture identifies devices in order to lend tangible context to the CableHome logical elements described in Section 5.1.3. CableHome device definitions provide an informative way of

EXHIBIT A

depicting home network topology, as well as logical elements located within the home network, but are not considered definitive or restrictive. CableHome 1.1 devices include the CableHome Residential Gateway and the CableHome Host.

The CableHome Residential Gateway device represents the physical location of the Portal Services (PS) logical element, which is described in Section 5.1.3.1. The CableHome Residential Gateway has a single WAN interface, a single PS logical element, and may have one or more LAN interfaces.

The CableHome 1.1 specification uses the term LAN IP Device to refer to any LAN Host that implements an IPv4 stack, including a DHCP client. A LAN IP Device that implements CableHome functionality, making it compliant with the CableHome specification, is referred to as a *CableHome Host device*. A LAN IP Device without CableHome functionality is referred to as a *Host*.

The CableHome Host device represents the physical location of the Boundary Point (BP). The BP, defined in Section 5.1.3.2, enables CableHome Hosts to interact with CableHome Residential Gateways. The CableHome Host has only one LAN interface in the CableHome Domain.

CableHome assumes a home networking topology with only one DOCSIS cable modem (CM) and one CableHome Residential Gateway on the home LAN. It is assumed that the DOCSIS CM is the only direct connection to the HFC. Ideally, the CableHome Residential Gateway will be directly connected to the CM with no other devices attached between the CM and CableHome Residential Gateway, in order for the CableHome Residential Gateway to provide the specified protection to the home network. All LAN Hosts are connected to the LAN behind the CableHome Residential Gateway.

5.1.3 Logical Elements

The CableHome architectural framework introduces the concept of logical elements. CableHome logical elements are logically bounded functional entities that can generate and respond to CableHome specified messages. CableHome logical elements operate at the IP protocol layer and above, thus remaining independent of any particular physical network technology. They also include the ability to gather and communicate information as needed to discover, manage, and deliver services over CableHome networks. CableHome 1.1 defines a logical entity specific to each CableHome Device: The PS logical entity encapsulates CableHome functionality defined for CableHome Residential Gateways and the BP logical entity encapsulates CableHome functionality defined for CableHome Hosts (see Section 5.1.2 for a description of the CableHome Devices).

5.1.3.1 Portal Services (PS)

The CableHome Portal Services is a logical element that provides in-premise and aggregated security, management, provisioning, addressing, and QoS services. The term "portal" is used to indicate services that interface the WAN to the LAN. This section describes features of the CableHome Portal Services logical element.

5.1.3.1.1 Standalone PS and PS with Embedded Cable Modem

The two primary components possible within a CableHome Residential Gateway, the DOCSIS Cable Modem (CM) and the Portal Services (PS) element, may use shared or independent hardware and software resources. It is this resource sharing between the CM and PS that distinguishes the Standalone PS from an Embedded PS.

A Standalone PS MUST NOT share hardware or software components with a CM. The separation of the CM from the standalone PS MUST appear to the PS as a simple disconnection of its WAN – i.e., the PS will continue fully functional as if it had the WAN disconnected. Otherwise, the PS will be considered Embedded. Given these definitions, it is possible that a PS might reside within the same physical enclosure as a CM, yet still be considered a Standalone PS.

EXHIBIT A

The CM and the PS are considered to be separate elements in the Standalone and Embedded cases, and respond to unique management addresses. In the Embedded case, the CM and PS share hardware or software components, but from the management perspective, they are separate entities.

Figure 5-2 illustrates the Standalone and Embedded PS. In both of these cases, the combination of a CM and a PS is considered to embody the concept of the HA device.

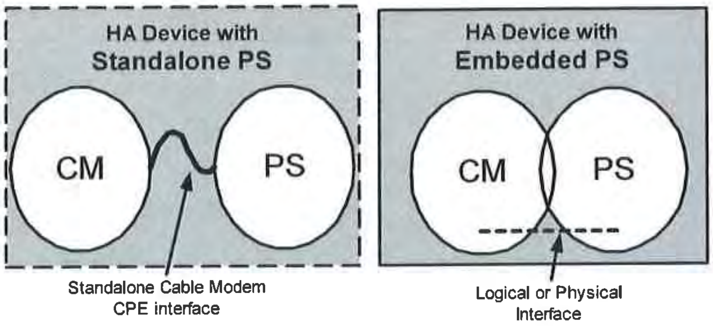


Figure 5-2 — Standalone PS and PS with Embedded CM

5.1.3.2 Boundary Point (BP)

A Boundary Point (BP) is a logical element which encapsulates all of the CableHome functionality defined for a CableHome Host. This functionality includes messaging and behavior required for device and application discovery by the cable operator, as well as for enabling prioritized QoS on the home network. The BP interacts with the PS in order to convey device and application information and to query cable operator-provisioned preferences for application priorities.

5.1.4 Address Realms

An Address Realm is defined as "a network domain in which the network addresses are uniquely assigned to entities such that datagrams can be routed to them" [RFC 2663]. Within the CableHome 1.1 specification, address realms are categorized as WAN address realms and LAN address realms. (See Figure 5-3).

EXHIBIT A

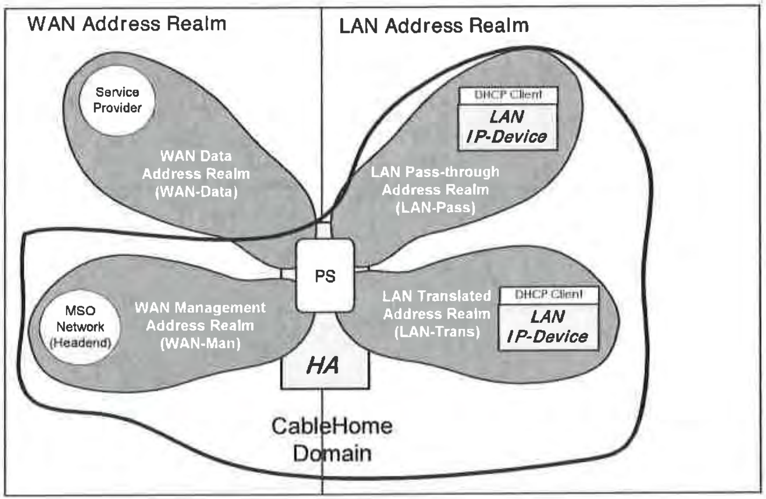

WAN Address Realm
LAN Address Realm
Service Provider
WAN Data Address Realm (WAN-Data)
DHCP Client
LAN IP-Device
LAN Pass-through Address Realm (LAN-Pass)
PS
MSO Network (Headend)
WAN Management Address Realm (WAN-Man)
LAN Translated Address Realm (LAN-Trans)
DHCP Client
LAN IP-Device
HA
CableHome Domain

Figure 5-3 — CableHome Address Realms

WAN addresses reside in one of two realms: the WAN Management Address Realm (WAN-Man), or the WAN Data Address Realm (WAN-Data). LAN addresses also reside in one of two realms: LAN Passthrough Address Realm (LAN-Pass), or LAN Translated Address Realm (LAN-Trans). The properties of these addressing realms are as follows:

- The WAN Management Address Realm (WAN-Man) is intended to carry network management traffic on the cable network between the network management system and the PS element. Typically, addresses in this realm will reside in private IP address space.
- The WAN Data Address Realm (WAN-Data) is intended to carry subscriber application traffic on the cable network and beyond, such as traffic between CableHome Hosts and Internet hosts. Typically, addresses in this realm will reside in public IP address space.
- The LAN Translated Address Realm (LAN-Trans) is intended to carry subscriber application and management traffic on the home network between CableHome Hosts, LAN IP Devices, and the PS element. Typically, addresses in this realm will reside in private IP address space, and can typically be reused across subscribers.
- The LAN Passthrough Address Realm (LAN-Pass) is intended to carry subscriber application traffic, such as traffic between CableHome Hosts, LAN IP Devices and Internet hosts, on the home network, cable network, and beyond. Typically, addresses in this realm will reside in public IP address space.

On the LAN side, the addresses in the LAN Passthrough Address Realm (LAN-Pass) are directly extracted from the addresses in WAN Data Address Realm. These are used by LAN IP Devices and applications such as PacketCable services that are intolerant of address translation and require a globally routable IP address. Additionally on the LAN side, LAN IP Devices may be assigned translated addresses from the LAN Translated Address Realm (LAN-Trans).

Physical LAN interfaces in the PS are assigned an index in accordance with the Interfaces Group MIB [RFC 2233] as described in Section 6.3.3.1.4.8 Interfaces Group MIB. A virtual LAN interface aggregating the physical LAN interfaces is also defined for the PS in Section 6.3.3.1.4.8. The LAN-side IP address defined for the PS is "bound" to this virtual interface. PS DHCP and domain name server functions, and

EXHIBIT A

the PS router function, are applications implemented in the PS addressed using the LAN-side IP address bound to the virtual LAN interface.

5.2 CableHome Functional Reference Model

CableHome Functions are IP-based services defined in the CableHome specification to be implemented by the PS, the BP, or the cable operator's data network, and support the delivery of cable-based services. CableHome functions are defined for each of the major CableHome specification areas: Provisioning, Management, Security, and Quality of Service.

Sub-elements are defined for both the PS and the BP. Sub-elements represent groupings of related functionality within the PS and BP. The PS and BP logical elements can contain any number of sub-elements, and sub-elements may themselves contain sub-groupings of functions (i.e. sub-elements within sub-elements).

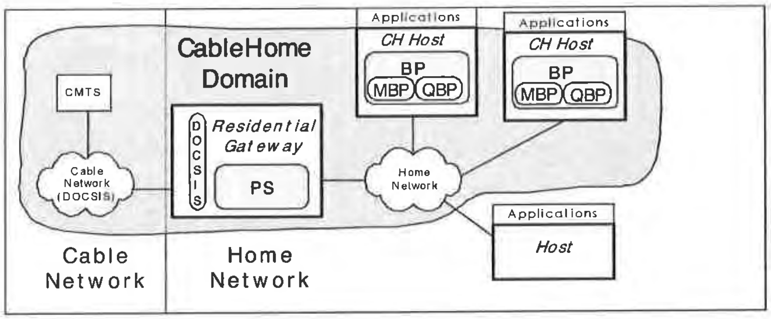


Figure 5-4 — CableHome Sub-elements

The PS contains a number of sub-elements, which are introduced below. Within the Boundary Point there are two primary sub elements, the Management Boundary Point (MBP) and the Quality of Service Boundary Point (QBP), which define CableHome discovery and management, and CableHome QoS functionality, respectively. The QBP contains additional sub-elements of its own.

5.2.1 CableHome Management and Provisioning Functions

To support the CableHome requirements during the provisioning and management of CableHome Hosts within the home, CableHome uses management and provisioning functions that reside in the cable data network, and defines functions for the PS and for the BP. Cable network-based management and provisioning functions include a number of services used by CableHome-defined management and provisioning processes. Portal Services management and provisioning functions are located within the CableHome Residential Gateway and include server-like, client-like, and other types of functionality. Boundary Point functions are found within CableHome Hosts and typically include client as well as other types of functionality. Examples of Cable Network, PS, and BP functions are introduced in Table 5-1, Table 5-2, and Table 5-3 and are illustrated in Figure 5-5.

Table 5-1 — Cable Network Management Functions

Cable Network Management Functions	Description
Cable Network DHCP Server	The DHCP server is a cable network component that provides address information for the WAN-Man and WAN-Data address realms to the PS

EXHIBIT A

Cable Network Management Functions	Description
Cable Network Management Servers	The CableHome management messaging, download, event notification servers including protocols such as SNMP, SYSLOG, and TFTP [RFC 2349]
Cable Network Time of Day Server	The time of day (ToD) server provides clients with the current time of day.

Table 5-2 — PS Management and Provisioning Functions

Management Portal Functions	Description
CableHome Address Portal (CAP)	Within the PS, the CAP interconnects the WAN and LAN address realms for data traffic. (See CAT/Passthrough)
CableHome Address Translation (CAT)	A sub-function of the CAP, a CAT translates public IP network addresses on the WAN-Data side of the CAP to private IP network addresses within a single logical subnet on the LAN-Trans side.
Passthrough	A sub-function of the CAP, the Passthrough function bridges packets on the WAN-Data side of the CAP to the LAN-Pass side unchanged.
CableHome Management Portal (CMP)	The function that provides an interfaces between the MSO and the PS - database.
CableHome DHCP Portal (CDP)	Address information functions (e.g. those transmitted via DHCP) including a server for the LAN realm and a client for the WAN realms
CableHome Naming Portal (CNP)	The CNP provides a simple DNS service for LAN IP Devices requiring naming services.
CableHome Testing Portal (CTP)	The CTP provides a remote means to initiate pings and loopbacks within the LAN.
HTTP Server	HTTP is the transport protocol used to convey SOAP messaging on the LAN. The PS contains an HTTP server which serves data upon BP requests
XML and SOAP Parsers	SOAP and XML are used for messaging on the LAN. The PS contains parsers for both.

Table 5-3 — BP Management and Provisioning Functions

Management Client Functions	Description
Cable Home Host DHCP Client	The CableHome DHCP client function is a in-home component used during the LAN IP Device provisioning process to dynamically request IP addresses and other logical element configuration information.
CableHome Host Loopback responder	Within LAN IP Device, the loopback responder loops data sourced from the CTP loopback function back to the CTP loopback function.
HTTP Client	HTTP is the transport protocol used to convey SOAP messaging on the LAN. The BP contains an HTTP client which requests data from the PS housed HTTP server
XML and SOAP Parsers	SOAP and XML are used for messaging on the LAN. The BP contains parsers for both.

EXHIBIT A

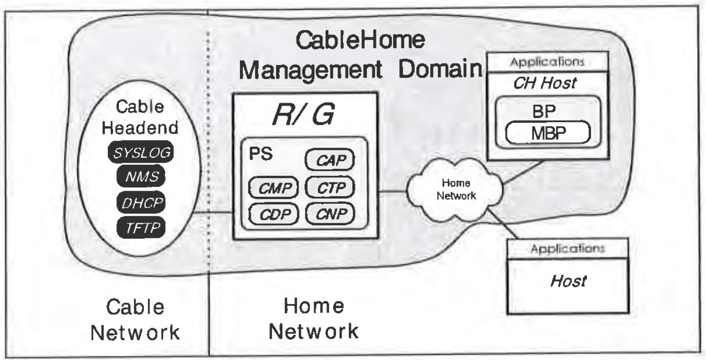


Figure 5-5 — CableHome Management Elements

5.2.2 CableHome Security Functions

To support the CableHome security requirements, CableHome uses security functions that reside in the cable data network and defines functions for the PS. Cable network-based security functions include servers used for key distribution, encryption, and authentication. Portal Services security functions are located within the CableHome Residential Gateway includes client functions and other types of functions. Examples of cable network-based and PS security functions are introduced in Table 5-4 and Table 5-5 and are illustrated in Figure 5-6.

Table 5-4 — Portal Services Security Functions

Portal Service Security Functions	Description
CableHome Security Portal (CSP)	The CSP communicates with Headend security servers, and includes functions that provide client side participation in the authentication, key exchange and certificate management processes. Other security functions include management message security, participation in secure download processes, and remote firewall management.
Firewall (FW)	The Firewall provides functionality that protects the home network from malicious attack.

Table 5-5 — Cable Network Security Function

Cable Network Security Functions	Description
Key Distribution Center (KDC) Servers	The key distribution center (KDC) servers provide security services to the CSP and include functions that participate in the authentication and key exchange processes.

EXHIBIT A

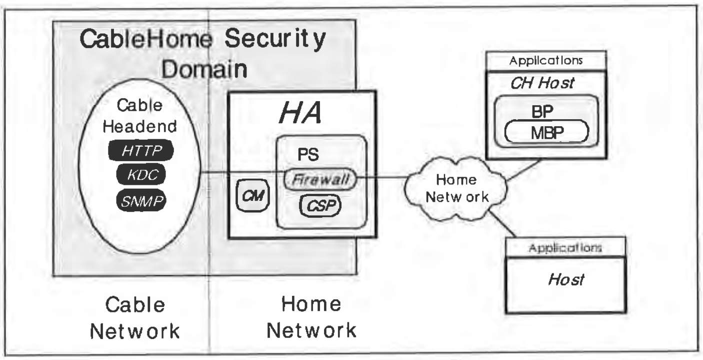


Figure 5-6 — CableHome Security Elements

5.2.3 CableHome QoS Functions

To support the CableHome Quality of Service requirements, CableHome defines functions for the PS and the BP. Portal Services QoS functions are located within the CableHome Residential Gateway and include a server function and other types of functions. BP QoS functions are located within CableHome Host devices and include a client and other types of functions. Examples of PS and BP QoS functions are introduced in Table 5-6 and Table 5-7 and are illustrated in Figure 5-7.

Table 5-6 — Portal Services QoS Functions

Portal Service QoS Functions	Description
QoS Characteristics Server (QCS)	Acquires QoS priority information for applications from the cable network management system Acquires BP application list from the BP. Provides information about application priorities to the BP, as established by the cable operator.
QoS Forwarding and Media access (QFM)	Orders the packets arriving from multiple LAN interfaces to the PS and forwards them to a destination LAN interface according to their priorities. Also provides prioritized access to the shared media during the packet transmission based on the packet priority.

Table 5-7 — BP QoS Function

Boundary Point QoS Functions	Description
QoS Characteristics Client (QCC)	Provides information to the PS about applications residing on the CableHome Host and also requests information about application priorities established by the MSO. Also provides prioritized access to the shared media during the packet transmission based on the packet priority.

EXHIBIT A

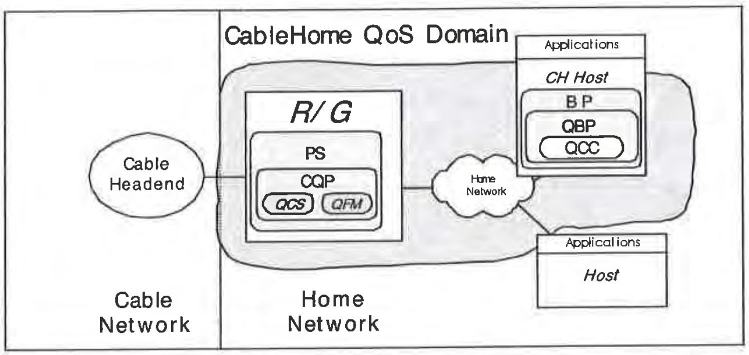


Figure 5-7 — CableHome QoS Elements

5.3 CableHome Messaging Interface Model

Communication between the functions in the cable data network, CableHome Residential Gateway, and LAN IP Devices occur on messaging interfaces identified and labeled in Figure 5-8. The types of messaging interfaces are differentiated by the elements that are involved in the communication.

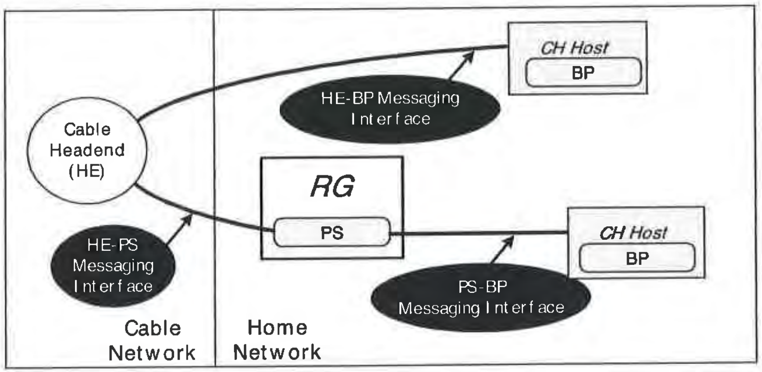


Figure 5-8 — CableHome Reference Interfaces

Table 5-8 identifies interfaces for which CableHome specifies messaging.

EXHIBIT A

Table 5-8 — Valid Interface Paths for Each Functionality

		Interface		
Functionality	**Protocol**	**HE-PS**	**HE-BP**	**RG-BP**
Name service	DNS	Unspecified	Unspecified	CableHome 1.1
Software Download	TFTP	CableHome 1.1	Unspecified	Unspecified
Address Acquisition	DHCP	CableHome 1.1	Unspecified	CableHome 1.1
Management (single) (bulk)	 SNMP TFTP or HTTP	 CableHome 1.1 CableHome 1.1	 Unspecified Unspecified	 Unspecified Unspecified
Event Notification	SNMP SYSLOG	CableHome 1.1 CableHome 1.1	Unspecified	Unspecified
QoS	PacketCable QoS Protocols, CableHome Priorities SOAP/XML	Unspecified	PacketCable	CableHome 1.1
Security (key distribution)	Kerberos	CableHome 1.1	Unspecified	Unspecified
Security (authentication)	Kerberos or TLS	CableHome 1.1	Unspecified	Unspecified
Ping	ICMP	CableHome 1.1	Unspecified	CableHome 1.1
Loopback/Echo	UDP/TCP	Unspecified	Unspecified	CableHome 1.1
Application Discovery	SNMP SOAP/XML	CableHome 1.1	Unspecified	CableHome 1.1

5.4 CableHome Information Reference Model

The operation of the CableHome management model is based upon a store of information maintained in the PS by the various sub-elements of the PS (CAP, CDP, CMP, etc.). These sub-elements need a means of interacting via information exchange, and the PS Database is a conceptual entity that represents a store for this information. The PS Database is not an actual specified database per se, but rather a tool to aid in the understanding of the information that is exchanged between the various CableHome elements.

Figure 5-9 shows the relationship between the database and the PS functions. Table 5-9 describes the typical information associated with each of these functions. Figure 5-10 shows a detailed example implementation indicating the set of information, the functions that derive the information, and the relationships between the functions and the information.

EXHIBIT A

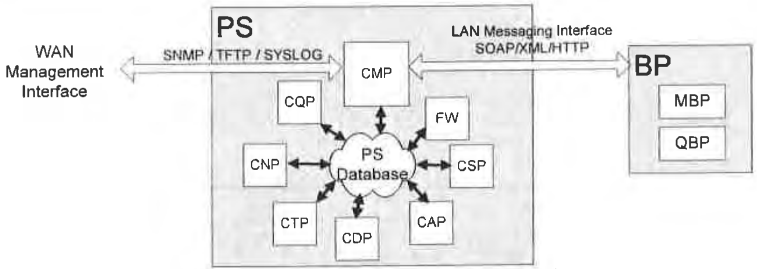


Figure 5-9 — PS Function and Database Relationship

The PS Database stores a myriad of data relationships. The CMP provides the WAN management interface (SNMP) to the PS database. The CableHome functions within the PS enter and revise data relationships in the PS Database. Additionally, the CableHome Functions within the PS may retrieve information from the PS Database that is maintained by other CableHome Functions within the PS.

Table 5-9 — Typical PS Database information examples

Name	Usage (In general)
CDP Information	Information associated with addresses acquired and allocated via DHCP.
CAP information	Information associated with CableHome address translation mappings.
CMP information	Information associated with the state of the PS functions. Information about CableHome Host devices.
CTP information	Information associated with results of LAN test performed by the CMP.
CNP information	Information associated with LAN IP Device name resolution.
USFS information	Information associated with the Upstream Selective Forwarding Switch function.
CSP information	Information associated with authentication, key exchange, etc.
Firewall information	Information associated with the behavior of the Firewall (ruleset), firewall events and logging.
Event information	Information associated with the local log for all general events, traps, etc.
CableHome Host Device Information	BP Device Profile information collected through BP_Init messaging from CableHome hosts.
CableHome Host QoS Characteristics Information	QoS Characteristics received from cable operator and QoS Profile information received from the CableHome hosts via BP_Init Messaging.

EXHIBIT A

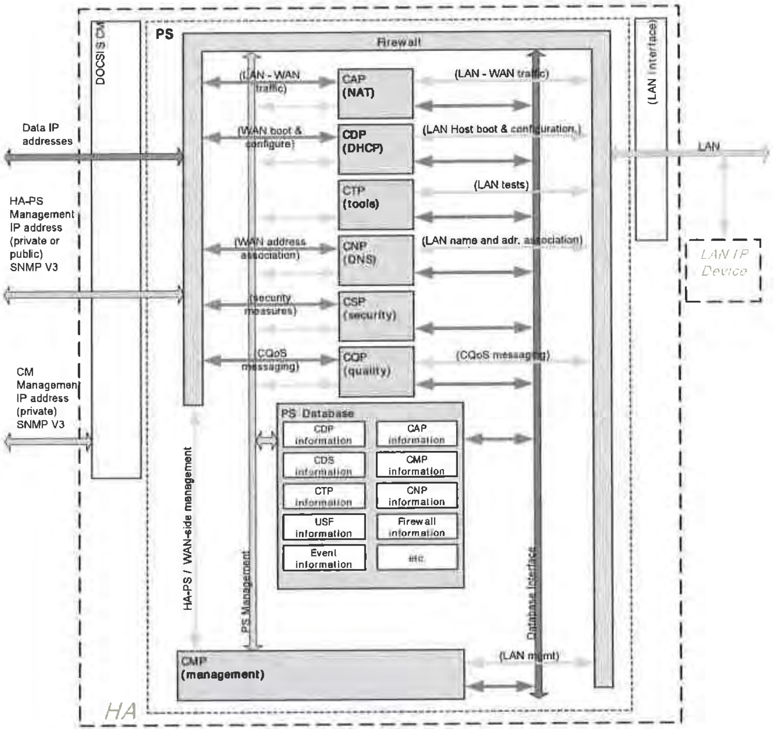


Figure 5-10 — PS Database Detailed Example Implementation

The PS is primarily managed from the WAN via the CMP, and to a large degree this involves access to the information in the PS Database. Management is used for initialization and provisioning of the PS functions, and remote diagnostics or status of the LAN. The diagnostics may rely on the CTP to get better visibility into the current state of the LAN. Connectivity and rudimentary network performance can be measured.

The CNP is the LAN Domain Name Server (DNS). All LAN-Trans LAN IP Devices are configured by the CDP to use the CNP as the primary Name Server. The CNP resolves textual host names of LAN IP Devices, returning their corresponding IP addresses and in addition, refers LAN IP Devices to external DNS servers for requests that cannot be answered from local information.

The CDP contains the address functions to act as the DHCP server in the LAN-Trans realm and implements a DHCP client in the WAN realms.

The CAP creates address translation mappings between the WAN-Data and LAN-Trans address realms. The CAP is also responsible for Upstream Selective Forwarding Switch decisions to preserve HFC upstream channel (WAN) bandwidth from the local LAN only traffic. Finally, the CAP contains the Passthrough function, which bridges traffic between the LAN and WAN address realms.

EXHIBIT A

The CSP provides PS authentication capabilities as well as key exchange activities.

The CQP is part of a system that enables CableHome QoS. The CQP provides CableHome traffic priorities as well as differentiated media access functions.

5.5 CableHome Operational Models

The functionality of the Portal Services element is compatible with a variety of cable network infrastructures, which are accommodated by a number of different PS operational modes. These various operating modes enable the PS to function properly within a DOCSIS 1.0, DOCSIS 1.1 and DOCSIS 2.0 infrastructure, as well as within an Extended CableHome infrastructure. The Extended CableHome infrastructure builds upon DOCSIS 1.0, 1.1, and 2.0 infrastructures to enable additional services, and incorporates a number of capabilities that are similar to those within a PacketCable provisioning system.

For the purpose of configuration, the PS may operate within one of two provisioning modes:

- The DHCP Provisioning Mode
- The SNMP Provisioning Mode

If the PS is not configured to operate in either DHCP Provisioning Mode or SNMP Provisioning Mode, it assumes that the CableHome back office support is not currently available, and will default to operate in Dormant CableHome Mode. In Dormant CableHome Mode, the CableHome Residential Gateway will be fully operational from the user perspective, but it will not be operator configured or managed.

When the PS is configured to operate in DHCP Provisioning Mode, it can be configured to begin a Transport Layer Security (TLS) session over HTTP in order provide secure download of PS and Firewall configuration files.

When the PS is operating within the DHCP Provisioning Mode, it can operate in one of two Network Management sub-modes:

- NmAccess Mode
- SNMP v3 Coexistence Mode

When the PS is configured to operate in SNMP Provisioning Mode, it operates in SNMPv3 Coexistence Network Management Mode only.

Figure 5-11 illustrates the various PS operational modes along with the associated triggers for each. See Section 7.3.3.2.4 (CDC Requirements) for a full description of provision mode determination.

EXHIBIT A

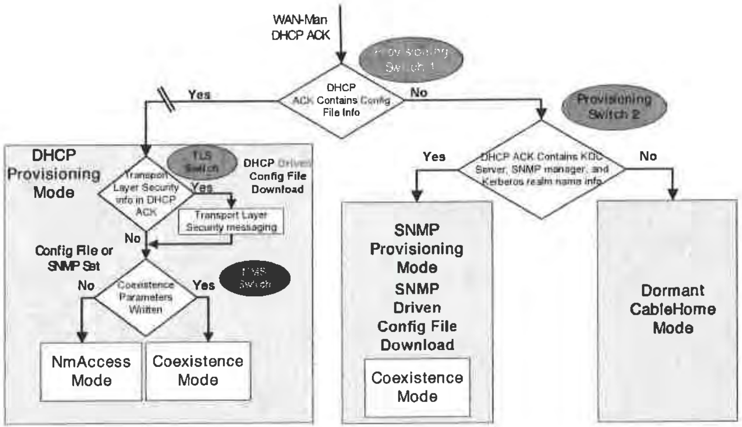

WAN-Man
DHCP ACK
Provisioning Switch 1
DHCP ACK Contains Config File Info
Yes
No
Provisioning Switch 2
DHCP Provisioning Mode
TLS Switch
Transport Layer Security info in DHCP ACK
Yes
DHCP Driven Config File Download
Transport Layer Security messaging
No
Config File or SNMP Set
No
Coexistence Parameters Written
Yes
NMS Switch
NmAccess Mode
Coexistence Mode
Yes
DHCP ACK Contains KDC Server, SNMP manager, and Kerberos realm name info
No
SNMP Provisioning Mode
SNMP Driven Config File Download
Coexistence Mode
Dormant CableHome Mode

Figure 5-11 — PS Operational Modes

Table 5-10 describes the infrastructures within which each PS mode is intended to operate.

Table 5-10 — PS Infrastructures

Mode	Capability Directly Effected	Intended Infrastructure
SNMP Provisioning Mode	Configuration file download.	Extended CableHome Infrastructure
DHCP Provisioning Mode	Configuration file download.	DOCSIS 1.0, 1.1, and 2.0 infrastructures with CableHome support
DHCP Provisioning Mode: with TLS/HTTP	Secure configuration file download	DOCSIS 1.0, 1.1, and 2.0 infrastructures with CableHome and TLS support
DHCP Provisioning Mode: NmAccess Network Management Mode	SNMP version used between NMS and PS	DOCSIS 1.0 Infrastructure (SNMP v1/v2) with CableHome support
DHCP Provisioning Mode: SNMP Coexistence Network Management Mode	SNMP version used between NMS and PS	DOCSIS 1.1 and 2.0, and Extended CableHome Infrastructures (SNMP v3) with CableHome support
Dormant CableHome Mode	Configuration and Management	No CableHome support

5.6 Physical Interfaces on the CableHome Residential Gateway[7]

There are many types of physical interfaces that may be implemented on a device containing PS functionality. Several are described in the following list:

- WAN Networking Interfaces, to the cable network via the cable modem acting as a transparent bridge for a PS with an embedded cable modem, and other WAN Networking Interfaces, intended for WAN connection, in the Standalone PS case.
- LAN Networking Interfaces for connection to LAN IP Devices and CableHome hosts.

[7] Revised title and last bullet paragraph per ECN CH1 1-N-03.0090-2 by GO on 12/5/03

EXHIBIT A

- Hardware Test Interfaces, such as JTAG and other proprietary approaches, which are part of the silicon and don't always have software controls to turn the interfaces off. These interfaces are hardware state machines that sit passively until their input lines are clocked with data. Though these interfaces can be used to read and write data, they require an intimate knowledge of the chips and the board layout and are therefore difficult to "attack". Hardware test interfaces MAY be present on a device implementing PS functionality. Hardware test interfaces MUST NOT be either labeled or documented for customer use.
- Management Access Interfaces, also called console ports, which are communications paths (usually RS-232, but could be Ethernet, etc.) and debugging software that interact with a user. The software prompts the user for input and accepts commands to read and write data to the PS. If the software for this interface is disabled, the physical communications path is disabled. A PS MUST NOT allow access to PS functions via a Management Access Interface. (CableHome PS functions are defined by the CableHome specification.) Access to PS functions MUST only be allowed via interfaces specifically prescribed by the CableHome specifications, e.g., operator-controlled access via SNMP.
- Read-only Diagnostic Interfaces can be implemented in many ways and are used to provide useful debug, trouble-shooting, and PS status information to users. A PS MAY have Read-only Diagnostic Interfaces.
- Some products might choose to implement higher layer functions (such as customer premise data network functions) that could require configuration by a user. A PS MAY provide the ability to configure non-CableHome functions. The PS SHOULD implement a User Interface to enable user configuration of non-CableHome functions and CableHome functions. The User Interface is permitted to provide user access to CableHome-defined management functions (i.e., to CableHome-defined MIB objects), but is required to adhere to cable operator-configured access rules. Refer to Section 6.3.3.1.4.2.2.

EXHIBIT A

6 MANAGEMENT TOOLS

6.1 Introduction/Overview

The CableHome Management Tools provide the cable operator with functionality to monitor and configure the Portal Services (PS) element, to discover LAN IP Devices and the applications they offer, to remotely check connectivity between the PS and LAN IP Devices, to provide Quality of Service policy to BPs in support of prioritized QoS between CableHome Host devices, and to report on status and exception events in the PS. This section describes and specifies requirements for these capabilities.

Differences between Management Tools defined in the CableHome 1.0 specification and those defined in this specification are listed below:

- CableHome 1.1 adds the requirement for the PS to support SNMP management from any LAN Interface
- CableHome 1.1 adds the requirement for both the PS and the BP to support PS-BP messaging for the exchange of QoS priorities
- CableHome 1.1 adds the requirement for the BP to implement a device profile in XML format
- CableHome 1.1 adds the following MIB objects to the PS:
  - objects needed to support prioritized Quality of Service on the LAN
  - objects supporting enhanced firewall functionality
  - objects enabling the cable operator to discover attributes of CableHome Host devices

6.1.1 Goals

The goals for the CableHome Management Tools include:

- Provide a means for the cable operator to discover LAN IP Devices.
- Provide cable operators with visibility to LAN IP Devices.
- Provide cable operators with visibility to applications on CableHome Host devices.
- Define a method for passing QoS priorities to the applications on CableHome Host devices.
- Define a minimum set of remote diagnostic tools that will allow the cable operator to verify connectivity between the Portal Services element and any LAN IP Device.
- Provide cable operators with access, via the MIBs, to internal data in the PS element and enable the cable operator to monitor CableHome-specified parameters and to configure or re-configure CableHome-specified capabilities as necessary.
- Provide a means for reporting exceptions and other events in the form of SNMP traps, messages to a local log, or messages to a system log (SYSLOG) in the cable network.

6.1.2 Assumptions

The assumptions for the CableHome network management environment include the following:

- CableHome-compliant devices implement the Internet Protocol (IPv4) suite of protocols.
- CableHome Host Devices implement a Device Profile and a Quality of Service Profile in XML format.
- SNMP is used for the exchange of management messages between the cable network NMS and the PS in the CableHome Residential Gateway device. SNMP provides visibility for the NMS to interfaces on the PS, via access to internal PS data, through required MIBs.

EXHIBIT A

- Any of SNMPv1/v2c/v3 can be used as a management protocol between the NMS and the CableHome Portal Services element.
- LAN IP Devices implement a DHCP client.
- The CableHome Residential Gateway and LAN IP Devices support ICMP.
- The PING utility supplies functionality sufficient to provide the cable operator with the desired information about connectivity between the PS element and LAN IP Devices.

6.2 Management Architecture

6.2.1 System Design Guidelines

The CableHome 1.1 Management Tools system design guidelines are listed in Table 6-1. This list provided guidance for the development of the CableHome management tools specifications.

Table 6-1 — Management Tools System Design Guidelines

Reference	Management Tools System Design Guidelines
Mgmt 1	The PS will implement SNMPv1/v2c/v3 protocols to provide access to internal Portal Services data
Mgmt 2	The PS will be capable of issuing a an ICMP Request (Ping) command to any LAN IP Device specified by the cable operator and store results in the PS Database. Remote Ping test results will be accessible through CTP MIB objects.
Mgmt 3	The PS will be capable of executing a Connection Speed Test with a specified LAN IP Device specified by the cable operator and store results in the PS Database. Remote Connection Speed test results will be accessible through CTP MIB objects.
Mgmt 4	The PS element will be capable of reporting events
Mgmt 5	The PS element will be capable of communicating with CableHome Host devices in the LAN-Pass and LAN-Trans realms for the exchange of device attributes, QoS priorities, and CableHome Host application information.
Mgmt 6	In the event that the PS loses connectivity with the cable data network and its applications, the Discovery function and LAN Messaging function will continue to operate.

6.2.2 Management Tools System Description

As shown in Figure 6-1, CableHome Management Tools architecture consists of the following components: (1) the CableHome Management Portal (CMP), (2) the CableHome Test Portal (CTP), (3) a Management Information Base (MIB), (4) an SNMP Network Management System (NMS) that is part of the cable network, and (5) a Device Profile in XML format implemented by each CableHome Host device (BP logical element).

EXHIBIT A

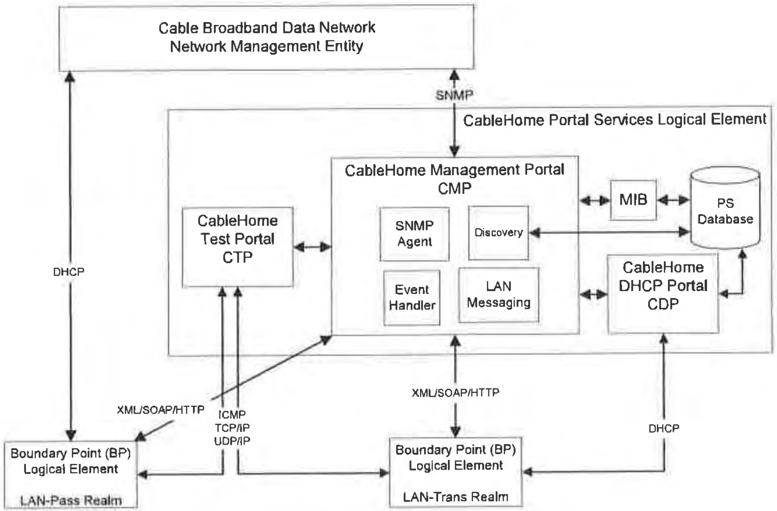


Figure 6-1 — CableHome Management Architecture

The cable data network NMS monitors and configures the PS by accessing the PS Database through MIBs specified in Section 6.3.3.1.4.7. The cable operator accesses CableHome Host Device and CableHome Residential Gateway attributes through the PSDev MIB [CH5] and through the QoS MIB [CH7], and configures CableHome Host devices with QoS policy (in the form of QoS priorities) using the PS as a proxy.

Upon receiving DHCP ACKNOWLEDGE (DHCPACK) [RFC 2131] from its DHCP server the BP logical element in each CableHome Host device initiates communication with the PS via a LAN messaging interface. This messaging, in the form of Simple Object Access Protocol (SOAP) on Hypertext Transfer Protocol (HTTP) transport, is done to inform the PS of device attribute information (Device Profile) and a list of applications (QoS Profile) implemented in the CableHome Host. When the PS receives the Device Profile and QoS Profile it does the following:

- Stores the BP Device Profile information in a BP device profile MIB table (cabhPsDevBpProfileTable).

  The BP Device Profile enables the cable operator to discover information about CableHome Host devices in the LAN-Pass realm, and provides the cable operator with information about CableHome Host devices in the LAN-Trans realm in addition to the information obtained via DHCP messaging between the PS and the LAN-Trans BP.

 Processes the BP QoS Profile information as described in Section 10.3.2.4.2 LAN Information Exchange.[8]

The NMS can also directly communicate with LAN IP Devices in the CableHome LAN-Pass realm.

[8] Revised this paragraph per ECN CH1.1-N-03.0109-1 by KB on 4/5/04.

EXHIBIT A

The CableHome DHCP Portal, described in the Provisioning Tools section (Section 7), plays a role in basic LAN IP Device discovery. Through DHCP communication between LAN IP Devices and the CDP, the LAN IP Device provides its hardware address and may provide configuration information to the CMP through DHCP Option codes. The CMP will use the information to populate CDP MIB LAN Address Table (cabhCdpLanAddrTable) objects.

The CMP and CTP functional elements reside within the PS. The PS logical element may be co-resident with an embedded cable modem or stand alone, without embedded cable modem functionality, as described in Section 5.1.3.1.1.

The CM and PS are separate and independent management entities. In the case of a PS with an embedded cable modem, no data sharing between CM and PS is implied, with the following exceptions:

1. the software image download is controlled via the cable modem's MIB,
2. the MIB for SNMP [RFC 3418], the SNMP Group of MIB-2 (mib-2 11) [RFC 1213], the IP Group and the ICMP Group of the SNMPv2 MIB for IP [RFC 2011], and the SNMPv2 MIB for UDP [RFC 2013] are allowed to be shared between the PS and CM.

In a PS with an embedded cable modem, the cable modem's docsDevSoftware objects are accessed to set up, initiate, and monitor the download of a single combined software image. This process is described in Section 11.8, Secure Software Download for the PS.

Because of this management independence, the CM and PS respond to different and independent management IP addresses. CM MIB Objects are only visible when the manager accesses them through the CM management IP address, and are not visible via the PS management IP address (and vice-versa). The SNMP access rights to the PS and CM entities MUST be set independently. CableHome does not preclude the use of a single SNMP agent for a PS with an embedded CM.

The Portal Services element supports SNMPv1, SNMPv2c, and SNMPv3 protocols. Section 5.5 introduced the provisioning modes supported by a CableHome Portal Services element, and Section 7 provides additional detail about these modes. The provisioning mode in which the PS is operating partially determines which version of SNMP the PS uses. Additional detail is provided in Section 6.3.3.

6.3 PS Logical Element - CableHome Management Portal (CMP)

The CableHome Management Portal (CMP) is a sub-element of the PS logical element. It serves as the hub of management control of the PS and for discovery of devices present on the LAN.

The CMP aggregates and interconnects management information in the WAN-Man and LAN-Trans realms, since they are not directly accessible to each other.

6.3.1 CMP Goals

The goals for the CableHome Management Portal include:

- Enable the NMS to remotely view and update CableHome Address Portal (CAP) configuration information
- Enable the NMS to remotely view and update Firewall configuration information
- Enable remote testing of connectivity between the CableHome Residential Gateway and LAN IP Devices in the LAN-Trans realm, via the CableHome Test Portal (CTP)
- Enable remote configuration of LAN IP Device Addressing parameters
- Enable viewing of LAN IP Device information obtained via the CableHome DHCP Portal (CDP)

EXHIBIT A

- Provide cable operator access to the attributes of CableHome Host devices and applications implemented by CableHome Host devices, acquired through the CableHome discovery process
- Support the exchange of device attributes, application list, and QoS priorities for applications between the CableHome Residential Gateway and CableHome Host devices
- Enable viewing of the results of LAN IP Device performance monitoring done by the CableHome Test Portal (CTP)
- Enable the NMS to access other PS configuration parameters
- Facilitate security by providing access to security parameters, and the use of SNMPv1/v2c/v3 in the appropriate network management mode
- Provide the capability to disable LAN segments

6.3.2 CMP Design Guidelines

The CableHome 1.1 CMP design guidelines are listed in Table 6-2. This list provides guidance for the specification of CMP functionality.

Table 6-2 — CMP System Design Guidelines

Reference	CMP System Design Guidelines
CMP 1	Interfaces will support the management and diagnosis features and functions required to support cable-based services provisioned across the home network.
CMP 2	Loss of connection between broadband service provider(s) and the home network will not disable or degrade the operation of internal home networking functions
CMP 3	The home network will recover from a power outage, and devices connected to the home network must return to the operational state they were in prior to the outage.
CMP 4	Home network devices will be easy to install and configure for operation, much like a home appliance.
CMP 5	The PS and LAN IP Devices will support a protocol for discovering LAN IP Devices connected to the home LAN.
CMP 6	The PS will provide to the cable operator, upon request, information about devices added to the home LAN.
CMP 7	The PS and BP will support a protocol for exchanging CableHome Host Device attributes and applications implemented by CableHome Host Devices, and the QoS priorities for those applications.
CMP 8	The PS will provide to the cable operator, upon request, information about CableHome Host Device attributes and applications implemented by CableHome Host Devices.
CMP 9	Discovery protocol message exchange within the home LAN will not noticeably degrade performance of the home LAN.
CMP 10	Discovery messaging will not propagate onto the WAN.

6.3.3 CMP System Description

The CMP is responsible for the following important CableHome capabilities:

- Enable management of the Portal Services functions from the cable operator's data network Network Management System (NMS) by providing access to the PS Database and its state variables through CableHome-specified Management Information Base (MIB) objects
- Enable visibility to the PS Database for the subscriber through CableHome-specified MIB objects
- Enable exchange of QoS priorities between the PS and BP
- Enable the manager to remotely discover devices connected to the home LAN and the applications running on them
- Process and log event messages

EXHIBIT A

The CMP is comprised of the following four functions to support the management and discovery responsibilities listed above. These functions are also shown in Figure 6-1:

1. SNMP agent function:

   The SNMP agent function receives and processes SNMP messages from the WAN Interface through the WAN-Man IP address and from the LAN Interface, through the PS Server Router IP address. It provides access to MIB objects for the purpose of monitoring and/or configuring PS and LAN IP Device functionality.

2. Event handling function:

   The CMP reports events according to the settings of the docsDevEvent table settings. The list of supported events appears in Appendix II.

3. Discovery function:

   The CMP, through its discovery functionality, acquires information about each CableHome Host device and the applications on it. The CMP stores this information in the PS database and makes it available to an SNMP management entity, via the PSDev MIB [CH5] and QoS MIB [CH7].

4. LAN Messaging function:

   The CMP exchanges QoS parameters and Device Profile attributes in XML format, with CableHome Hosts across the LAN using Simple Object Access Protocol.

These functions are described in Section 6.3.3.1 - Section 6.3.3.4.

6.3.3.1 CMP SNMP Agent Function

6.3.3.1.1 SNMP Agent Function Goals

Goals of the SNMP Agent function of the CMP are listed below:

- Receive and process SNMP messages received through PS WAN-Man and PS Server Router (LAN) Interfaces
- Provide SNMP manager access to the PS Database through CableHome-specified MIBs
- Enforce PS Database access rules defined by the docsDevNmAccessTable and VACM views
- Support authentication and encryption/decryption processes for SNMP defined by IETF RFCs
- Adhere to SNMP implementation rules and guidelines defined by IETF RFCs

6.3.3.1.2 SNMP Agent Function System Design Guidelines

The system design guidelines listed in Table 6-3 guided development of SNMP Agent Function requirements.

Table 6-3 — System Design Guidelines

Reference	SNMP Agent Function System Design Guidelines
SNMP Agent 1	The PS will provide remote access to manageable parameters in the PS database via CableHome specified MIBs.
SNMP Agent 2	The PS will implement an SNMP agent compatible with existing cable data network management systems.

EXHIBIT A

Reference	SNMP Agent Function System Design Guidelines
SNMP Agent 3	The PS will support access control methods enabling the cable operator to configure control of PS Database access.

6.3.3.1.3 SNMP Agent Function System Description

The CMP SNMP Agent function serves as the hub of Management control for WAN side management accesses and it gathers information for, and interconnects management of, WAN Management and LAN network elements. It also supports management messaging, via SNMP through any LAN Interface.

The CMP works in any of three network management modes:

- SNMP Provisioning Mode/SNMPv3 Coexistence Management Mode
- DHCP Provisioning Mode/NmAccess Table Management Mode
- DHCP Provisioning Mode/SNMPv3 Coexistence Management Mode

SNMP Provisioning Mode/SNMP Coexistence Management Mode

As described in Section 5.5, when in SNMP Provisioning Mode, the PS defaults to operating in SNMPv3 Coexistence Mode with SNMPv1 and SNMPv2 not enabled, and uses Kerberos to distribute keying material. User-based Security Model (USM) [RFC 3414] and View-based Access Control Model (VACM) [RFC 3415] are supported to allow the cable operator to implement management policy for access to CableHome-specified MIBs.

DHCP Provisioning Mode/NmAccessTable Management Mode

As described in Section 5.5, when in DHCP Provisioning Mode, the PS defaults to operate in NmAccess Table mode. In NmAccessTable mode, management access is controlled by the NmAccessTable of the DOCSIS Device MIB [RFC 2669] and the SNMPv1/v2c protocols are supported.

DHCP Provisioning Mode/SNMPv3 Coexistence Management Mode

When the PS is operating in DHCP Provisioning Mode, the cable operator can populate the Coexistence Table via SNMP set-request messages or via PS configuration file, thereby configuring the PS to operate in SNMPv3 Coexistence Management Mode. For a PS configured to operate in SNMPv3 Coexistence Mode, management access is controlled as described in [RFC 2576], the SNMPv1/v2c/v3 protocols are supported, USM and VACM are supported, and SNMPv3 keying material is distributed using [RFC 2786] and TLVs in the PS Configuration File.

Table 6-4 contains definitions for terms that are specific to the CMP.

Table 6-4 — Definition of Terms

Management-control	Read or write access to a set of parameters that control or monitor the behavior of the PS.
PS Database	A set of parameters that controls or monitors the behavior of the PS element readable by the WAN management system. It can be thought of as a repository of information describing the current state of the PS.
User	As defined in SNMP (section 2.1 of [RFC 3414]), a User has a name associated with it, associated security definitions and access to a View.
View	A View is a set of MIB objects and the access rights to those objects. Each View has a name and it is associated with a User (section 2.4 of [RFC 3415]).
Ultimate Authorization	The single authority that establishes, modifies, or deletes User IDs, authentication keys, encryption keys, and access rights to the PS Database. This User is entrusted with all security management operations.

EXHIBIT A

Maintenance User	A User that typically performs only read-only operations on the PS database. This is typically used for performance monitoring and accounting.
Administrator User	A User that typically performs both read and write operations on the PS database. These operations are used for Configuration and Fault Management.

Examples of the types of information that can be read or manipulated via CableHome Management-control include the firewall policy settings, NMS-configured NAT mappings, remote diagnostic tool initiation and results access, PS status, discovered device and applications information, and LAN address range configuration. As will be illustrated later, the various management messaging interfaces may have access rights to different sets of parameters. A CableHome 1.1-compliant PS supports access to the PS database through the MIB hierarchy from both the WAN and LAN using SNMP. CableHome 1.1-compliant CableHome Host devices can also exchange messages with the CableHome Residential Gateway using XML-formatted data transported, via HTTP. Figure 6-2 indicates management messaging interfaces:

- NMS - CMP: management message exchange between the cable network NMS and the CMP.
- CMP - CableHome Host/LAN-Trans: message exchange between the CMP and CableHome Hosts in the LAN-Trans realm.
- CMP - CableHome Host/LAN-Pass: message exchange between the CMP and CableHome Hosts in the LAN-Pass realm.
- NMS - LAN IP Device: management message exchange between the cable network NMS and LAN IP Devices in the LAN-Pass realm. This management messaging is outside the scope of the CableHome 1.1 specification.

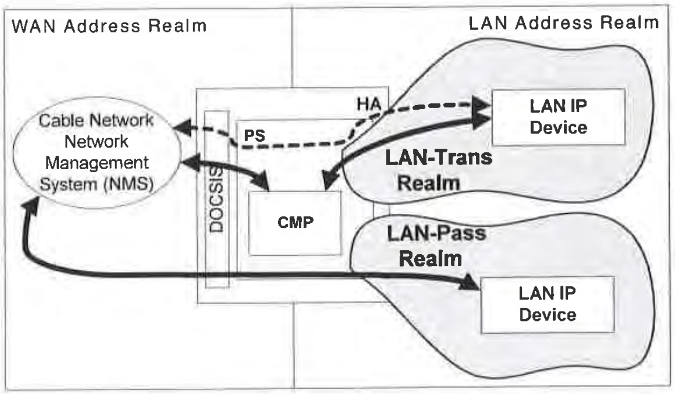


Figure 6-2 — CableHome Management Message Interfaces

The CMP is primarily a WAN (NMS) accessed and WAN controlled entity, but also supports access from the PS LAN interface (Server Router address - usually the default gateway for LAN IP Devices in the LAN-Trans realm). Additionally the CMP may be called upon to inform the cable network NMS of events or transfer system log files as required. An example of a CMP implementation is illustrated in Figure 6-3, to convey concepts for CMP functionality.

EXHIBIT A

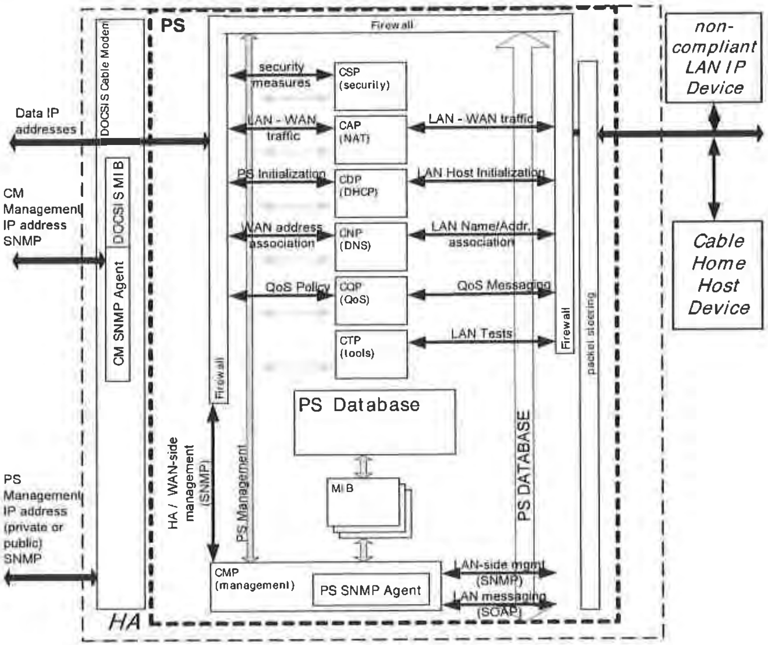


Figure 6-3 — PS Block Diagram

The NMS management tools use SNMP to access and manage objects in the PS. If the PS is operating in SNMPv3 Coexistence Mode, SNMPv3 provides NMS operator User authentication to the PS, view-based access to the management information base (MIB) objects in the PS, and encryption of management messages if requested.

The CMP SNMP agent function has the task of mapping the Object ID (OID) and the instance of the OID for all the leaves within the functional blocks in the PS, such as the CAP or local storage such as the PS Database.

A cable data network NMS operator may access or "manage" CableHome Hosts in one of two ways The cable operator can directly access CableHome Hosts using pass-through addressing between the cable network and the LAN device element (BP) to be managed. The cable operator can also access BP Device profile attributes through the PSDev MIB in the PS and a list of BP applications and their priorities through the QoS MIB in the PS. The cable operator accesses these MIBs via SNMP set-request or SNMP get-request messages issued to the PS WAN-Man IP address and the PS, acting as a management proxy, accesses a BP using SOAP/HTTP. The cable operator can provision QoS Policy, in the form of QoS priorities for CableHome Host applications, in the PS via SNMP.

EXHIBIT A

6.3.3.1.4 SNMP Agent Function Requirements[9]

The PS MUST implement an SNMP agent compliant with IETF RFCs as indicated in Section 6.3.3.1.4.1, "SNMP Protocol Requirements," on page 51.

When operating in DHCP Provisioning Mode or SNMP Provisioning Mode (cabhPsDevProvMode = dhcpmode(1) or snmpmode(2)), the SNMP agent in the PS MUST only receive and process SNMP messages from the WAN that are addressed to its WAN-Man IP address.

When operating in DHCP Provisioning Mode or SNMP Provisioning Mode (cabhPsDevProvMode = dhcpmode(1) or snmpmode(2)), while in NAPT or NAT Primary Packet-handling Mode (cabhCapPrimaryMode = napt(1) or nat(2)), the SNMP agent in the PS MUST only receive and process SNMP messages from the LAN that are addressed to its LAN side CDP Server Router address (cabhCdpServerRouter).

When operating in DHCP Provisioning Mode or SNMP Provisioning Mode (cabhPsDevProvMode = dhcpmode(1) or snmpmode(2)), while in Passthrough Primary Packet-handling Mode (cabhCapPrimaryMode = passthrough(3)), the SNMP agent in the PS MUST only receive and process SNMP messages from the LAN that are addressed to its LAN side Well Known PS LAN IP Address (192.168.0.1).

When operating in Dormant CableHome Mode (cabhPsDevProvMode = dormantCHmode(3)), the SNMP agent in the PS MUST ignore all SNMP messages from the WAN and MUST only receive and process SNMP messages from the LAN that are addressed to its LAN side CDP Server Router address (cabhCdpServerRouter).

The PS MUST ignore SNMP messages received through any LAN interface addressed to the PS WAN-Man IP address.

In the case of a PS co-resident with an embedded cable modem, i.e., an embedded PS, the PS and cable modem MUST respond to different and independent management IP addresses.

The PS MUST implement ICMP Echo and Echo Reply Message types (Type 8 and Type 0) as described in [RFC 792], and reply appropriately to Ping requests received on any interface.

If the PS is operating in DHCP Provisioning Mode (indicated by a value of '1' in cabhPsDevProvMode) the PS MUST default to using SNMPv1/v2c for management messaging with the NMS and follow rules for NmAccess mode and Coexistence Mode, described in Section 6.3.3.1.4.2.1, "Network Management Modes for a PS Operating in DHCP Provisioning Mode," on page 52.

If the PS is operating in SNMP Provisioning Mode (indicated by a value of '2' in MIB object cabhPsDevProvMode), the PS MUST use SNMPv3 for management messaging with the NMS, following rules described in Section 6.3.3.1.4.3, "Network Management Mode for a PS Operating in SNMP Provisioning Mode," on page 54.

When the PS is operating in SNMP Coexistence Mode, the default Ultimate Authorization setting MUST be WAN Administrator (CHAdministrator).

The PS MUST include - in the following specified order - the hardware version, vendor name, boot ROM image version, software version, and model number in the sysDescr object (from [RFC 3418]). The format of the specific information contained in the sysDescr MUST be as shown in Table 6-5:

[9] Revised this section per ECN CH1.1-N-03.0077-4 by GO on 12/2/03.

EXHIBIT A

Table 6-5 — Format of sysDescr Fields

To Report	Format of Each Field
Hardware Version	HW_REV: <hardware version>
Vendor Name	VENDOR: <vendor name>
Boot ROM	BOOTR: <boot ROM version>
Software Version	SW_REV: <software version>
Model Number	MODEL: <model number>

The sysDescr MUST be composed of a list of five Type/Value pairs enclosed in double angle brackets. The separation between the Type and Value is ": " - a colon and a blank space. For instance, a sysDescr of a PS of vendor X, hardware version 5.2, Boot ROM version 1.4, software version 2.2, and model number X would appear as follows:

anytext<<HW_REV: 5.2, VENDOR: X; BOOTR: 1.4; SW_REV: 2.2; MODEL: X>>any text

The PS MUST report in the sysDescr at least all of the information necessary to determine what software and firewall policy versions the PS is capable of loading. If any fields of the sysDescr object are not applicable, the PS MUST report "NONE" as the value. For example, a PS with no BOOTR will report "BOOTR: NONE".

The value of the docsDevSwCurrentVers MIB object MUST contain the same software version information as that contained in the software version information included in the sysDescr object.

When a PS and a CM are embedded in the same device, the sysDescr and docsDevSwCurrentVers objects of the PS MUST report the same values as those of the CM.

The sysObjectID object of the MIB-2 System group [RFC 3418] MUST be implemented and MUST be persistent across device reset and power cycles.

The sysUpTime object of the MIB-2 System group [RFC 3418] MUST be implemented. SysUpTime is the amount of time that has elapsed since the system reset.

The sysContact object of the MIB-2 System group [RFC 3418] MUST be implemented and MUST be persistent across device reset and power cycles. SysContact returns the name of the user or system administrator if known.

The sysLocation object of the MIB-2 System group [RFC 3418] MUST be implemented and MUST be persistent across device reset and power cycles.

The sysServices object of the MIB-2 System group [RFC 3418] MUST be implemented and MUST be persistent across device reset and power cycles.

The sysName object of the MIB-2 System group [RFC 3418] MUST be implemented and MUST be persistent across device reset and power cycles. Querying sysName returns the system name.

The Interfaces Group MIB [RFC 2863] MUST be implemented in accordance with Appendix I and requirements in Section 6.3.3.1.4.8.

The MIB-2 SNMP group [RFC 3418] MUST be implemented.

EXHIBIT A

The snmpSetSerialNo object of the snmpSet group [RFC 3418] MUST be implemented. SnmpSetSerialNo is an advisory lock used to allow several cooperating SNMPv2 entities, all acting in a manager role, to coordinate their use of the SNMPv2 set operation.

The PS MUST count LAN-to-WAN and WAN-to-LAN octets as defined by cabhPsDevLanIpTrafficTable [CH5], according to the value of cabhPsDevLanIpTrafficEnabled [CH5].[10]

When the PS element MIB objects are set to their factory defaults using the cabhCapSetToFactory, cabhCdpSetToFactory, cabhCtpSetToFactory, or cabhPsDevSetToFactory MIB objects the corresponding PS functionality MUST use these factory default settings for operation without having to re-provision the PS element.

6.3.3.1.4.1 SNMP Protocol Requirements

The PS MUST adhere to or implement, as appropriate, the following IETF RFCs:

- "A Simple Network Management Protocol" [RFC 1157]
  NOTE: This RFC has been declared "historic" by [RFC 3410]. The PS is required to support SNMPv1.
- "Introduction to Community-based SNMPv2" [RFC 1901]
  NOTE: This RFC has been declared "historic" by [RFC 3410]. The PS is required to support SNMPv2c.
- "Introduction and Applicability Statements for Internet Standard Management Framework" [RFC 3410]
- "An Architecture for Describing Simple Network Management Protocol Management Frameworks" [RFC 3411]
- "Message Processing and Dispatching for SNMP" [RFC 3412]
- "Simple Network Management Applications" [RFC 3413]
- "User-based Security Model (USM) for the Simple Network Management Protocol" [RFC 3414]
- "View-based Access Control Model (VACM) for the Simple Network Management Protocol" [RFC 3415]
- "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)" [RFC 3416]
- "Transport Mappings for the Simple Network Management Protocol" [RFC 3417]
- "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)" [RFC 3418]
- "Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework" [RFC 2576]

In support of SMIv2, the PS MUST implement the following IETF RFCs:

- "Structure of Management Information Version 2 (SMIv2)" [RFC 2578]
- "Textual Conventions for SMIv2" [RFC 2579]
- "Conformance Statements for SMIv2" [RFC 2580]

6.3.3.1.4.2 Network Management Mode Requirements

Section 5.5 introduced two provisioning modes, (DHCP Provisioning Mode and SNMP Provisioning Mode) and two network management modes (NmAccessTable Mode and SNMPv3 Coexistence Mode) that the PS is required to support. Section 7.3.3.1 and Section 7.3.3.2 provide additional detail about PS operation in each of the two provisioning modes, in addition to Dormant CableHome Mode of operation.

[10] Deleted two previous paragraphs and added this per ECN CH1.1-N-03051 by GO on 07/07/03.

EXHIBIT A

This section describes rules for the network management modes the PS is required to support. Section 6.3.3.1.4.2.1 and its sub-sections describe network management modes for a PS operating in DHCP Provisioning Mode. Section 6.3.3.1.4.3 and its sub-sections describe network management modes for a PS operating in SNMP Provisioning Mode.

The PS can operate in SNMPv3 Coexistence network management mode, regardless of whether it is configured to operate in DHCP Provisioning Mode or SNMP Provisioning Mode. It defaults to operation in SNMPv3 Coexistence mode when operating in SNMP Provisioning Mode. When operating in DHCP Provisioning Mode the PS defaults to operating in NmAccessTable network management mode, but can be configured to operate in SNMPv3 Coexistence Mode.

Control of access to the MIBs implemented by the PS depends upon the network management mode in which the PS is configured to operate. When the PS is configured to operate in NmAccessTable network management mode, MIB access is controlled by writing to the docsDevNmAccessTable [RFC 2669]. When operating in SNMPv3 Coexistence Mode, access to the MIBs is controlled by the SNMPv3 tables ([RFC 2576], [RFC 3413], [RFC 3414], and [RFC 3415]). The SNMPv3 tables can be configured by the NMS through SNMP Set commands, or via the PS Configuration File. Section 6.3.3.1.4.6 Mapping TLV Fields Into Created SNMPv3 Table Rows describes how PS Configuration File configuration parameters are mapped into these SNMPv3 tables.

6.3.3.1.4.2.1 Network Management Modes for a PS Operating in DHCP Provisioning Mode

The PS MUST support SNMPv1, SNMPv2c, and SNMPv3 and SNMP Coexistence as described by [RFC 3411] through [RFC 3415] and [RFC 2576]. The PS MUST also support NmAccessTable mode as defined by [RFC 2669]. Support for the network management modes for a PS operating in DHCP Provisioning Mode is subject to the guidelines described in Section 6.3.3.1.4.2.2, Section 6.3.3.1.4.3, and Section 6.3.3.1.4.4.

6.3.3.1.4.2.2 Basic Operation for a PS Operating in DHCP Provisioning Mode

Initial operation of the PS configured for DHCP Provisioning Mode can be thought of as having three steps: (1) behavior of the PS after it has been configured for DHCP Provisioning Mode, but before its network management mode has been configured via the PS Configuration File; (2) determination of the network management mode, and; (3) behavior of the PS after its network management mode has been configured. Rules of operation for each of these steps follow:

1. Once the PS has been configured to operate in DHCP Provisioning Mode (indicated by a cabhPsDevProvMode value of '1' (DHCPmode)), but before it has been configured for a network management mode, the PS MUST operate as follows:

- All SNMP packets are dropped.
- None of the SNMPv3 MIBs (Community MIB, TARGET-MIB, VACM-MIB, USM-MIB, NOTIFICATION-MIB) are accessible to the SNMP manager in the NMS.
- None of the elements in the SNMP-USM-DH-OBJECTS-MIB is accessible to the SNMP manager in the NMS.
- The PS Configuration File specified in the DHCP OFFER is downloaded and processed.
- Successful processing of all MIB elements in the PS Configuration File MUST be completed before beginning the calculation of the public values in the USMDHKickstart Table.

2. If a PS is operating in DHCP Provisioning Mode, the content of the PS Configuration File determines the network management mode, as described below:

EXHIBIT A

- The PS is in SNMPv1/v2c docsDevNmAccess mode if the PS Configuration File contains ONLY docsDevNmAccess Table setting for SNMP access control.
- If the PS Configuration File does not contain SNMP access control items (docsDevNmAccessTable or snmpCommunityTable or TLV 34.1/34.2 or TLV38), then the PS is in NmAccess mode.
- If the PS Configuration File contains snmpCommunityTable setting and/or TLV type 34.1 and 34.2 and/or TLV type 38, then the PS is in SNMP Coexistence Mode. In this case, any entries made to the docsDevNmAccessTable are ignored.

3. After completion of the provisioning process described in Section 13.2 (indicated by the value 'pass' (1) in cabhPsDevProvState), the PS operates in one of two network management modes. The network management mode is determined by the contents of the PS Configuration File as described above. Rules for PS operation for each of the two network management modes follow:

NmAccess Mode using SNMPv1/v2c

- The PS MUST process SNMPv1/v2c packets and drop SNMPv3 packets.
- docsDevNmAccessTable controls access and trap destinations as described in [RFC 2669]. The PS operating in NmAccess Network Management Mode MUST enforce the management access policy, as defined by the NmAccess Table, for any access to the CableHome-specified MIB objects, regardless of the interface (such as a vendor-specific graphical user interface (GUI)) or access protocol used.[11]
- None of the SNMPv3 MIBs (Community MIB, TARGET-MIB, VACM-MIB, USM-MIB, NOTIFICATION-MIB) is accessible.

When the PS is operating in SNMP v1/v2c NmAccess mode it MUST support the capability of sending traps as specified by the following MIB object (proposed MIB extension to the docsDevNmAccess table):

```
DocsDevNmAccessTrapVersion OBJECT-TYPE

   SYNTAX INTEGER {

         DisableSNMPv2trap(1),

         EnableSNMPv2trap(2),

          }

   MAX-ACCESS read-create

   STATUS current

   DESCRIPTION

      "Specifies the TRAP version that is sent to this NMS. Setting this object to
disableSNMPv2trap

         (1) causes the trap in SNMPv1 format to be sent to particular NMS. Setting this object to

         EnableSNMPv2trap(2) causes the trap in SNMPv2 format be sent to particular NMS"

   DEFVAL { DisableSNMPv2trap }

   ::={docsDevNmAcessEntry 8}
```

[11] Revised this bullet statement per ECN CH1.1-N-03.0090-2 by GO on 12/5/03.

EXHIBIT A

Coexistence Mode using SNMPv1/v2c/v3

When in SNMPv3 Coexistence Mode, the PS MUST support the "SNMPv3 Initialization" and "DH Key Changes" requirements specified in Section 11.4.4.1.3 and Section 11.4.4.1.4. These requirements include calculation of USM Diffie-Hellman Kickstart Table public parameters. The following rules for PS operation apply during and after calculation of the public parameters (values) as indicated:

During calculation of USMDHKickstartTable public values:

- The PS MUST NOT allow any SNMP access from the WAN.
- The PS MAY continue to allow access from the LAN with the limited access as configured by USM MIB, community MIB and VACM-MIB.

After calculation of USMDHKickstartTable public values:

- The PS MUST send the cold start or warm start trap to indicate that the PS is now fully SNMPv3 manageable.
- SNMPv1/v2c/v3 Packets are processed as described by [RFC 3411], [RFC 3412], [RFC 3413], [RFC 3414], [RFC 3415], and [RFC 2576].
- docsDevNmAccessTable is not accessible.
- Access control and trap destinations are determined by the snmpCommunityTable, Notification MIB, Target MIB, VACM-MIB, and USM-MIB. The PS MUST enforce the management access policy, as defined by the VACM View configured by the cable operator, for any access to the CableHome-specified MIB objects, regardless of the interface (such as a vendor specific graphical user interface (GUI)) or access protocol used.[12]
- Community MIB controls the translation of SNMPv1/v2c packet community string into security name which select entries in the USM MIB. Access control is provided by the VACM MIB.
- USM MIB and VACM MIB controls SNMPv3 packets.
- Trap destinations are specified in the Target MIB and Notification MIB.

In case of failure to complete SNMPv3 initialization for a User (i.e., NMS cannot access the PS via SNMPv3 PDU), the USM User Table for that User MUST be deleted, the PS is in Coexistence Mode, and the PS will allow SNMPv1/v2c access if and only if the community MIB entries (and related entries) are configured.

6.3.3.1.4.3 Network Management Mode for a PS Operating in SNMP Provisioning Mode

If the PS is operating in SNMP Provisioning Mode following DHCP ACK (as indicated by a value '2' (SNMPmode) for cabhPsDevProvMode), it operates in SNMPv3 Coexistence Mode using SNMPv3 by default for exchanging management messages with the NMS, and uses Kerberos for exchanging key material with the KDC, following rules described in this section. Just as when the PS is operating in DHCP Provisioning Mode and has been configured for SNMPv3 Coexistence network management mode, when the PS is operating in SNMP Provisioning Mode and SNMPv3 Coexistence network management mode it is required to ignore attempts to configure the docsDevNmAccessTable.

6.3.3.1.4.4 Management Views

The management controls defined for CableHome are in the CMP function of the PS. Settings, based on management mode, define the access rights that are granted to a User for access to the Portal Services

[12] Revised this bullet statement per ECN CH1.1-N-03.0090-2 by GO on 12/5/03.

EXHIBIT A

database, through CableHome-specified MIBs, via SNMP from the PS WAN-Man or LAN Server Router interfaces. A single User is defined by the CableHome 1.1 specification.

The concept of Management Views was introduced with SNMPv3, and is defined in [RFC 3410] through [RFC 3415] and [RFC 2576]. It is a method for specifying what user(s) is/are allowed to access which MIB object(s).

Figure 6-4 illustrates some possible management Views for the PS. A WAN Administrator View (CHAdministrator view) and a WAN Administrator User (CHAdministrator user) are defined by CableHome 1.1. Other Views and Users, such as the WAN Maintenance View, the LAN Administrator View, or the LAN User View can be established by the Ultimate Authorization (CHAdministrator), following rules defined in [RFC 3414] and [RFC 3415].

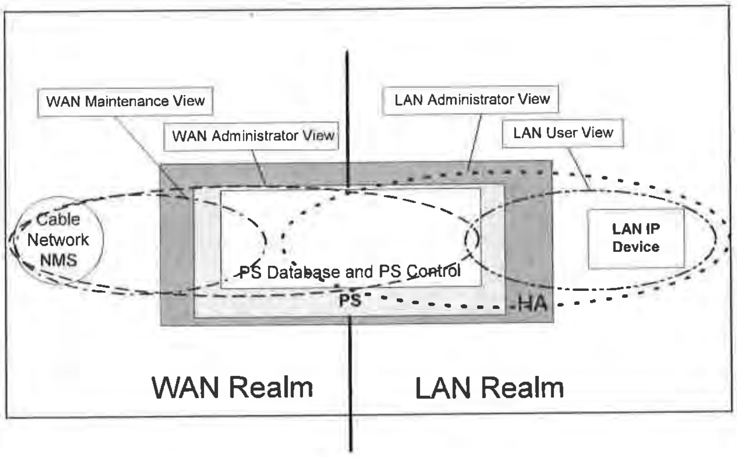


Figure 6-4 — Management Views

Managed parameters defined by CableHome are stored in the PS Database. As shown in Figure 6-4, there is a concept of Access Views into the PS Database and PS Control, which allows simultaneous management from both the LAN and WAN by defining Management Views into the PS Database and PS Control. The Views are a mechanism to provide privacy and security, and the policy can be set separately by the CHAdministrator User.

The Ultimate Authorization (CHAdministrator User) has its own User ID and keys, and has the following responsibilities:

- Responsible for setting up all access Views on both the LAN and WAN management interface.
- Responsible for creating and managing all User profiles including user IDs, Keys, and PS database access privileges.
- Responsible for setting policy for both LAN and WAN side access.

Descriptions for how View-based Access Control Model and User-based Security Model work are provided in [RFC 3414] and [RFC 3415].

The CHAdministrator View provides full read and write access to all MIBs specified by CableHome.

EXHIBIT A

Management View requirements are specified in Section 6.3.3.1.4.5 of this specification.

6.3.3.1.4.4.1 WAN-Access Control

CableHome defines two methods for controlling access to manageable parameters via CableHome-defined MIBs. The docsDevNmAccessTable [RFC 2669] defines management access when the PS is operating in NmAccess Network Management Mode (refer to Section 6.3.3.1.4.2.2). When the PS is operating in SNMPv3 Coexistence Network Management Mode (Section 6.3.3.1.4.2.2), per User Security Model (USM) [RFC 3414] and View-based Access Control Model (VACM) [RFC 3415], Table settings are used to control access to CableHome-specified MIB objects, regardless of the interface (such as a graphical user interface) through which the request arrives. VACM defines a set of services that can be used for checking access rights. VACM Groups define the rights to access the CMP.[13]

As defined in [RFC 3415] section 2.4, a "MIB View" is a specific set of managed object types that can be defined, and this concept is used in CableHome to support WAN Management of the PS. The CHAdministrator User access and View for CableHome 1.1 are specified in Section 11.4.4.1.3 and Section 6.3.3.1.4.5. An example sequence of PS Database access from the WAN interface is provided in Section 12.3.1.

6.3.3.1.4.4.2 Security

Security of management messages is provided by SNMPv3. Refer to Section 11 for a detailed description of how SNMPv3 is used. The CMP may use SNMP v3 to counter threats identified in Appendix III.

To protect against replay attacks, a time of day clock is utilized to provide timestamps for messaging. Management messaging security requirements are specified in Section 11.4.

6.3.3.1.4.5 View-based Access Control Model (VACM) Requirements

To provide controlled access to management information and the creation of distinct management realms for a PS operating in SNMP v3 Coexistence Mode, View-based Access Control Model (VACM) MUST be employed as defined by [RFC 3415].

The WAN Administrator View MUST be implemented in a CableHome 1.1-compliant Portal Services element. Default Views other than the WAN Administrator View MUST NOT be available on the PS. Other Views MAY be created by the Ultimate Authorization through the cable network NMS by configuring the VACM MIB.

The User specification for the WAN Administrator View MUST be implemented as follows:

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

The Group specification for the CHAdministrator View MUST be implemented as follows:

[13] Revised this paragraph per ECN CH1.1-N-03.0090-2 by GO on 12/5/03.

EXHIBIT A

CHAdministrator Group

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

The VACM View for the CHAdministrator view MUST be implemented as follows:

CHAdministratorView subtree 1.3.6.1 (Entire MIB)

6.3.3.1.4.6 Mapping TLV Fields Into Created SNMPv3 Table Rows

This section details how the *SNMP Notification Receiver* Configuration File Element (TLV Type 38) is mapped into SNMPv3 functional tables. Refer to Section 7.4.4.1.10 SNMP Notification Receiver for a description of configuration parameter TLV Type 38. Details of how the encryption keys are exchanged for SNMP v3 operation are provided in Section 11.4.4.2.2.

Upon receiving one Type 38 configuration file element, the PS MUST make MIB table entries following the procedure described in Table 6-6 snmpNotifyTable through Table 6-15 vacmSecurityToGroupTable, using values passed in the TLV as described below. The MIB tables the PS is required to populate when it receives a Type 38 configuration file element are listed below for convenience:

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

A PS configuration file is allowed to contain TLV MIB elements (Type 28) that make entries to any of the 11 tables listed above.

EXHIBIT A

The tables in this section show how the fields from the PS Configuration file TLV element (the tags in angle brackets <>) are placed into the SNMP V3 tables.

The correspondence between TLV fields and table tags <TAG> is shown below:

PS<IP Address> TLV 38.1

<Port> - TLV 38.2

<Trap type> TLV 38.3

<Timeout> TLV 38.4

<Retries> TLV 38.5

<Filter OID> TLV 38.6

<Security Name> TLV 38.7

These tables are shown in the order that the agent will search down through them when a notification is generated in order to determine who to send the notification to and how to fill out the contents of the notification packet.

snmpNotifyTable

Create two rows with fixed values, if one or more TLV elements are present.

Table 6-6 — snmpNotifyTable

snmpNotifyTable [RFC 3413] **SNMP-NOTIFICATION-MIB**	**First Row**	**Second Row**
Column Name (* = Part of Index)	Column Value	Column Value
* snmpNotifyName	"@PSconfig_inform"	"@PSconfig_trap"
snmpNotifyTag	"@PSconfig_inform"	"@PSconfig_trap"
snmpNotifyType	inform(2)	trap(1)
snmpNotifyStorageType	volatile	volatile
snmpNotifyRowStatus	Active(1)	Active(1)

snmpTargetAddrTable

Create one row for each TLV element in the PS configuration file. snmpTargetAddrExtTable

Table 6-7 — snmpTargetAddrTable

snmpTargetAddrTable [RFC 3413] **SNMP-TARGET-MIB**	**New Row**
Column Name (* = Part of Index)	Column Value
* snmpTargetAddrName	"@PSconfig_n", where n ranges from 0 to m-1, and m is the number of notification receiver TLV elements in the PS configuration file
snmpTargetAddrTDomain	snmpUDPDomain – snmpDomains

EXHIBIT A

snmpTargetAddrTable [RFC 3413] SNMP-TARGET-MIB	New Row
snmpTargetAddrTAddress (IP Address and UDP Port of the Notification Receiver)	OCTET STRING (6) Octets 1 – 4: <IP Address> Octets 5 – 6: <Port>
snmpTargetAddrTimeout	<Timeout> from the TLV
snmpTargetAddrRetryCount	<Retries> from the TLV
snmpTargetAddrTagList	If <Trap type> == 1,2, or 4 "@PSconfig_trap" Else If <Trap type> = 3 or 5 "@PSconfig_inform"
snmpTargetAddrParams	"@PSconfig_n" (same as snmpTargetAddrName value)
snmpTargetAddrStorageType	volatile
snmpTargetAddrRowStatus	active(1)

Create one row for each TLV element in the PS configuration file.

Table 6-8 — snmpTargetAddrExtTable

snmpTargetAddrExtTable [RFC 2576] SNMP-COMMUNITY MIB	New Row
Column Name (* = part of index)	Column Value
* snmpTargetAddrName	"@PSconfig_n", where n ranges from 0 to m – 1, and m is the number of notification receiver TLV elements in the PS configuration file
snmpTargetAddrMask	<zero length octet string>
snmpTargetAddrMMS	0

snmpTargetParamsTable

Create 1 row for each TLV element in the config file. If <Trap type> is 1, 2, or 3, or if the <Security Name> Field is zero-length, create the table as follows:

Table 6-9 — snmpTargetParamsTable for <Trap Type> 1, 2, or 3

snmpTargetParamsTable [RFC 3413] SNMP-TARGET-MIB	New Row
Column Name (* = part of index)	Column Value
* snmpTargetParamsName	"@PSconfig_n", where n ranges from 0 to m – 1, and m is the number of notification receiver TLV elements in the PS configuration file

snmpTargetParamsMPModel
SYNTAX:
SnmpMessageProcessingModel
	If <Trap type> = 1
	SNMPv1(0)
	Else if <Trap type> = 2 or 3
	SNMPv2c(1)
	Else if <Trap type> = 4 or 5
	SNMPv3(3)

EXHIBIT A

snmpTargetParamsTable [RFC 3413] SNMP-TARGET-MIB	New Row
snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	If <Trap type> = 1 SNMPv1(1) Else if <Trap type> = 2 or 3 SNMPv2c(2) Else if <Trap type> = 4 or 5 USM(3) **NOTE: The mapping of SNMP protocol types to value here are different from snmpTargetParamsMPModel**
snmpTargetParamsSecurityName	"@PSconfig"
snmpTargetParamsSecurityLevel	noAuthNoPriv
snmpTargetParamsStorageType	volatile
snmpTargetParamsRowStatus	active(1)

If <Trap type> is 4 or 5, and the <Security Name> field is non-zero length, create the table as follows:[14]

Table 6-10 — snmpTargetParamsTable for <Trap Type> 4 or 5

snmpTargetParamsTable [RFC 3413] SNMP-TARGET-MIB	New Row
Column Name (* = part of index)	Column Value
* snmpTargetParamsName	"@PSconfig_n", where n ranges from 0 to m – 1, and m is the number of notification receiver TLV elements in the PS configuration file

snmpTargetParamsMPModel
SYNTAX:
SnmpMessageProcessingModel
	If <Trap type> = 1
	SNMPv1(0)
	Else if <Trap type> = 2 or 3
	SNMPv2c(1)
	Else if <Trap type> = 4 or 5
	SNMPv3(3)

snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	If <Trap type> = 1 SNMPv1(1) Else if <Trap type> = 2 or 3 SNMPv2c(2) Else if <Trap type> = 4 or 5 USM(3) NOTE: The mapping of SNMP protocol types to value here are different from snmpTargetParamsMPModel
snmpTargetParamsSecurityName	<Security Name>
snmpTargetParamsSecurityLevel	The security level of <Security Name>
snmpTargetParamsStorageType	volatile
snmpTargetParamsRowStatus	active(1)

snmpNotifyFilterProfileTable

[14] Revised this sentence per ECN CH1.1-N-03.0090-2 by GO on 12/5/03.

EXHIBIT A

Create one row for each TLV that has a non-zero <Filter Length>.

Table 6-11 — snmpNotifyFilterProfileTable

snmpNotifyFilterProfileTable [RFC 3413] **SNMP-NOTIFICATION-MIB**	**New Row**
Column Name (* = Part of Index)	Column Value
*snmpTargetParamsName	"@PSconfig_n", where n ranges from 0 to m-1 and m is the number of notification receiver TLV elements in the PS configuration file.
snmpNotifyFilterProfileName	"@PSconfig_n", where n ranges from 0 to m-1 and m is the number of notification receiver TLV elements in the PS configuration file
snmpNotifyFilterProfileStorType	volatile
snmpNotifyFilterProfileRowStatus	active(1)

snmpNotifyFilterTable

Create one row for each TLV that has a non-zero <Filter Length>.

Table 6-12 — snmpNotifyFilterTable

snmpNotifyFilterTable [RFC 3413] **SNMP-NOTIFICATION-MIB**	**New Row**
Column Name (* = Part of Index)	Column Value
* snmpNotifyFilterProfileName	"@PSconfig_n" , where n ranges from 0 to m-1 and m is the number of notification receiver TLV elements in the PS configuration file.
* snmpNotifyFilterSubtree	<Filter OID> from the TLV
snmpNotifyFilterMask	<Zero Length Octet String>
snmpNotifyFilterType	included(1)
snmpNotifyFilterStorageType	volatile
snmpNotifyFilterRowStatus	active(1)

snmpCommunityTable

Create one row with fixed values if 1 or more TLV's are present. This causes SNMPV1 and V2c Notifications to contain the community string in snmpCommunityName.

Table 6-13 — snmpCommunityTable

snmpCommunityTable [RFC 2576] **SNMP-COMMUNITY-MIB**	**First Row**
Column Name (* = Part of Index)	Column Value
* snmpCommunityIndex	"@PSconfig"
snmpCommunityName	"public"
snmpCommunitySecurityName	"@PSconfig"
snmpCommunityContextEngineID"	<The PS engineID>
snmpCommunityContextName	<Zero length octet string>
snmpCommunityTransportTag	<Zero length octet string>
snmpCommunityStorageType	volatile
snmpCommunityStatus	active(1)

EXHIBIT A

usmUserTable

Create one row with fixed values, if one or more TLVs are present. Other rows are created, one each time the engine ID of a trap receiver is discovered. This specifies the user name on the remote notification receivers to send notifications to.

One row in the usmUserTable is created. Then when the engine ID of each notification receiver is discovered, the agent copies this row into a new row and replaces the 0x00 in the usmUserEngineID column with the newly discovered value.

Table 6-14 — usmUserTable

usmUserTable [RFC 3414] **SNMP-USER-BASED-SM-MIB**	**First Row**
Column Name (* = Part of Index)	Column Value
* usmUserEngineID	0
* usmUserName	"@PSconfig" When other rows are created, this is replaced with the <Security Name> field from the TLVelement.
usmUserSecurityName	"@PSconfig" When other rows are created, this is replaced with the <Security Name> field from the TLVelement.
usmUserCloneFrom	<don't care> - cannot clone this row
usmUserAuthProtocol	None. When other rows are created, this is replaced with None or MD5, depending upon the security level of the v3 User.
usmUserAuthKeyChange	<don't care> - write only
usmUserOwnAuthKeyChange	<don't care> - write only
usmUserPrivProtocol	None. When other rows are created, this is replaced with None or DES, depending on the security level of the v3 User
usmUserPrivKeyChange	<don't care> - write only
usmUserOwnPrivKeyChange	<don't care> - write only
usmUserPublic	<zero length string>
usmUserStorageType	volatile
usmUserStatus	active(1)

vacmSecurityToGroupTable

Create three rows with fixed values, if one or more TLVs are present.

These are the three rows with fixed values, which are used for the TLV entries with <Trap Type> set to 1, 2, or 3 or with a zero length <Security Name>.

Table 6-15 — vacmSecurityToGroupTable

vacmSecurityToGroupTable **[RFC 3415]** **SNMP-VIEW-BASED-ACM-MIB**	**First Row**	**Second Row**	**Third Row**
Column Name (* = Part of Index)	Column Value	Column Value	Column Value

EXHIBIT A

vacmSecurityToGroupTable [RFC 3415] SNMP-VIEW-BASED-ACM-MIB	First Row	Second Row	Third Row
* vacmSecurityModel	SNMPv1(1)	SNMPv2c(2)	USM(3)
* vacmSecurityName	"@PSconfig"	"@PSconfig"	"@PSconfig"
vacmGroupName	"@PSconfigv1"	"@PSconfigv2"	"@PSconfigUSM"
vacmSecurityToGroupStorageType	volatile	volatile	volatile
vacmSecurityToGroupStatus	active(1)	active(1)	active(1)

6.3.3.1.4.7 CableHome MIB Requirements

The PS MUST implement each MIB object listed in Appendix I. If the Persistent column for a MIB object listed in Appendix I contains the value Yes, the PS MUST retain the value of the object across a PS power cycle or re-boot, making the same value available for access by an SNMP manager immediately after provisioning complete (cabhPsDevProvState = pass(1)), following a re-boot that was available for access by that SNMP manager immediately before re-boot.

Required MIB objects are from the following MIB documents:

- Interfaces Group MIB [RFC 2863]
- DOCSIS Cable Device MIB [RFC 2669]
- CableLabs Definition MIB [CableLabs2]
- CableHome PSDev MIB [CH5]
- CableHome CAP MIB [CH2]
- CableHome CDP MIB [CH3]
- CableHome CTP MIB [CH4]
- CableHome Security MIB [CH1]
- CableHome QoS MIB [CH7]
- [draft-ietf-ipcdn-bpiplus-mib-05]
- IP MIB (SNMPv2) [RFC 2011]
- UDP MIB (SNMPv2) [RFC 2013]
- Diffie-Hellman USM Key [RFC 2786]
- INET Address MIB [RFC 3291]
- DOCS IF MIB [RFC 2670]
- IANA ifType MIB [IANAType]

In a CableHome Residential Gateway or any other device with an embedded PS and embedded cable modem, the cable modem management entity and PS management entity (CMP) MUST respond to different and independent management IP addresses. DOCSIS and CableHome specify some of the same MIB objects but if a DOCSIS-compliant cable modem and a CableHome-compliant PS Element are embedded in the same device, each is required to maintain its own, separate instance of specified MIB objects, accessible through different management IP addresses, with the exception of the SNMP group of MIB 2 and SNMPv2 MIB, which MAY be common to and shared between the cable modem and the Portal Services Element, and MAY be accessible through either the cable modem management IP address or the PS management IP address.

In a PS with an embedded cable modem, software download of the single image of the combined cable modem software and Portal Services software, is controlled by the cable modem. The following

EXHIBIT A

docsDevSoftware group objects [RFC 2669] MUST NOT be implemented for a PS with an embedded cable modem, i.e., these objects MUST only be accessible through the cable modem management IP address in a PS with an embedded CM:

- docsDevSwServer
- docsDevSwFilename
- docsDevSwAdminStatus
- docsDevSwOperStatus

The docsDevSoftware Group of objects MUST be implemented in a Standalone PS. Modification of the docsDevSoftware objects (as specified in Section 11.8.4) by the cable operator for the purpose of downloading the standalone PS software image MUST result in proper secure software download operation.

In a PS with an embedded cable modem, cable modem MIB objects MUST only be visible and accessible when the manager accesses them through the cable modem management IP address, and MUST NOT be visible or accessible via any PS management IP address, with the exception of the SNMP group of MIB 2 and the SNMPv2 MIB which are allowed to be shared between the CM and PS management entities.

In a PS with an embedded cable modem, CableHome-specified MIB objects MUST only be visible and accessible when the manager accesses them through the PS management IP address (PS WAN-Man IP address) or through the PS LAN Server Router IP address, and MUST NOT be visible or accessible via the cable modem management IP address, with the exception of the SNMP group of MIB 2 and the SNMPv2 MIB which are allowed to be shared between the CM and PS management entities.

The general CableHome MIB hierarchy is illustrated in Figure 6-5. Specific OIDs required for individual MIBs are listed in Appendix I.

EXHIBIT A

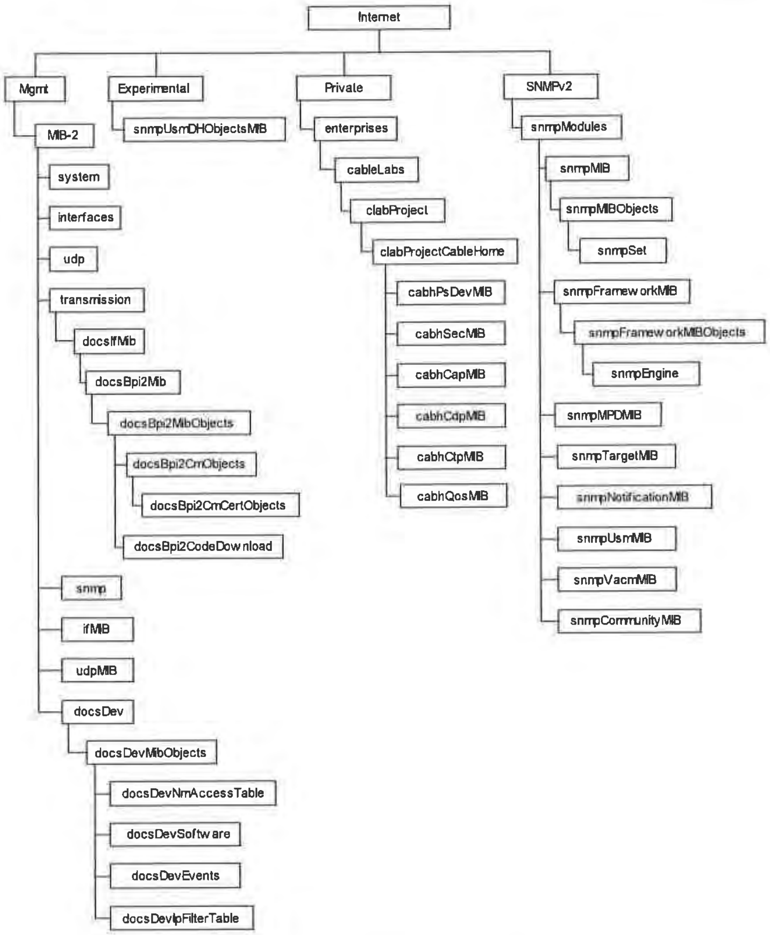


Figure 6-5 — CableHome MIB Hierarchy

6.3.3.1.4.8 Interfaces Group MIB

The Interfaces Group MIB [RFC 2863] provides a powerful tool to allow cable operators to understand the state of and see statistics for all of the physical interfaces on the Portal Service element. A *physical interface* is one for which a connector is exposed on the exterior of the device enclosure, and for which the object *ifConnectorPresent* is true. In order to enable the intelligent use of this MIB, an interface numbering scheme is essential. Therefore PS elements need to comply to the following requirements:

EXHIBIT A

An instance of ifEntry MUST exist for the WAN-Data interface of the PS element, even if that interface is internal - as exists in the case of an Embedded PS utilizing an integrated chip design.

An instance of ifEntry MUST exist for each physical LAN interface of the PS element.

An instance of ifEntry MUST exist for an "Aggregated LAN Interfaces" interface, which is identified by the ifIndex value 255.

The PS ifTable interfaces MUST be numbered as shown in Table 6-16.

Table 6-16 – Numbering Interfaces in the ifTable

Interface	Description
1	WAN-Man Interface
2	WAN-Data Interface
2+n	Each LAN Interface
255	Aggregated LAN Interface

If a given interface's ifAdminStatus = down, that interface MUST NOT accept or forward any traffic. The ifAdminStatus object corresponding to ifIndex value 255 MUST provide administrative control over all LAN interfaces and MUST be implemented as read-write.

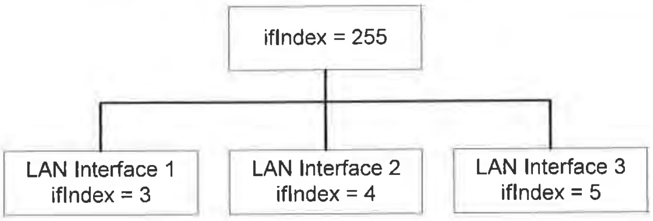
The PS MUST assign the value other(1) to ifTable [RFC 2233] ifType entries corresponding to ifIndex 255. An embedded PS element MUST assign the value other(1) to ifTable ifType entries corresponding to ifIndex values 1 and 2. A standalone PS element MUST assign the appropriate IANAifType [IANAType] value to the ifTable ifType value corresponding ifIndex values 1 and 2.

The ifTable ifPhysAddress value corresponding to ifIndex 255 MUST be a zero length octet string.

The ifTable counters of WAN interfaces of ifIndex values 1 and 2 MUST be shared between the two interfaces. The ifTable counters for ifIndex value 255 MAY be implemented.

The Interface Stack (ifStack) group of [RFC 2233] MUST be implemented to identify relationships among the higher-layer "Aggregated LAN Interfaces" interface and the lower-layer LAN sub-interfaces. Figure 6-6 illustrates the use of the ifStack group for a PS with three LAN interfaces.

EXHIBIT A



Implementation of ifStack for this example:

ifStackHigherLayer	ifStackLowerLayer
255	3
255	4
255	5

Figure 6-6 — ifStack Implementation Example

6.3.3.1.4.9 ipNetToMediaTable Requirements[15]

The ipNetToMediaTable [RFC 2011] maps IP addresses to physical addresses, and its use is straightforward if each IP address is associated to one physical interface, and if each physical interface is associated to one physical address. The PS, however, implements different IP addresses that may apply to several physical interfaces, and associates the physical WAN interface to two hardware addresses. The PS also implements different Primary Packet-handling Modes, which also has an affect on the ipNetToMediaTable. The PS MUST list in the ipNetToMediaTable, each of the IP addresses that are part of its active configuration, creating one entry per distinct IP value and abiding by Table 6-17 for NAPT and NAT Primary Packet-handling Modes (including Mixed Mode), and abiding by Table 6-18 for Passthrough Primary Packet-handling Mode.

Table 6-17 — PS Static Entries in the ipNetToMediaTable for NAPT, NAT, & Mixed Modes

ipNetToMediaAddress	ipNetToMediaPhysAddress	ipNetToMediaIfIndex	ipNetToMediaType
WAN-Man IP Address	WAN-Man hardware address	1	static(4)
1st WAN-Data IP Address	WAN-Data hardware address	2	static(4)
2 nd WAN-Data IP Address	WAN-Data hardware address	2	static(4)
N th WAN-Data IP Address	WAN-Data hardware address	2	static(4)
CDP Server Router IP Address	Zero length octet string	255	static(4)
Well Known PS LAN IP Address (if different from ServerRouter IP)	Zero length octet string	255	static(4)

Table 6-18 — PS Static Entries in the ipNetToMediaTable for Passthrough Mode

ipNetToMediaAddress	ipNetToMediaPhysAddress	ipNetToMediaIfIndex	ipNetToMediaType
WAN-Man IP Address	WAN-Man hardware address	1	static(4)
Well Known PS LAN IP Address	Zero length octet string	255	static(4)

[15] Revised this section per ECN CH1.1-N-03.0077-4 by GO on 12/2/03.

EXHIBIT A

The PS element MUST dynamically learn the IP and hardware addresses of OSI Layer 3 devices off each of its active physical LAN interfaces and each of its active WAN interfaces. IP and hardware addresses learned by the PS element, along with the appropriate PS ifIndex numbers and ipNetToMediaType information, MUST be accessible to the NMS system (through the CMP) via the [RFC 2011] ipNetToMediaTable. All dynamically learned entries in the ipNetToMediaTable MUST have an ipNetToMediaType value of dynamic(3).

A row entry for the PS's CM MUST NOT appear in the PS's ipNetToMediaTable since the CM acts as a transparent bridge from the perspective of the PS.

As a result of completing the PS provisioning process, the PS MUST create a row entry in its ipNetToMediaTable representing the next hop router for the WAN-Man interface, with an ifIndex value of 1, ipNetToMediaPhysAddress & ipNetToMediaNetAddress values specific to that router, and a ipNetToMediaType value of dynamic(3). If the PS has an active WAN-Data interface, the PS MUST create a row entry in its ipNetToMediaTable representing the next hop router for the WAN-Data interface, with an ifIndex value of 2, ipNetToMediaPhysAddress & ipNetToMediaNetAddress values specific to that router, and an ipNetToMediaType value of dynamic(3).

The PS element MUST delete entries from its ipNetToMediaTable that have an ipNetToMediaType value of dynamic(3) when an implementation-specific inactivity timeout expires.

6.3.3.2 CMP Event Reporting Function

The CMP is required to support the handling and reporting of events generated by the PS, for the WAN Domain. Event messages defined by CableHome for the PS element can be reported via SNMP Trap to the cable operator's notification receiver, via a System Log message sent to the cable operator's system log, or via a log local to the PS and accessible through CableHome-specified MIB objects. Events defined for the PS are listed in Appendix II Format and Content for Event, SYSLOG, and SNMP Trap. These are the same processes defined in DOCSIS specifications for event reporting in cable modems.

CableHome Host devices are not required to support event messaging. Therefore, LAN Domain event messaging is not defined by CableHome 1.1 specifications.

Event Reporting for the WAN Domain

CableHome uses the [RFC 2669] event reporting and control mechanisms for events generated in the PS (CMP). [RFC 2669] defines a standard format for reporting event information, regardless of the message type, including a local event log table in which certain entries will persist across reboot of the PS. Note that events may be generated by any part of a PS, but the CMP logs and/or reports the event either locally or to a Syslog or Trap server.

6.3.3.2.1 Event Reporting Function Goals

The goals of the CMP Event Reporting function are listed below:

- enable the transfer of unsolicited messages from the PS to the NMS across the WAN in the form of SNMP Traps and SYSLOG messages
- enable the logging of status and exception information in the PS Database (local log)
- enable access to local log status and exception information via MIB objects
- maintain compatibility with event reporting as defined in DOCSIS specifications

6.3.3.2.2 Event Reporting Function System Design Guidelines

The system design guidelines listed in Table 6-19 guided specification of the CMP Event Reporting Function.

EXHIBIT A

Table 6-19 — CMP Event Reporting Function System Design Guidelines

Reference	Event Reporting Function System Design Guidelines
EvRep 1	The PS will support the reporting of status and exception information as SNMP Notifications, SYSLOG messages, and volatile and non-volatile local log messages.
EvRep 2	The PS will support configurable event throttles and limits.
EvRep 3	The PS will support configurable event priorities.

6.3.3.2.3 Event Reporting Function System Description

Event reporting is a means for an element to report on status or an error condition in an unsolicited message. CableHome supports four types of event reporting:

1. SNMP notify or trap
2. SYSLOG messaging
3. Non-volatile local log
4. Volatile local log

CableHome requires the use of the DOCSIS Device MIB [RFC 2669] to configure the PS for where to send SNMP traps (notifications) and SYSLOG messages and for event inhibiting and throttling values. Event notification by the PS is fully configurable. The CableHome specification defines where the PS is to report events assigned a particular priority (ref.: Table 6-20) and the DOCSIS Device MIB allows the priority of each event to be configured. The DOCSIS Device MIB also maintains statistics for the occurrence of each event. The Event Table (docsDevEventTable) in the DOCSIS Device MIB includes an entry for each unique event reported by the PS, a count for the number of occurrences for each unique event entry, and the time at which the last entry was made for each event entry.

CableHome defines the procedure for re-indexing the Event Table in the event that the PS is re-initialized such that volatile local log entries are lost. When volatile local log entries are lost the PS is required to re-index the Event Table such that the remaining (volatile) local log entries are sequentially indexed.

6.3.3.2.4 Event Reporting Function Requirements

PS requirements for CMP Event Reporting Function are specified in Sections 6.3.3.2.4.1 - 6.3.3.2.4.9.

6.3.3.2.4.1 Event Notification

The PS MUST generate asynchronous events that indicate important events and situations as specified (refer to Appendix II). Events can be stored in an internal event LOG, stored in non-volatile memory, reported to other SNMP entities (as TRAP or INFORM SNMP messages), or sent as a SYSLOG event message to the SYSLOG server whose IP address is passed in DHCP Option 7 of the DHCP OFFER received from the Headend DHCP server through the PS WAN-Man Interface.

The PS MUST support the following event notification mechanisms:

- local event logging where certain entries in the local log can be identified to persist across a reboot of the PS
- SNMP TRAP and INFORM
- SYSLOG

EXHIBIT A

The PS MUST implement the docsDevEvControlTable from [RFC 2669] to control reporting of events. The following BITs values for the [RFC 2669] object docsDevEvReporting MUST be supported by the PS:

- local-nonvolatile(0)
- traps(1)
- syslog(2)
- local-volatile(3)

SNMP SET request messages to the [RFC 2669] object docsDevEvReporting using the following values MUST result in a 'Wrong Value' error for SNMP PDUs:

- 0x20 = syslog only
- 0x40 = trap only
- 0x60 = (trap + syslog) only

An event reported by Trap, Syslog, or Inform MUST also generate a local log entry, whether volatile or non-volatile according to Table 6-20, and as described in Section 6.3.3.2.4.2.

6.3.3.2.4.2 Local Event Logging

The PS MUST maintain a single local-log event table that contains events stored as both local-volatile events and local-nonvolatile events. Events stored as local-nonvolatile events MUST persist across reboots of the PS. The local-log event-table MUST be organized as a cyclic buffer with a minimum of ten entries. The single local-log event-table MUST be accessible through the docsDevEventTable as defined in [RFC 2669].

Event descriptions MUST appear in English. Event descriptions MUST NOT be longer than 255 bytes, which is the maximum defined for SnmpAdminString.

The EventId is a 32 bit unsigned integer. EventIds ranging from 0 to ((2^31) - 1) are reserved by CableHome. The EventId MUST be converted from the error codes defined in Appendix II. The EventIds ranging from 2^31 to ((2^32)-1) MUST be used as vendor specific EventIds using the following format:

- Bit 31 set to indicate vendor specific event
- Bits 30-16 contain bottom 15 bits of vendor's SNMP enterprise number
- Bits 15-0 used by vendor to number their events

The [RFC 2669] object docsDevEvIndex provides for relative ordering of events in the log. The tagging of local log events as local-volatile and local-nonvolatile necessitates a method for synchronizing docsDevEvIndex values between the two types of events after a PS reboot. After a PS reboot, to synchronize the docsDevEvIndex values for volatile and non-volatile events, the following procedure MUST be used:

- The values of docsDevEvIndex for local log events tagged as local-nonvolatile MUST be renumbered beginning with 1.
- The local log MUST then be initialized with the events tagged as local-nonvolatile in the same order as they had been immediately prior to the reboot.
- Subsequent events recorded in the local log, whether tagged as local-volatile or local-nonvolatile, MUST use incrementing values of docsDevEvIndex.

A reset of the local log initiated through an SNMP SET of [RFC 2669] object docsDevEvControl MUST clear all events from the local log, including log events tagged as both local-volatile and local-nonvolatile.

EXHIBIT A

6.3.3.2.4.3 SNMP TRAP and INFORM

The PS MUST support the SNMP Trap PDU as described in [RFC 3411]. The PS MUST support the SNMP INFORM PDU as described in [RFC 3411]. INFORM is a variation of trap and requires the receiving host to acknowledge the arrival of an InformRequest-PDU with an InformResponse-PDU.

When a standard CableHome SNMP trap is enabled in the PS, it MUST send notifications for any event in that category whose priority is either "error" or "notice".

The PS MAY support vendor-specific events. If supported, vendor-specific PS events reportable via SNMP TRAP MUST be described in a private MIB that is distributed with the PS. When defining a vendor-specific SNMP trap, the OBJECTS statement of the private trap definition SHOULD contain at least the objects explained below:

- EvLevel
- EvIdText
- Event Threshold (if any for the trap)
- IfPhysAddress (the physical address associated with the WAN-Man IP address of the PS)

More objects can be contained in the OBJECTS statement as desired.

6.3.3.2.4.4 Syslog

SYSLOG messages issued by the PS MUST be in the following format:

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

Where:

Level - ASCII presentation of the event priority, enclosed in angle brackets, which is constructed as the bitwise of the default Facility (128) and event priority (0-7). The resulted level has the range between 128 and 135.

vendor - Vendor name for the vendor-specific SYSLOG messages or "CABLEHOME" for the standard CableHome messages.

EventId - ASCII presentation of the INTEGER number in decimal format, enclosed in angle brackets, that uniquely identifies the type of event. This EventID MUST be the same number that is stored in docsDevEvId object in docsDevEventTable. For the standard CableHome events, this number is converted from the error code using the following rules:

- The number is an eight digit decimal number.
- The first two digits (left most) are the ASCII code (decimal) for the letter in the Error code.
- The next four digits are filled by 2 or 3 digits between the letter and the dot in the Error code with zero filling in the zap in the left side.
- The last two digits are filled by the number after the dot in the Error code with zero filling in the zap in the left.

For example, event D04.2 is converted into 68000402, and Event I114.1 is converted into 73011401.

Please note that this notion only uses a small portion of available number space reserved for CableHome (0 to 2^31-1). The first letter of an error code is always in upper case.

EXHIBIT A

text - for the standard CableHome messages, this string MUST have the textual description as defined in Appendix II of this specification

The example of the syslog event for the event D04.2: "Time of the day received in invalid format":

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

The number 68000402 in the given example is the number assigned by CableHome to this particular event.

6.3.3.2.4.5 Format of Events

The CableHome Management Event messages MAY contain any of the following information:

- Event Counter - indicator of event sequence
- Event Time - time of occurrence
- Event Priority - severity of condition. [RFC 2669] defines eight levels of severity. The default event severity can be changed to a different value for each given event via the SNMP interface.
- Event Enterprise Number - This number identifies the event as either a standard event or a vendor-defined event.
- Event ID - identifies the exact event when combined with the Event Enterprise Number. Vendors define their own Event ID's. CableHome standard management events are defined in Appendix II. Each management event described in the appendix is assigned a CableHome Event ID.
- Event Text - describes the event in human readable form
- PS WAN-Man-MAC address - describes the MAC address of the PS Element used for management of the box
- PS WAN-Data-MAC address - describes the MAC address of the PS Element optionally used for data

The exact format of this information for traps and informs is defined in Appendix II. The format for SYSLOG messages is defined in the requirements portion of this subsection.

6.3.3.2.4.6 Event Priorities

[RFC 2669] document defines 8 different priority levels and the corresponding reporting mechanism for each level. The standard CableHome events specified in this document utilize these priority levels.

Emergency event (priority 1)

> Reserved for vendor-specific 'fatal' hardware or software errors that prevent normal system operation and cause the reporting system to reboot. Each vendor may define its own set of emergency events. Examples of such events could be 'no memory buffers available', 'memory test failure' etc.

Alert event (priority 2)

> A serious failure which causes the reporting system to reboot but the reboot is not caused by either hardware or software malfunctioning. After recovering from the event, the system MUST send the cold/ warm start notification.

Critical event (priority 3)

> A serious failure that prevents the device from transmitting data but could be recovered without rebooting the system. After recovering from a Critical event, the PS MUST send the Link Up

EXHIBIT A

notification. Examples of such events could be PS Configuration File problems or the inability to get an IP address through DHCP.

Error event (priority 4)

A failure that could interrupt the normal data flow but does not cause device to reboot. Error events can be reported in real time by using either the TRAP or SYSLOG mechanism.

Warning event (priority 5)

A failure that could interrupt the normal data flow. Syslog and Trap reporting are enabled by default for this level.

Notice event (priority 6)

An event of importance that is not a failure and could be reported in real time by using either the TRAP or SYSLOG mechanism. Examples of the NOTICE events are 'Cold Start', 'Warm Start', 'Link Up' and 'SW upgrade successful'.

Informational event (priority 7)

An event of importance that is not a failure, but which could be helpful for tracing the normal operation of the device.

Debug event (priority 8)

Reserved for vendor-specific non-critical events

The priority associated with CableHome standard events MUST NOT be changed.

Table 6-20 shows the default notification types for the various event priorities. The PS MUST implement the default notification types as defined in Table 6-20 Default Notification Types for PS Event Priorities, for the eight event priorities. For example, the default notification type for Emergency and Alert events is to place them in the local-log as nonvolatile entries.[16]

Table 6-20 — Default Notification Types for PS Event Priorities

Event Priority	Local-non-volatile (bit-0)	SNMP Trap (bit-1)	SYSLOG (bit-2)	Local-volatile (bit-3)	Note
1 Emergency	Yes	No	No	No	Vendor Specific
2 Alert	Yes	No	No	No	CableHome
3 Critical	Yes	No	No	No	CableHome
4 Error	Yes	Yes	Yes	No	CableHome
5 Warning	Yes	Yes	Yes	No	CableHome
6 Notice	No	Yes	Yes	Yes	CableHome
7 Informational	No	No	No	No	CableHome and Vendor Specific
8 Debug	No	No	No	No	Vendor Specific

The PS MUST support the ability to be configured to generate all notification types for each event priority level listed in Table 6-20.

[16] Editorial correction to Table 6-20 per ECN CH1.1-N-03069 by GO on 10/28/03.

EXHIBIT A

6.3.3.2.4.7 Standard Events

The PS MUST send the following generic SNMP traps, as defined in [RFC 3418] and [RFC 2863]:

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

The PS MUST be capable of generating event notifications based on standard CableHome events listed in Appendix II.

6.3.3.2.4.8 Event Throttling and Limiting

The PS MUST support SNMP TRAP/INFORM and SYSLOG throttling and limiting as described in [RFC 2669].

The PS MUST consider events identical if their EventIds are identical.

[RFC 2669] specifies four throttling states:

- unconstrained(1) causes traps and syslog messages to be transmitted without regard to the threshold settings.
- maintainBelowThreshold(2) causes trap transmission and syslog messages to be suppressed if the number of traps would otherwise exceed the threshold.
- stopAtThreshold(3) causes trap transmission to cease at the threshold, and not resume until directed to do so.
- inhibited(4) causes all trap transmission and syslog messages to be suppressed.

A single event MUST be treated as a single event for threshold counting, that is, an event causing both a trap and a syslog message is still treated as a single event.

6.3.3.2.4.9 Secure Software Download Event Reporting

Table II-1 in Appendix II, Format and Content for Event, SYSLOG and SNMP Trap, describes events associated with Portal Services software upgrades, in three categories: Software Upgrade Initialization (SW UPGRADE INIT), Software Upgrade General Failure, and Software Upgrade Success. These events apply only to the standalone PS, since software upgrade (also referred to as secure software download) for a PS with an embedded cable modem is controlled and managed by the DOCSIS cable modem. Section 11.8, Secure Software Download for the PS defines requirements for secure software download for the two classes of Portal Services elements. The embedded PS, as defined in Section 5.1.3.1, Embedded PS and Standalone PS, MUST NOT generate events categorized in Table II-1, Defined Events for CableHome as "Software Upgrade Initialization" (SW UPGRADE INIT) events, "Software Upgrade General Failure" (SW UPGRADE GENERAL FAILURE) events, or "Software Upgrade Success" (SW UPGRADE SUCCESS) events.[17]

6.3.3.3 CMP Discovery Function

6.3.3.3.1 Discovery Function Goals

The goals for the CableHome 1.1 CMP Discovery function are listed below:

- Provide cable operators with visibility to CableHome Host device and CableHome Residential Gateway device attributes.

[17] Revised this paragraph per ECN CH1.1-N-03.0091-1 by GO on 12/5/03.

EXHIBIT A

- Provide cable operators with visibility to applications implemented on CableHome Host devices.
- Co-existence and interoperability between PS, CableHome Hosts and LAN IP devices that are NOT CableHome 1.1 compliant.

Note: The goals for CableHome 1.1 Discovery do NOT preclude the use of other discovery methods, protocols, etc. on the LAN but are only intended to specify the requirements for CableHome 1.1 compliant devices. However, CableHome Host devices MUST NOT interfere with correctly operating non-CableHome LAN IP Devices.

Assumptions

The assumptions for the CableHome 1.1 CMP discovery capability include the following:

- CableHome Host devices, LAN IP devices, and CableHome Residential Gateway devices implement the Internet Protocol (IPv4) suite of protocols
- CableHome Hosts implement a Device Profile in XML format as described in Section 6.5.3.1.3 and a QoS Profile in XML format described Section 10.3.2.4.2.1

6.3.3.3.1.1 Discovery Function System Design Guidelines

The system design guidelines listed in Table 6-21 provided guidance in the development of the CMP Discovery function specification.

Table 6-21 — PS Discovery System Design Guidelines

Reference	Discovery System Design Guidelines
Discovery 1	The PS and BP will support a protocol for discovering CableHome Host devices connected to the home LAN.
Discovery 2	The PS will provide to the cable operator upon request information about devices added to the home LAN.
Discovery 3	The PS will provide to the cable operator upon request information about applications implemented on CableHome Host devices.
Discovery 4	Discovery protocol message exchange within the home LAN will not appreciably degrade performance of the home LAN.
Discovery 5	Home LAN discovery protocol messaging will not propagate onto the WAN.

6.3.3.3.2 Discovery Function System Description

The purpose of the CMP Discovery Function is to provide the cable operator with information about the devices and applications available on a subscriber's LAN.

The CableHome 1.1 Discovery specifies the PS to serve as a central repository of information about devices and applications available on the subscriber's LAN. CableHome-specified BP logical elements provide device-specific information about the device in which they reside, and a list of applications implemented in the device in which they reside.

The CableHome 1.1 Discovery function consists of the following two steps:

1. The PS learns each CableHome Host's IP address and MAC address. The PS learns this information directly for LAN-Trans devices when it receives and responds to their DHCP DISCOVER requests. Refer to Section 7.3.3.1.4 CDS Requirements. The PS is required to learn this information from LAN-Pass devices in order to support USFS functionality (refer to Section 8.3.3.4 for Upstream Selective

EXHIBIT A

Forwarding Switch Overview and Requirements), but CableHome specifications do not prescribe how this is to be done.

2. The PS acquires device attributes and applications information from each BP. Each BP is required to send its Device Profile and QoS Profile to the PS. This is done through a "BP initiated" model, in which the BP sends the information to the CMP. The BP is permitted to initiate this information transfer at any time but is required to do so each time it acquires or renews its IP address lease. The PS receives this information and stores it, making it accessible to the cable operator through the PSDev MIB [CH5].

The PS maintains information about the CableHome Residential Gateway device, analogous to the BP's Device Profile, in the PS Database. This information, enabling the cable operator to discover attributes of the CableHome Residential Gateway, is available via SNMP through the sysDescr, sysName, and sysLocation objects of MIB-2 [RFC 1213] and through the PS Device Profile Group of the PSDev MIB [CH5].

6.3.3.3.3 Discovery Function Requirements

The PS MUST store the Device Profile information (ref.: Section 6.5.3.1 BP Device Profile) received in the BP_Init message from each BP, in the PS Database and make it accessible via the PS Device MIB CableHome Host/BP Device Profile Table (cabhPsDevBpProfileTable) [CH5]. The PS is also required to store application information received from the QoS Profile resulting in discovery of this application information. See Section 10.3.2.4.2.

The PS MUST store its Device Profile attributes listed below in the PS Database and make them accessible to the SNMP entity via the PS Device Profile Group of the PS Device MIB [CH5]:

- Device Type (cabhPsDevPsDeviceType)
- Manufacturer Universal Resource Locator (cabhPsDevPsManufacturerUrl)
- Device Model Universal Resource Locator (cabhPsDevPsModelUrl)
- Device Universal Product Code (cabhPsDevPsModelUpc)

6.3.3.4 CMP LAN Messaging Function

LAN Messaging refers to the exchange of messages between the PS and a BP. Although SNMP systems are prevalent in cable operators' data networks for the purpose of monitoring and configuring Cable Modem Termination Systems (CMTS) and cable modems (CM), SNMP is not prevalent among devices that cable data service subscribers have connected to their home LANs. Consequently, CableHome defines an in-home messaging protocol to satisfy cable operators' needs to support their data service subscribers while maintaining compatibility with messaging protocols typically implemented in LAN-based data communications devices. This section describes the CableHome 1.1 LAN messaging solution.

It is critical to note that a BP could reside in either the LAN-Trans or LAN-Pass domain. A BP in the LAN-Trans domain can easily address packets to the PS, since the PS Server Router address (cabhCdpServerRouter) is the LAN-Trans BP's default gateway, passed to the BP in DHCP Option Code 3. However, a LAN-Pass BP has no legitimate knowledge of the PS Server Router IP address. LAN messages sent to the PS from a LAN-Trans BP can use the PS Server Router IP address as the destination IP address. Another method has to be defined for the LAN-Pass BP.

One way to ensure LAN-Pass BP-to-PS messaging, and the method adopted for CableHome 1.1, is to define a fixed, "well-known" IP address in the PS that the LAN-Pass BP will use as a destination. Since the PS is a layer-2 bridge for LAN-Pass devices, the USFS function will be relied upon to capture messages sent by a LAN-Pass BP to the well-known destination IP address. The packet(s) addressed to the well-known PS IP address that are captured by the USFS function are then processed by the PS. The address 192.168.0.1 is defined as the "well-known" PS IP address that LAN-Pass BPs are required to use as the destination IP address for BP-PS LAN messaging. This fixed, well-known PS IP address is not permitted

EXHIBIT A

to be assigned by the CDS to LAN-Trans devices. The well-known PS IP address defined above has the same value as the *default* value of cabhCdpServerRouter, but the well-known PS IP address defined for LAN messaging is fixed. It cannot be changed, while the value of cabhCdpServerRouter can be changed via PS Configuration File or SNMP Set command. The PS is required to respond to both addresses, if they are different.

Since a BP could reside in either address domain, it needs to support the addressing method defined for LAN-Trans as well as the addressing method defined for LAN-Pass BPs. In other words, BPs are required to support both LAN-Trans - to - PS addressing and LAN-Pass - to - PS addressing, and the PS is required to accept messages destined to either the fixed "well-known" PS IP address or the PS Server Router address (which could be the same or could be different). The BP will use the presence or absence of DHCP Option code 43 sub-option 101 value "CableHome1.1LAN-Trans" in the DHCP ACK received from its DHCP server to determine which addressing method it is required to use. If this value is present in the DHCP Option code 43 sub-option 101 the BP is required to send its BP_Init messages to its (the BP's) default gateway, i.e., the PS Server Router address. If the value is not present in the DHCP ACK the BP is required to send its BP_Init messages to 192.168.0.1.

The PS will reply to a BP using as the destination address the BP address the PS received as a source IP address, i.e., the PS replies by sending to the address from which it received the BP-initiated message. To a LAN-Pass BP, this message appears to originate from a device in the LAN-Trans domain.

Figure 6-7 summarizes the BP-to-PS addressing requirements for a CableHome 1.1-compliant BP logical element.

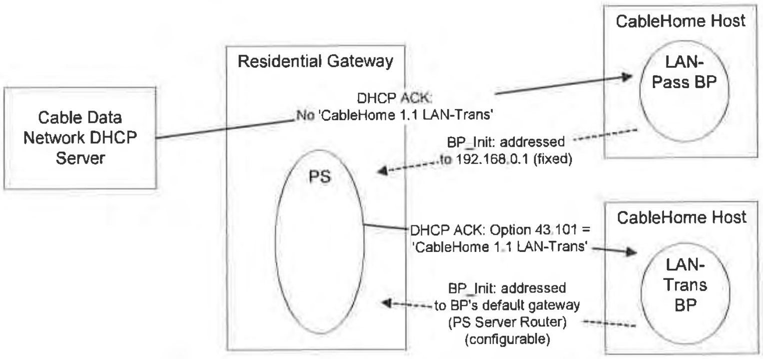

CableHome Host
LAN-Pass BP
Residential Gateway
DHCP ACK:
No 'CableHome 1.1 LAN-Trans'
Cable Data Network DHCP Server
BP_Init: addressed to 192.168.0.1 (fixed)
PS
CableHome Host
DHCP ACK: Option 43.101 = 'CableHome 1.1 LAN-Trans'
LAN-Trans BP
BP_Init: addressed to BP's default gateway (PS Server Router) (configurable)

Figure 6-7 — CableHome 1.1 BP_Init Message Addressing

6.3.3.4.1 LAN Messaging Function Goals

Goals for CableHome 1.1 LAN Messaging function are listed below:

- Support device and application discovery requirements by enabling the transfer of Device Profile information from BP logical elements in CableHome Host devices to the PS element in CableHome compliant residential gateway devices.
- Specify an open, industry standard method for the exchange of Device Profile and prioritized Quality of Service Profile between the BP logical element in each CableHome Host device and the PS logical element in a CableHome compliant residential gateway device.

EXHIBIT A

6.3.3.4.2 LAN Messaging Function System Design Guidelines

The design guidelines listed in Table 6.3.3.4.3 guided specification of the LAN Messaging function.

6.3.3.4.3 LAN Messaging Function System Design Guidelines

Reference	LAN Messaging Function System Design Guidelines
LAN Msg 1	The PS and BP will support a protocol for exchanging XML-formatted information.
LAN Msg 2	The LAN messaging protocol will be an open standard.
LAN Msg 3	The LAN messaging protocol will be as compatible as possible with existing LAN IP Devices and Residential Gateway devices.

6.3.3.4.4 LAN Messaging Function System Description

Due to its flexibility, industry acceptance, and capabilities to pass configuration and status information, XML [XML1] was chosen as the information format for CableHome 1.1 LAN (BP-PS) messaging. XML has gained acceptance as a communication protocol for the Internet, and is an open, non-proprietary format popular for its adaptation to disparate systems. XML benefits include its ability to enable the creation, modification, organization, and storage of information in any form tailored to the needs of management messages. XML document rules and character support provide additional benefit. The capabilities of XML make it a good fit for messages exchanged between CableHome PS and BP logical elements.

Simple Object Access Protocol (SOAP) [SOAP] is a member of the family of XML-associated protocols. It is a lightweight protocol for the exchange of information in a decentralized, distributed environment. SOAP is an XML-based protocol that consists of three parts:

- an envelope the defines a framework for describing what is in a message and how to process it
- a set of encoding rules for expressing instances of application-defined datatypes, and
- a convention for representing remote procedure calls and responses

CableHome 1.1 specifies SOAP for the exchange of Device Profiles and QoS Profiles between the PS and BP logical elements.

6.3.3.4.4.1 Simple Object Access Protocol (SOAP)

Encoding a Profile in XML is only the first step for the exchange of messages between CableHome Residential Gateway and CableHome Host devices. The CableHome specification has to also provide conventions for the following:

- types of information to be exchanged
- how the information is to be expressed as XML
- how the information is sent from one logical element to another

Without these conventions, the PS and the BP cannot decode the information they're given, even if it is encoded in XML. These required conventions are provided by SOAP [SOAP]. Since CableHome 1.1 specifies SOAP only for messaging within a subscriber's home LAN, not all of the SOAP messaging formats are required for CableHome 1.1.

Transport Layer of SOAP

HTTP is the most commonly used transport mechanism for SOAP messaging. The PS and the BP are required to use HTTP over TCP as the transport mechanism for SOAP messaging to insure interoperability

EXHIBIT A

between various PS and BP implementations. In order to support this scheme, the PS implements an HTTP server listening on port 80 and the BP implements an HTTP client. The PS and the BP are each also required to have a SOAP Processing application running.[18]

When the SOAP processing application running on a BP or on a PS receives a SOAP message, it processes that message by performing the following actions in the order listed below. The BP is prohibited from making modifications to the Device Profile or to the QoS Profile as a result any SOAP message other than the BP_Init_Response message received from the PS:

1. Identify all parts of the SOAP message intended for that application.
2. Verify that all mandatory parts identified in step 1 are supported by the application for this message and process them accordingly. If this is not the case then discard the message. The processor has the option to ignore optional parts identified in step 1 without affecting the outcome of the processing.
3. If applicable, send a response message as defined in later sections.

6.3.3.4.4.1.1 SOAP Message Formatting[19]

This section introduces the format of SOAP messages required by CableHome 1.1 to support LAN messaging requirements.

The SOAP messaging that takes place between the PS and the BP (for the purpose of exchanging the device and QoS profiles) is initiated by the BP. This messaging is referred to as "BP_Init Operation".

All the IP addresses in BP_Init messaging are expressed in decimal dotted notation (example: 192.168.0.11).

CableHome 1.1 defines a *confirmation code* tag used in CableHome SOAP messaging. The confirmation code values associated with this tag are described below:

Confirmation Code Values

Confirmation code values in a BP_Init_Response message indicate the success/failure of the previous BP_Init message in the transaction. The CableHome-defined confirmation code values are listed in Table 6-22.

Table 6-22 — CableHome LAN Messaging Confirmation Code Values

Confirmation Code	Meaning
0	Success
-10	Error

CableHome defines one confirmation code tag, the BP_Init Confirmation Code, to which the confirmation code values listed above apply. The BP_Init Confirmation Code refers to the quality of the whole BP_Init message.

[18] Revised this paragraph per ECN CH1.1-N-03060 by GO on 10/28/03.
[19] Revised this section per ECN CH1.1-N-03.0087-4 by GO on 12/5/03.

EXHIBIT A

6.3.3.4.4.2 BP-initiated SOAP Messaging (BP_Init Operation)[20]

Figure 6-8 presents the message flow diagram for the messages exchanged between a BP and PS during BP initiated SOAP messaging. The message sent by the BP to the PS is referred to as a BP_Init message. The response issued by a PS to the BP_Init message is a BP_Init_Response. The messaging shown in Figure 6-8 is the establishment of a TCP connection between the BP and the PS, a BP_Init message issued by the BP with its profile information to the PS (BP_Init message), the PS response to the BP_Init message (BP_Init_Response message), and the TCP connection termination.

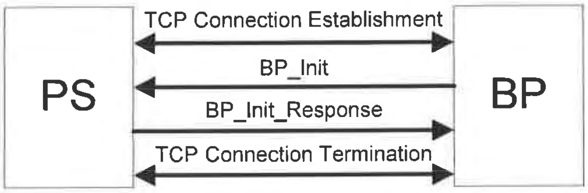


Figure 6-8 — BP-initiated SOAP Messaging: BP_Init Operation

Note: The BP performs an active TCP open upon it having a BP_Init message to transmit, and the PS performs a passive TCP open.

6.3.3.4.4.2.1 BP_Init XML Schema[21]

The format of the BP_Init message follows, using the transfer of the BP's Device Profile and QoS Profile to the PS. See Appendix VI for an example of a BP_Init message.[22]

```
POST /DevQoSProfileService HTTP/1.1
HOST IP Address of PS
Content-Type: text/xml; charset="utf-8"
Content-Length: nnnn
SOAPAction: "/DevQoSProfileService"

<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <ch:BP_Init xmlns:m= "IP Address of PS" >
      <ch:BP_IP>
        IP Address of BP
      </ch:BP_IP>
        Device profile from BP
        QoS profile from BP
      </ch:BP_Init>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```

[20] Revised this section per ECN CH1.1-N-03060 by GO on 10/28/03.
[21] Revised this section per ECN CH1.1-N-03071 and ECN CH1.1-N-03.0089-2 by GO on 10/28/03 and 12/2/03.
[22] Revised this paragraph per ECN CH1.1-N-03068 by GO on 10/31/03.

EXHIBIT A

6.3.3.4.4.2.2 BP_Init_Response XML Schema[23]

The format of the response message to the BP_Init message, the BP_Init_Response message, is shown below, using by way of example the response to the Device Profile and QoS Profile BP_Init message described above. See Appendix VI for an example of a BP_Init_Response message.

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/xml; charset="utf-8"
Content-Length: nnnn

<SOAP-ENV:Envelope
 xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
 SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
   <SOAP-ENV:Body>
     <ch:BP_Init_Response xmlns:m= "IP Address of PS">
        <ch:BPInitConfirmationCode>0</ch:BPInitConfirmationCode >
        <ch:QoSProfile> QoS Profile from PS </ch:QoSProfile>
     </ch: BP_Init_Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

6.3.3.4.5 LAN Management Messaging Function Requirements[24]

The PS MUST implement a HTTP server in accordance with Server requirements of [RFC 2616], listening on port 80.

The PS MUST implement a TCP stack in accordance to the requirements of [[RFC 793].

The PS MUST implement an XML parser in accordance with [XML1].

The PS MUST implement a SOAP parser compliant with specifications described in [SOAP].

The PS MUST use HTTP over TCP as the transport mechanism for SOAP messaging to insure interoperability between various PS and BP implementations.

The PS MUST run a SOAP-over-HTTP web service named DevQoSProfileService.

The PS MUST perform the following actions in the order listed when it receives a BP_Init SOAP message:

1. Identify all parts of the message intended for the PS.
2. Verify that the received message is formatted as specified in Section 6.3.3.4.4.2.1 and process the message. If the message does not contain all mandatory components, discard the message. The processor has the option to ignore optional parts identified in step 1 without affecting the outcome of the processing.
3. Return a BP_Init_Response message with the appropriate confirmation code and QoS profile as described in Section 6.3.3.4.4.1.1 SOAP Message Formatting.

[23] Revised this section per ECN CH1.1-N-03071, ECN CH1.1-N-03.0089-2, and CH1.1-N-03.0087-4 by GO on 10/28/03, 12/2/03, and 12/5/03.
[24] Revised this section per ECN CH1.1-N-03060 and CH1.1-N-03.0087-4 by GO on 10/28/03 and 12/5/03.

EXHIBIT A

The PS MUST observe the following SOAP Syntax Rules:

- A SOAP message MUST be encoded using XML.
- A SOAP message MUST have a SOAP Envelope.
- A SOAP message MAY have a SOAP header.
- A SOAP message MUST have a SOAP Body.
- A SOAP message MUST use the SOAP Envelope namespaces.
- A SOAP message MUST use the SOAP Encoding namespace.
- A SOAP message MUST NOT contain a Document Type Declaration (DTD).
- A SOAP message MUST NOT contain XML Processing Instructions.
- The PS MUST use the following default namespaces:
    - for SOAP envelope syntax: http://schemas.xmlsoap.org/soap/envelope/
    - for SOAP encoding and data types: http://schemas.xmlsoap.org/soap/encoding/
    - for 'BP_Init_Response': IP Address of PS

The PS MUST accept active TCP opens initiated from the LAN side to the destination IP address of 192.168.0.1 or with a destination IP address equal to the value of cabhCdpServerRouter.

The PS MUST accept and process each BP_Init message it receives on TCP connections established from LAN devices to its 192.168.0.1 or cabhCdpServerRouter IP addresses.

The PS MUST ignore any BP_Init messages received on the PS WAN Interface.

The PS MUST respond with a BP_Init_Response message to each BP_Init message received on its LAN interface. The PS MUST identify a BP_Init message by the string 'POST /DevQoSProfileService HTTP/1.1', which is defined in section 6.3.3.4.4.2.1, BP_Init Message Format. The PS MUST send the BP_Init_Response message to the IP address which was the source IP address of the BP_Init message.[25]

The PS MUST close the TCP connection once the BP_Init_Response message transmission is completed.

The PS is not required to respond to BP_Init messages that carry neither a Device Profile nor a QoS Profile. If the BP_Init message received by the PS contains a Device Profile, the BP_Init_Response message issued by the PS MUST contain a valid Device Confirmation Code.

If the BP_Init message received by the PS contains a QoS Profile, the BP_Init_Response message issued by the PS MUST contain a valid QoS Confirmation Code and MAY contain a QoS Profile.

The PS MUST NOT transmit a BP_Init_Response message out any PS WAN interface.

6.4 PS Logical Element CableHome Test Portal (CTP)

6.4.1 CTP Goals

The goals for the CableHome Test Portal include:

- Enable LAN IP Device and CableHome Host fault diagnostics
- Enable visibility to LAN IP Devices and CableHome Hosts, as well as access to the number and types of LAN IP Devices and CableHome Host
- Enable LAN IP Device and CableHome Host performance monitoring

[25] Revised this paragraph per ECN CH1.1-N-03 0087-4 by GO on 12/8/03.

EXHIBIT A

6.4.2 CTP Design Guidelines

The CableHome 1.1 Test Portal system design guidelines are listed in Table 6-23. A number of these guidelines are common with the CMP design guidelines. This list provided guidance for the specification of CTP functionality.

Table 6-23 — CTP System Design Guidelines

Reference	CTP System Design Guidelines
CTP 1	The need exists for interfaces to support the management and diagnosis features and functions required to support cable-based services provisioned across the home network.
CTP 2	Local and remote monitoring capabilities are needed that can monitor home network operation and help the consumer and cable operator identify problem areas.
CTP 3	The cable network NMS requires a method to gather identification information about each IP device connected to the home network.
CTP 4	The cable network NMS requires a method to detect whether a connected device is in an operable state.

6.4.3 CTP System Description

The CTP (CableHome Test Portal) contains the "remote tools" with which the NMS can collect further LAN device information. Tests must be run remotely, since getting past a network address translation (NAT) function in a router can be a challenge. For example, a WAN-to-LAN ping will not pass through a PS, unless the CAP has been preconfigured to pass this traffic. The CTP is a local proxy used to interpret and execute the remote fault/diagnostic class of SNMP messages it receives from the NMS operator. These LAN IP Device and CableHome Host tests are defined based on problems likely to be encountered for CableHome 1.1 type of home networks: connectivity and throughput diagnostics.

These functions are termed the CTP Connection Speed Tool and CTP Remote Ping Tool. The Connection Speed and Remote Ping Tools enable the cable operator's customer support center and network operations center to learn more about the connection between the PS element and LAN IP Devices and CableHome Hosts in the home.

6.4.3.1 CTP Connection Speed Tool Function

6.4.3.1.1 Connection Speed Tool Function Goals

The goal of the CableHome Connection Speed function is to enable the CableHome system manager to remotely acquire metrics about the performance of the home LAN between the PS and a specific LAN IP Device or CableHome Host.

6.4.3.1.2 Connection Speed Tool System Design Guidelines

Design guidelines listed in Table 6-23 *CTP System Design Guidelines* were used to guide specification of the Connection Speed Tool function.

6.4.3.1.3 Connection Speed Tool Function System Description

The Connection Speed Tool function is used to get a rough measure of the throughput performance across the link between the PS and a LAN IP Device or CableHome Host. It sends a burst of packets between the PS and the LAN IP Device or CableHome Host under test, and the round trip time is measured for the burst. Generally speaking, the NMS operator fills in a few parameters and triggers the function, and results are stored in the PS Database for later retrieval through the CTP MIB [CH4].

EXHIBIT A

The Connection Speed function relies on the LAN IP Devices and CableHome Hosts to have a "loop-back function" or "echo-service" embedded. The Internet Assigned Numbers Authority (IANA) has assigned the echo service port 7 for both TCP and UDP [RFC 347]. The default value of the source IP address (cabhCtpConnSrcIp) is the same as the value of the PS LAN default gateway (cabhCdpServerRouter). The value of cabhCtpConnSrcIp can be set to any valid PS WAN-Data IP address or to any valid PS LAN Interface IP address. The PS WAN-Man IP address is not used as the source IP address for a CTP tool since when a PS WAN-Man IP address is present but a PS WAN-Data IP address is not, the PS is operating in Passthrough Primary Packet-handling mode and the cable operator can test LAN IP Devices and CableHome Hosts directly from the NMS console if desired. This test feature works on LAN IP Devices and CableHome Hosts in either the LAN-Trans or LAN-Pass address realms that implement the Echo Service function as described in [RFC 347].

The CTP Testable Requirements section below lists the parameters and responses for the Connection Speed Tool. Section 12.2.1.1 details the operation of the Connection Speed Tool.

6.4.3.1.4 Connection Speed Tool Function Requirements[26]

> The PS MUST implement the Connection Speed Tool, and MUST comply with the default values and value ranges defined for the Connection Speed Tool-specific objects of the CableHome CTP MIB [CH4].
>
> The PS SHOULD transmit the bytes of test data as fast as possible when running the Connection Speed Tool.
>
> The PS MUST use Port 7 as the Destination Port when running the Connection Speed Tool.
>
> The PS MUST NOT generate packets out any WAN Interface when running the Connection Speed Tool function.

When the NMS triggers the CTP to initiate the Connection Speed Tool by setting cabhConnControl = start(1), the PS MUST do the following:

- reset the timer
- set cabhCtpConnStatus = running(2)
- transmit the number of packets equal to the value of cabhCtpConnNumPkts, each of the size equal to the value of cabhCtpConnPktSize, to the IP address equal to the value of cabhCtpConnDestIp and port number 7, using the protocol specified by cabhCtpConnProto
- initiate the timer with the first bit transmitted
- terminate the timer when the last bit is received back from the target LAN IP Device or when the value of the timer is equal to the value of cabhCtpConnTimeOut, whichever occurs first
- when the timer is terminated, set cabhCtpConnStatus = complete(3) and report the appropriate event (refer to Appendix II - CTP Events)
- store the value of the timer (in milliseconds) in cabhCtpConnRTT
- if the Connection Speed Tool test times out before the last bit is received from the target LAN IP Device or CableHome Host, report the appropriate event (refer to Appendix II - CTP Events)
- calculate the throughput as defined in the requirement below and store the value in cabhCtpConnThroughput

If the Connection Speed Tool is terminated by the NMS setting the object cabhCtpConnControl = abort(2) or for any other reason before the last bit is received from the target LAN IP Device and CableHome Host

[26] Revised this section per ECN CH1.1-N-03.0107-1 by KB on 4/5/04.

EXHIBIT A

or before the Connection Speed Tool test times out, the PS MUST set cabhCtpConnStatus = aborted(4) and report the appropriate event (refer to Appendix II - CTP Events).

When the Connection Speed Tool function is executing, the PS MUST determine the average round-trip throughput between the PS and the LAN IP Device or CableHome Host whose address is passed in cabhCtpConnDestIp (the target LAN IP Device) in kilobits per second, round the number to the nearest whole integer, and store the result in cabhCtpConnThroughput.

The PS MUST reset cabhCtpConnPktsSent, cabhCtpConnPktsRecv, cabhCtpConnRTT and cabhCtpConnThroughput each to a value of 0 when the Connection Speed Tool is initiated (i.e., when the value of cabhCtpConnControl is set to start(1)).

Connection Speed Tool RTT is measured at the PS as the time from the first bit of the first sent packet to the last bit of the last received packet. RTT is only valid if the number of received packets is equal to the number of transmitted packets.

The PS MUST allow the Connection Speed Tool destination IP address (cabhCtpConnDestIp) to be set to any valid IPv4 address of any LAN IP Device accessible through any LAN Interface of the PS running the CTP Connection Speed Tool.

Setting the Connection Speed Tool control object, cabhCtpConnControl, with the value start(1) MUST result in the execution of the Connection Speed Tool.

Setting the Connection Speed Tool control object, cabhCtpConnControl, with the value abort(2) MUST result in the termination of the Connection Speed Tool.

The default value of cabhCtpConnStatus is notRun(1), which indicates that the Connection Speed Tool has never been executed.

The PS MUST set the value of cabhCtpConnStatus to running(2) if the Tool has been instructed to start, has not been terminated, and if the Connection Speed Timer has not timed out.

The PS MUST set the value of cabhCtpConnStatus to complete(3) when the last packet sent by the Connection Speed Tool is received by the CTP.

The PS MUST set the value of cabhCtpConnStatus to aborted(4) if the Connection Speed Tool is terminated after it is initiated by an SNMP set of the value abort(2) to the object cabhCtpConnControl, or if the test is otherwise terminated before the last packet sent by the Connection Speed Tool is received and before the Connection Speed Tool timer (cabhCtpConnTimeOut) expires.

The PS MUST set the value of cabhCtpConnStatus to timedOut(5) if the Connection Speed Tool timer (cabhCtpConnTimeOut) expires before the last packet sent by the Connection Speed Tool is received by the CTP.

The PS MUST NOT use any IP address for the Connection Speed Tool source IP address (cabhCtpConnSrcIp) except a current, valid PS WAN-Data IP address (i.e., an active cabhCdpWanDataAddrIp object value) or a current, valid PS LAN Interface IP address. If an invalid value is configured for cabhCtpConnSrcIp, the PS MUST treat the execution of the test as an aborted case and set the Connection Speed Tool status object cabhCtpConnStatus to 'aborted' and report the appropriate event (see Table II-1).

EXHIBIT A

6.4.3.2 CTP Ping Tool Function

6.4.3.2.1 Ping Tool Function Goals

The goal of the Ping Tool function is to enable the CableHome system manager to remotely test or verify connectivity between the PS and a specific LAN IP Device.

6.4.3.2.2 Ping Tool Function System Design Guidelines

Design guidelines listed in Table 6-23 "CTP System Design Guidelines" were used to guide specification of the Ping Tool function.

6.4.3.2.3 Ping Tool Function System Description

The Ping Tool function is called to test connectivity between the PS and individual LAN IP Devices or CableHome Host devices. Results of multiple executions of the Ping Tool test can be assembled by the NMS to create a network scan of the LAN IP Devices or CableHome Host devices. The DHCP table of the CDP has a list of historical devices, but only the devices that employ DHCP. Ping may capture a current state including non-DHCP clients. To keep the PS simple, it is expected that the NMS increments the address and stores the results in the NMS tool to perform a scan of a LAN subnet.

The PING Tool is initiated by a series of SNMP set-request messages issued by the cable network NMS console to the PS management address.

Section 12.2.1.2 details the operation of the Ping Tool.

6.4.3.2.4 Ping Tool Function Requirements[27]

The CTP Ping Tool MUST be implemented using the Internet Control Message Protocol (ICMP) "Echo" facility. The CTP will issue an ICMP Echo Request and the LAN IP Device is expected to return an ICMP Echo Reply.

The CTP MUST ignore, and exclude from the cabhCtpPingNumRecv count, any Echo Reply received after cabhCtpPingTimeOut expires.

The PS MUST implement the CTP Ping Tool, and MUST comply with the default values and value ranges defined for the Ping Tool-specific objects of the CableHome CTP MIB [CH4].

When the NMS triggers the PS to initiate the Ping Tool by setting cabhPingControl = start(1), the PS MUST do the following:

- set cabhCtpPingStatus = running(2)
- issue as many Pings (ICMP requests) as specified by the value cabhCtpPingNumPkts, to the IP address defined by the value of cabhCtpPingDestIp, using the value of cabhCtpPingSrcIp as the source address of each request. The size of each test frame issued is the value of cabhCtpPingPktSize. A timeout for each ping (ICMP Echo Request/Response pair) is the value of cabhCtpPingTimeOut.
- if the value of cabhCtpPingNumPkts is greater than 1, wait the amount of time defined by the value of cabhCtpPingTimeBetween between each Ping request issued by the CTP.

If the CTP receives all Ping replies before their individual timeout timer expires, the PS MUST set cabhCtpPingStatus = complete(3) and report the appropriate event (refer to Appendix II - CTP Events).

If the Ping Tool is terminated by the NMS setting the object cabhCtpPingControl = abort(2) or for any other reason before the last bit is received from the target LAN IP Device and before the timer is

[27] Revised this section per ECN CH1.1-N-03.0106-2 by KB on 4/5/04.

EXHIBIT A

terminated, the PS MUST set cabhCtpPingStatus = aborted(4) and report the appropriate event (refer to Appendix II - CTP Events).

If a timeout timer expires for at least one of the pings, before its reply is received from the target LAN IP Device, the PS MUST set cabhCtpPingStatus = timedOut(5) and report the appropriate event (refer to Appendix II - CTP Events).

When the CTP Ping Tool function is initiated, the PS MUST determine the average round-trip time between the PS and the LAN IP Device or CableHome Host device whose address is passed in cabhCtpPingDestIp (the target LAN IP Device), over the number of Ping requests defined by cabhCtpPingNumPkts, and store the result in cabhCtpPingAvgRTT. When the CTP Ping Tool function is initiated, the PS MUST determine the minimum and maximum round-trip times between the PS and the target LAN IP device, for the set of Ping requests defined by cabhCtpPingNumPkts, and store the values in cabhCtpPingMinRTT and cabhCtpPingMaxRTT, respectively.

If an ICMP error occurs during execution of the Ping Tool, the PS MUST increment the value of cabhCtpPingNumIcmpError and log the error in cabhCtpPingIcmpError. The last ICMP error that occurs will over-write the previous one written.

The PS MUST reset cabhCtpPingNumSent, cabhCtpPingNumRecv, cabhCtpPingAvgRTT, cabhCtpPingMaxRTT, cabhCtpPingMinRTT, cabhCtpPingNumIcmpError and cabhCtpPingIcmpError each to a value of 0 when the Ping Tool is initiated (i.e., when the value of cabhCtpPingControl is set to start(1)).

Ping Tool RTT is measured at the PS as the time from the last bit of each ICMP Echo Request packet transmitted by the CTP Ping Tool, to the time when the last bit of the corresponding ICMP Echo Reply packet is received.

The PS MUST allow the Ping Tool destination IP address (cabhCtpPingDestIp) to be set to any valid IPv4 address of any LAN IP Device or CableHome Host device accessible through any LAN Interface of the PS running the CTP Ping Tool.

The PS MUST NOT generate packets out any WAN Interface when executing the Ping Tool function.

The PS MUST NOT use any IP address for the Ping Tool source IP address (cabhCtpPingSrcIp) except a current, valid PS WAN-Data IP address (i.e., an active cabhCdpWanDataAddrIp object value) or a current, valid PS LAN Interface IP address. If an invalid value is configured for cabhCtpPingSrcIp, the PS MUST treat the execution of the test as an aborted case and set the Ping Tool status object cabhCtpPingStatus to "aborted" and report the appropriate event (see Table II-1).

6.5 BP Logical Element - Management Boundary Point (MBP)

Section 5 defines the Boundary Point (BP), which is the CableHome-defined logical element aggregating CableHome-specified functionality of a CableHome Host device. The Management Boundary Point (MBP) is the logical element of the BP responsible for CableHome-defined discovery capabilities of the BP.

Discovery of CableHome Host devices is the first step of the eventual management of CableHome-specified functionality in these devices. The CableHome 1.1 specification enables discovery of CableHome Host devices through access to the Profile information via HTTP, from the CMP.

EXHIBIT A

6.5.1 MBP Goals

The goal for the CableHome 1.1 MBP is to fulfill CableHome requirements for CableHome Host device discovery and LAN messaging. The MBP is required to provide the cable operator with the Device Profile for each CableHome Host device, through the PS acting as a proxy.

6.5.2 MBP System Design Guidelines

System design guidelines listed in Table 6-24 guided specification of the MBP.

Table 6-24 — MBP System Design Guidelines

Reference	MBP System Design Guidelines
MBP 1	The MBP will maintain information about the attributes of the CableHome Host device in which the BP resides.
MBP 2	The MBP will provide CableHome Host device and application information to the CableHome system manager during the BP initialization process.
MBP 3	The MBP will provide CableHome Host device and application information to the CableHome system manager periodically after BP initialization completes.

6.5.3 MBP System Description

The BP is required to maintain a Device Profile as described in Section 6.5.3.1.3 Device Profile Description and a QoS Profile described in Section 10.3.2.4.2.1 QoS Profile XML Schema.

The BP is further required to send the Device Profile to the PS, thereby providing the CableHome system manager access to each CableHome Host device's attribute information through the PS Device MIB [CH5] via SNMP access over the cable data WAN. By providing access to the CableHome Host device's attribute information in this fashion, the MBP satisfies CableHome 1.1 requirements for device discovery.

The BP is also required to support LAN messaging using SOAP over HTTP/TCP transport, as the means by which the Device Profile and QoS Profile are transferred from the BP to the PS.[28]

6.5.3.1 BP Device Profile

The Device Profile and QoS Profile are XML-formatted structures containing information about the CableHome Host device and the applications it implements. The Device Profile is used as a means for maintaining and communicating information about the CableHome Host device. The BP is required to implement a Device Profile and provide its Device Profile information to the PS, which makes the information available through the PS Device MIB [CH5]. The cable operator's data network NMS and other subscriber-support organizations can obtain basic information about the CableHome Host device by querying the PS Device MIB over the cable data network using SNMP Get-request messages.

6.5.3.1.1 Device Profile Goals

The goals of the BP Device Profile are listed below:

- aggregate information specific and unique to the CableHome Host device implementing the BP
- provide the CableHome system manager with information about the CableHome Host device

[28] Revised this paragraph per ECN CH1.1-N-03060 by GO on 10/28/03.

EXHIBIT A

6.5.3.1.2 Device Profile System Design Guidelines

System design guidelines listed in Table 6-25 guided the specification of the MBP Device Profile.

Table 6-25 — MBP Device Profile System Design Guidelines

Reference	MBP Device Profile System Design Guidelines
MBP DevProf 1	The MBP will maintain a set of device-specific information about the CableHome Host device in which the BP resides.
MBP DevProf 2	The format of the device-specific information will adhere to an open standard.
MBP DevProf 3	The format of the device-specific information maintained by an MBP will compatible with LAN IP Device operating systems, will be flexible to accommodate any kind or amount of device-specific information, and will be as compatible as possible with industry protocols and trends.

6.5.3.1.3 Device Profile Description

CableHome 1.1 specifies implementation of a Device Profile and a QoS Profile in BP logical elements to support discovery of CableHome Host Devices and to support the provisioning of QoS priorities in BPs. The Device Profile and QoS Profile are XML-formatted structures. The Device Profile contains a set of attributes that describe the CableHome Host device. A Device Profile includes CableHome-specified attributes and could include vendor-specified attributes as well. The QoS Profile is described in the Section 10.3.2.4.2.1 QoS Profile XML Schema. The Device Profile is described in this section.[29]

Table 6-26 presents a high-level description of the Device Profile required for BP elements.[30]

Table 6-26 — BP Device Profile Attributes

Attribute Name	Attribute Type	Use
Device Type	String	required
Manufacturer	String	required
Manufacturer's URL	String	optional
Hardware Revision	String	required
Hardware Options	String	optional
Serial Number	String	required
Model Name	String	optional
Model Number	String	optional
Model URL	String	optional
Model UPC	String	optional
Model Software OS	String	required
Model Software Version	String	required
LAN Interface Type (IANA ifType)	Integer	required
Number of Media Access Priorities	Integer	required
Physical Location	String	optional
Physical Address	String	required

[29] Revised this paragraph per ECN CH1.1-N-03.0109-1 by KB on 4/4/04.
[30] Revised Table 6-26 per ECN CH1.1-N-03071 by GO on 10/28/03.

EXHIBIT A

Device Profile Attribute Details:

The *Device Type* attribute can have one of the following values: CableHome Residential Gateway or CableHome Host.

The *Manufacturer* attribute is the name of the device manufacturer.

The *Manufacturer's URL* attribute is the Uniform Resource Locator for the manufacturer's web site.

The *Hardware Revision* attribute is a string assigned by the manufacturer uniquely identifying a specific product hardware revision.

The *Hardware Options* attribute is a string assigned by the manufacturer identifying optional product hardware features implemented in the product.

The *Serial Number* attribute is the unique identifying serial number for the CableHome Host device, assigned by the device manufacturer.

The *Model Name* attribute is the CableHome Host device's model name or other identifying name assigned by the device manufacturer.

The *Model Number* attribute is the model number or other identifying value assigned by the device manufacturer.

The *Model URL* attribute is the Uniform Resource Locator for the model's web site.

The *Model UPC* attribute is the Universal Product Code value assigned to the device.

The *Model Software OS* attribute is the operating system implemented on the device.

The *Model Software Version* attribute is the version of software currently running on the device.

The *LAN Interface Type* attribute is an integer containing the IANAifType value [IANAType] for ISO OSI Layer 2 networking technology implemented by the product.[31]

The *Number of Media Access Priorities* attribute refers to the number of media access priorities the CableHome Host device's LAN interface supports. This attribute and its uses are described in detail in Section 10 (QoS Section).

The *Physical Location* attribute is a value that can be assigned by the device owner indicating the physical location of the device, such as *Office* or *Living Room*.

The *Physical Address* attribute is the device's hardware address, such as the Media Access Control (MAC) address of an 802.3-based device.

[31] Revised this statement per ECN CH1.1-N-03071 by GO on 10/28/03.

EXHIBIT A

6.5.3.1.4 Device Profile XML Schema[32]

The Device Profile in XML format as required by CableHome is shown below.

```
<xs: element name="ch:DeviceProfile" type="ch:DeviceProfileEntry"/>

<xs: complexType name="ch:DeviceProfileEntry">

    <xs:element name="ch:deviceType" type="xs:string"/>

    <xs:element name="ch:manufacturer" type="xs:string"/>

    <xs:element name="ch:manufacturerURL" type="xs:string"/>

    <xs:element name="ch:hardwareRevision" type="xs:string"/>

    <xs:element name="ch:hardwareOptions" type="xs:string"/>

    <xs:element name="ch:serialNumber" type="xs:string"/>

    <xs:element name="ch:modelName" type="xs:string"/>

    <xs:element name="ch:modelNumber" type="xs:string"/>

    <xs:element name="ch:modelURL" type="xs:string"/>

    <xs:element name="ch:modelUPC" type="xs:string"/>

    <xs:element name="ch:modelSoftwareOS" type="xs:string"/>

    <xs:element name="ch:modelSoftwareVersion" type="xs:string"/>

    <xs:element name="ch:lanInterfaceType" type="xs:int"/>

    <xs:element name="ch:numberMediaAccessPriorities" type="xs:int"/>

    <xs:element name="ch:physicalLocation" type="xs:string"/>

    <xs:element name="ch:physicalAddress" type="xs:string"/>

</xs:complexType>
```

6.5.3.1.5 Device Profile Requirements

The BP MUST implement a Device Profile as described in Section 6.5.3.1.4, consistent with XML formatting rules described in [XML1].

The BP MUST populate the Device Type attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with the string "CableHome Host" (without the quotes).

[32] Replaced this section per ECN CH1.1-N-03071 by GO on 10/28/03.

EXHIBIT A

The BP MUST populate the Manufacturer attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with a string whose value identifies the manufacturer of the CableHome Host device in which the BP resides.

The BP MUST populate the Hardware Revision attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with a string whose value accurately represents the manufacturer's hardware revision number for the CableHome Host device in which the BP resides.

The BP MUST populate the Serial Number attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with a string whose value is equal to the serial number uniquely identifying the CableHome Host device in which the BP resides.

The BP MUST populate the Model Software OS attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with a string whose value accurately represents the software operating system implemented on the CableHome Host device in which the BP resides.

The BP MUST populate the Model Software Version attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with a string whose value accurately represents the version of BP software implemented on the CableHome Host device in which the BP resides.

The BP MUST populate the LAN Interface Type attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with an integer whose value is equal to the IANAifType [IANAType] representing the LAN technology supported by the CableHome Host device in which the BP resides.[33]

The BP MUST populate the Number of Media Access Priorities attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with an integer in the range 1 - 8 whose value is equal to the number of LAN interface priorities supported by the CableHome Host device in which the BP resides.

The BP MAY populate the Manufacturer's URL attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with a string whose value accurately and uniquely identifies a Uniform Resource Locator for the manufacturer of the CableHome Host device in which the BP resides.

The BP MAY populate the Hardware Options attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with a string whose value represents the hardware options of the CableHome Host device in which the BP resides.

The BP MAY populate the Model Name attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with a string whose value accurately and uniquely identifies the manufacturer's model name for the CableHome Host device in which the BP resides.

The BP MAY populate the Model Number attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with a string whose value accurately and uniquely identifies the manufacturer's model number for the CableHome Host device in which the BP resides.

The BP MAY populate the Model URL attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with a string whose value accurately and uniquely identifies a Uniform Resource Locator for the CableHome Host device model in which the BP resides.

The BP MAY populate the Model UPC attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with a string whose value accurately and uniquely identifies the Universal Product Code for the CableHome Host device in which the BP resides.

[33] Revised this paragraph per ECN CH1.1-N-03071 by GO on 10/28/03.

EXHIBIT A

The BP MAY populate the Physical Location attribute of the BP Device Profile (ref.: Section 6.5.3.1.4 Device Profile in XML Format) with a string value that identifies the physical location of the CableHome Host device in which the BP resides.

The BP MUST populate the Physical Address attribute of the BP Device Profile (ref: Section 6.5.3.1.4 Device Profile in XML Format) with a string value representing the Media Access Control (MAC) Address of the BP's interface. The format of the MAC address is a sequence of 6 hexadecimal numbers, of 2 digits each, separated by colons (example: 00:11:22:AA:CC:DD).[34]

6.5.3.2 MBP LAN Messaging Function

6.5.3.2.1 MBP LAN Messaging Function Goals

The goals of the MBP LAN Messaging Function are listed in Section 6-7 LAN Messaging Function Goals.

6.5.3.2.2 MBP LAN Messaging Function System Design Guidelines

The MBP LAN Messaging Function System Design Guidelines are listed in Table 6.3.3.4.3 LAN Messaging Function System Design Guidelines.

6.5.3.2.3 MBP LAN Messaging Function System Description

The MBP LAN Messaging Function is as described in Section 6.3.3.4.4 LAN Messaging Function System Description.[35]

6.5.3.2.4 MBP LAN Messaging Function Requirements[36]

The BP MUST implement an Echo Service responder, such that the BP immediately echoes any IP packet received on Port 7 to the sender of the packet, bit for bit, changing only the source IP address and port for the destination IP address and port, and vice versa.

The BP MUST implement ICMP Echo and Echo Reply Message types (Type 8 and Type 0) and ICMP Timestamp and Timestamp Reply Message types (Type 13 and Type 14) as described in [RFC 792], and reply appropriately to Ping requests received on any interface.

The BP MUST implement an HTTP client in accordance with the Client requirements of [RFC 2616].

The BP MUST implement a TCP stack in accordance to the requirements of [RFC 793].

The BP MUST implement an XML parser in accordance with [XML1].

The BP MUST implement a SOAP parser in accordance with [SOAP].

The BP MUST use HTTP over TCP as the transport mechanism for SOAP messaging to insure interoperability between various PS and BP implementations.

The BP MUST actively open a TCP connection against the PS immediately before sending a BP_Init message.

If the BP received DHCP Option Code 43 sub-option 101 containing the string 'CableHome 1.1 LAN-Trans' in the DHCP ACK, the BP MUST open the TCP connection for the LAN messaging exchange against the default gateway IP address (value of DHCP Option 3 received in the DHCP ACK).

[34] Revised the preceding paragraph and added this paragraph per ECN CH1.1-N-03.0087-4 by GO on 12/8/03.
[35] Corrected a typographical error per ECN CH1.1-N-03.0087-4 by GO on 12/8/03.
[36] Revised this section per ECN CH1.1-N-03060 by GO on 10/28/03.

EXHIBIT A

If the BP did not receive Option Code 43 sub-option 101 containing the string 'CableHome 1.1 LAN-Trans' in the DHCP ACK, the BP MUST open the TCP connection for the LAN messaging exchange against the IP address 192.168.0.1.

The BP MUST NOT transmit a BP_Init message more frequently than once per 20 seconds.

The BP MUST NOT transmit a BP_Init message any time other than the specific occasions listed in Section 10.4.1.4.1.1, "BP information to the PS using BP_Init Message," on page 180.

The BP MUST NOT transmit a BP_Init message to any address other than the BP's default gateway address or 192.168.0.1.

The BP MUST close the TCP connection against the PS after a BP_Init_Response message is received.

The BP MUST observe the following SOAP Syntax Rules:

- A SOAP message MUST be encoded using XML.
- A SOAP message MUST have a SOAP Envelope.
- A SOAP message MAY have a SOAP header.
- A SOAP message MUST have a SOAP Body.
- A SOAP message MUST use the SOAP Envelope namespaces.
- A SOAP message MUST use the SOAP Encoding namespace.
- A SOAP message MUST NOT contain a Document Type Declaration (DTD).
- A SOAP message MUST NOT contain XML Processing Instructions.
- The BP MUST use the following default namespaces:
  - for SOAP envelope syntax: http://schemas.xmlsoap.org/soap/envelope/
  - for SOAP encoding and data types: http://schemas.xmlsoap.org/soap/encoding/
  - for 'BP_Init': IP Address of PS

The BP MUST perform the following actions in the order listed when it receives a SOAP message:

1. Identify all parts of the SOAP message intended for the BP.

2. Verify that the received message is formatted as specified in Section 6.3.3.4.4.2.1 and process the message. If the message does not contain all mandatory components, discard the message. The processor has the option to ignore optional parts identified in step 1 without affecting the outcome of the processing.

3. If the message cannot be processed because it is incorrectly formatted, contains an invalid value, or does not conform with the CableHome specification or [SOAP] in some other way, the BP will re-issue the BP_Init message as defined in Section 6.5.3.3.4.

6.5.3.3 MBP Discovery Function

6.5.3.3.1 MBP Discovery Function Goals

The goal for the CableHome MBP Discovery functionality is to provide the CableHome system manager with information about the CableHome Host device in which the BP resides.

EXHIBIT A

6.5.3.3.2 MBP Discovery Function System Design Guidelines

The design guidelines listed in Table 6-27 provided guidance for the specification of the MBP Discovery function.

Table 6-27 — MBP Discovery Function System Design Guidelines

Reference	MBP Discovery System Design Guidelines
MBP Disc 1	The MBP will provide device-specific information about the CableHome Host in which it resides to the cable operator through the PS acting as a proxy.
MBP Disc 2	The MBP will provide information about the applications implemented by a CableHome Host device to the cable operator through the PS acting as a proxy.

6.5.3.3.3 MBP Discovery Function System Description

Each BP is required to implement a Device Profile in XML format as described in Section 6.5.3.1.4 Device Profile in XML Format. Each BP is also required to implement a QoS Profile described in Section 10.3.2.4.2.1 QoS Profile XML Schema. When the BP is operational and has completed initialization, it is required to send Device Profile and QoS Profile information to the PS using LAN Messaging described in Section 6.3.3.4 CMP LAN Messaging Function. By providing the PS with Device Profile and QoS Profile information, the BP enables the cable operator to discover attributes of the CableHome Host device in which the BP resides and the applications running on it, through the PS acting as a proxy for the cable operator's network management system.

6.5.3.3.4 Discovery Function Requirements[37]

Upon receipt of any DHCPACK message [RFC 2131] addressed to itself, the BP MUST transmit as described in Section 6.3.3.4.4.2 a BP_Init message containing its Device Profile and its QoS Profile in the message body. The BP sends BP_Init messages at other times for which the Qos Profile is mandatory (as described in Section 10.4.1.4.1, "LAN Information Exchange). At those times, however, the BP is not required to include the Device Profile.[38]

If the BP cannot establish TCP connectivity with the PS, or if an existing connection is lost, the BP MUST wait 30 seconds and retry to establish the TCP connection. The total number of TCP connection establishment attempts that the BP is allowed to perform in order to complete a BP_Init/BP_Init_Response messages exchange is three. If the third connection fails before a BP_Init_Response is received the BP MUST discard the BP_Init message, and wait until the next DHCPACK [RFC 2131] to repeat the process.

If the BP, having established TCP connectivity with the PS, does not receive a BP_Init_Response message within one minute after the BP_Init message was sent, or within this period receives a BP_Init_Response message that is not properly formatted or contains errors and thus cannot be processed, or receives a BP_Init_Response message that can be processed but that contains a negative Confirmation Code value, it MUST retransmit the BP_Init message repeating the process for a total of three attempts or until the BP receives a valid BP_Init_Response message, whichever occurs first.[39]

If the BP, having established TCP connectivity against the PS, does not receive a valid BP_Init_Response message after sending the BP_Init messages three times, it MUST terminate the TCP connection and wait until it receives the next DHCPACK [RFC 2131] message to repeat the process.

[37] Revised this section per ECN CH1.1-N-03060 by GO on 10/28/03.

[38] Revised this paragraph per ECN CH1.1-N-03.0087-4 by GO on 12/8/03.

[39] Revised this paragraph per ECN CH1.1-N-03.0087-4 by GO on 12/8/03.

EXHIBIT A

7 PROVISIONING TOOLS

7.1 Introduction/Overview

The Portal Services element and LAN IP Devices must be properly initialized and configured in order to exchange meaningful information with one another and with elements connected to the cable network and the Internet. CableHome provisioning tools provide the means for this initialization and configuration to occur seamlessly and with minimum user intervention. They also enable cable operators to add value to high-speed data service subscribers by defining processes through which the cable operator can facilitate and customize PS and LAN IP Device initialization and configuration. The three provisioning tools defined by CableHome to accomplish this task are listed below:

- CableHome DHCP Portal (CDP) function in the Portal Services element
- Bulk Portal Services Configuration (BPSC) tool
- Time of Day Client in the Portal Services element

7.1.1 Goals

Goals of the CableHome 1.1 Provisioning Tools are listed below:

- Enable the PS to acquire a network address on its WAN interface to be used for management of the PS
- Enable the PS to acquire one or more network addresses on its WAN interface to be used for the exchange of traffic between LAN IP Devices and the Internet or between CableHome Host devices and the Internet
- Enable the PS to request and acquire configuration parameters in a configuration file
- Enable the PS to acquire current time of day from time of day services in the cable operator's data network
- Enable the PS to assign network address leases to LAN IP Devices and CableHome Host devices
- Enable the PS to assign configuration parameters to LAN IP Devices and CableHome Host devices

7.1.2 Assumptions

The CableHome Provisioning Tools operating assumptions are listed below:

- LAN IP Devices and CableHome Host devices implement a DHCP client as defined by [RFC 2131].
- The cable network provisioning system implements a DHCP server as defined by [RFC 2131].
- If the cable network provisioning system's DHCP server supports DHCP Option 61 (client identifier option), the WAN-Man and all WAN-Data IP interfaces can share a common MAC address.
- LAN IP Devices and CableHome Host devices may support various DHCP Options and BOOTP Vendor Extensions, allowed by [RFC 2132].
- Bulk PS configuration will be accomplished via the download of a PS Configuration File containing one or more parameters, using Trivial File Transfer Protocol (TFTP) [RFC 1350] or Hypertext Transfer Protocol (HTTP) [RFC 2616] with Transport Layer Security (TLS) [RFC 2246].
- The Headend DHCP server will provide a DHCP option, to the WAN-Management interface, which points to a Time of Day server, operating within the Headend network.

EXHIBIT A

7.2 Provisioning Architecture

7.2.1 Provisioning Modes

Three provisioning modes are supported by CableHome 1.1. They are referred to as DHCP Provisioning Mode (DHCP Mode), SNMP Provisioning Mode (SNMP Mode), and Dormant CableHome Mode. The three provisioning modes are compared in Table 7-1.

Table 7-1 — CableHome 1.1 Provisioning Modes

	DHCP Mode	SNMP Mode	Dormant CableHome Mode
DHCP Fields and Option Codes	Receives configuration file information in 'siaddr' and 'file' fields. Receives no Option 177	Receives no configuration file information. Receives valid values for Option 177 sub-options 3, 6, and 51	Receives no configuration file information and no Option 177, or receives an invalid combination of configuration file information and Option 177 sub-options.
PS Configuration File Trigger	Triggered by presence of TFTP server information in DHCP message	Triggered by NMS via SNMP message	PS receives no configuration file
PS Configuration File Requirement	PS Configuration File download is required	PS Configuration File download is not required	PS configuration file is not required

Specified behavior of the Provisioning Tools is dependent upon the Provisioning Mode in which the PS operates.

Section 13, Provisioning Processes, describes the sequence of events for DHCP and SNMP Provisioning Modes.

7.2.2 Provisioning Architecture Description

The CableHome provisioning architecture is illustrated in Figure 7-1. Portal Services elements will interact with server functions in the cable network over the HFC interface, or with CableHome Host Devices to satisfy the system design guidelines listed in Section 7.3.1.

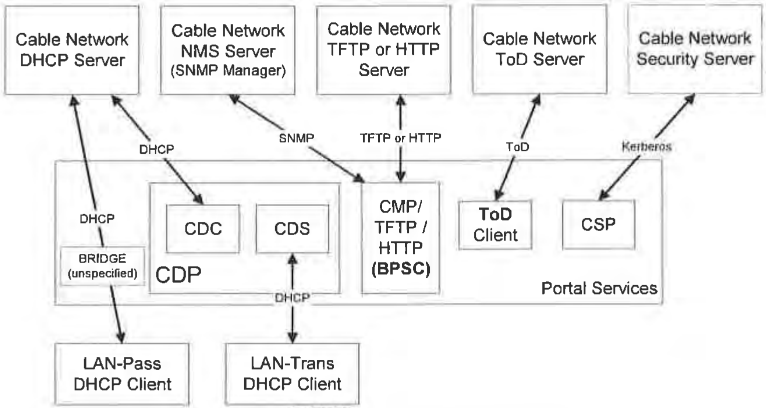


Figure 7-1 — CableHome Provisioning Architecture

EXHIBIT A

7.3 PS Logical Element - CableHome DHCP Portal (CDP)

The CableHome DHCP Portal (CDP) is a logical sub-element of the PS logical element. The CDP has two primary roles: acquisition of network address leases for the PS and assignment of network address leases to LAN IP Devices and CableHome Host devices in the LAN, and is one of the three provisioning tools introduced in Section 7.1. This section describes the Goals, System Design Guidelines, System Description, and Requirements pertaining to the CDP.

7.3.1 CDP Goals

The goals of the CDP include the following:

- Enable client functions in the PS to communicate with corresponding server functions in the cable data network
- Provide the PS with initial configuration parameters, giving it the ability to further configure itself

7.3.2 CDP System Design Guidelines

The following design guidelines drive the capabilities defined for the CDP:

Table 7-2 — CDP System Design Guidelines

Number	CDP System Design Guidelines
CDP 1	CableHome addressing mechanisms will be MSO controlled, and will provide MSO knowledge of and accessibility to CableHome network elements and LAN IP Devices.
CDP 2	CableHome address acquisition and management processes will not require human intervention (assuming that a user/household account has already been established).
CDP 3	CableHome address acquisition and management will be scalable to support the expected increase in the number of LAN IP devices.
CDP 4	It is preferable for LAN IP Device addresses to remain the same after events such as a power cycle or Internet Service Provider switch.
CDP 5	CableHome will provide a mechanism by which the number of LAN IP Devices in the LAN-Trans realm can be monitored and controlled.
CDP 6	In-home communication will continue to work as provisioned during periods of Headend address server outage. Addressing support will be provided for newly added LAN IP Devices and address expirations during remote address server outages.
CDP 7	IP addresses will be conserved when possible (both globally routable addresses and private cable network management addresses).

7.3.3 CableHome DHCP Portal System Description

The CableHome DHCP Portal (CDP) is the logical entity that is responsible for CableHome addressing activities. The CDP address request and address allocation responsibilities within the CableHome environment include:

- IP address assignment, IP address maintenance, and the delivery of configuration parameters (via DHCP) to LAN IP Devices in the LAN-Trans Address Realm.
- Acquisition of a WAN-Man and zero or more WAN-Data IP addresses and associated DHCP configuration parameters for the Portal Services (PS) element.
- Provide information to the CableHome Name Portal (CNP) in support of LAN IP Device host name services.

The PS maintains two hardware addresses, one of which is to be used to acquire an IP address for management purpose, the other could be used for the acquisition of one or more IP address(es) for data. To

EXHIBIT A

prevent hardware address deception, the PS does not allow either of the two hardware addresses to be modified.

The Portal Services element requires an IP Address on the home LAN for its role on the LAN as a router (see Section 8, Packet Handling and Address Translation), DHCP Server (CDS), and DNS Server (see Section 9, Name Resolution). The PS listens on a single LAN-side IP address for each of these functionalities. The PS needs to communicate the IP address for each of these server functionalities to the LAN IP Devices in the DHCP OFFER and ACK option fields. In order to uniquely identify these option values, each of these server addresses are identified by different MIB objects in the PS, which are listed below and in Table 7-2.[40]

Router (default gateway) Address	cabhCdpServerRouter	Option 3
Domain Name Server (DNS) Address	cabhCdpServerDnsAddress	Option 6
Dynamic Host Configuration Server (DHCP) (CDS) Address	cabhCdpServerDhcpAddress	Option 54

The default value of cabhCdpServerRouter is 192.168.0.1. However, the NMS can set cabhCdpServerRouter to a different value.

The value of cabhCdpServerDhcpAddress is always the same as the value of cabhCdpServerRouter and the NMS cannot change its value directly.

The default value of cabhCdpServerDnsAddress is equal to the value of the cabhCdpServerRouter. However, the NMS can change it to a different value (e.g. DNS server in the cable operator's date network) so that a LAN IP Device can direct its DNS queries to a server other than the PS DNS server.

Thus, the PS always listens on the IP address assigned to cabhCdpSeverRouter for its LAN side router, Name Server (DNS), and DHCP server functionality.

As shown in Figure 7-2, the CDP capabilities are embodied by two functional elements residing within the CDP:

- CableHome DHCP Server (CDS)
- CableHome DHCP Client (CDC)

Figure 7-2 also illustrates interaction between the CDP components and the address realms introduced in Section 5. The CDC exchanges DHCP messages with the DHCP server in the cable network (WAN Management address realm) to acquire an IP address and DHCP options for the PS, for management purposes. The CDC could also exchange DHCP messages with the DHCP server in the cable network (WAN Data address realm) to acquire zero (0), or more IP address(es) on behalf of LAN IP Devices in the LAN-Trans realm. The CDS exchanges DHCP messages with LAN IP Devices in the LAN-Trans realm, and assigns private IP addresses, grants leases to, and could provide DHCP options to DHCP clients within those LAN IP Devices.

LAN IP Devices in the LAN-Pass realm receive their IP addresses, leases, and DHCP options directly from the DHCP server in the cable network. The CDP bridges DHCP messages between the DHCP server in the cable network, and LAN IP Devices in the LAN-Pass realm.

[40] Revised this paragraph and the following four paragraphs per ECN CH1.1-N-03.0104-2 by GO on 12/5/03.

EXHIBIT A

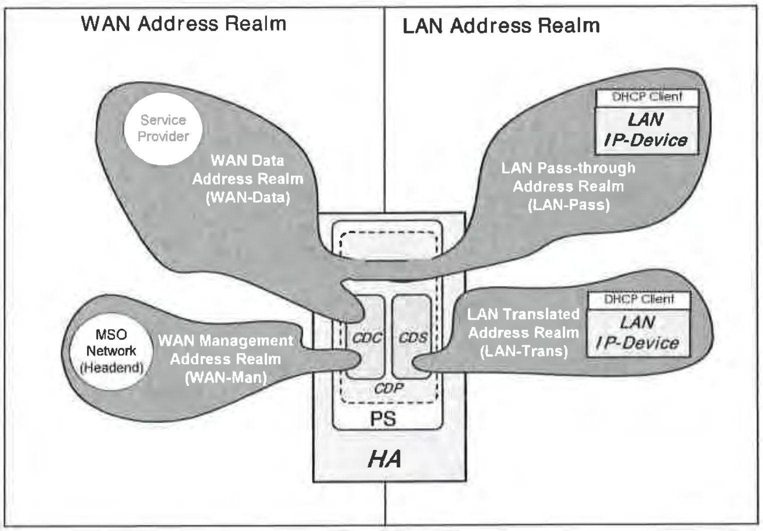

WAN Address Realm
LAN Address Realm
Service Provider
WAN Data Address Realm (WAN-Data)
DHCP Client
LAN IP-Device
LAN Pass-through Address Realm (LAN-Pass)
MSO Network (Headend)
WAN Management Address Realm (WAN-Man)
CDC
CDS
CDP
PS
HA
LAN Translated Address Realm (LAN-Trans)
DHCP Client
LAN IP-Device

Figure 7-2 — CDP Functions

7.3.3.1 CableHome DHCP Server (CDS) Sub-element

The CDS is a sub-element of the CDP logical element of the PS, and is the function responsible for allocating network address leases to LAN IP Devices in the LAN-Trans realm. It is also responsible for providing LAN IP Devices with configuration information via DHCP Option codes, as specified in [RFC 2132]. The CDS is required to perform this function whether or not the PS has an active WAN connection.

7.3.3.1.1 CDS Function Goals

Goals for the CDS Function include the following:

- allocate network address leases to LAN IP Devices in the LAN-Trans realm according to CDP MIB settings and according to [RFC 2131]
- allocate configuration information according to [RFC 2132]
- satisfy CableHome goals for operation in the absence of a WAN connection by allocating LAN-Trans IP address leases and providing configuration information to LAN IP Devices upon request as long as the PS is operational, whether or not the PS has an active WAN connection
- do not allocate IP address leases and do not provide configuration information to LAN IP Devices for which the PS has been configured to treat as existing in the LAN-Pass realm

7.3.3.1.2 CDS Function System Design Guidelines

The design guidelines listed in Table 7-3 guided development of the CDS Function specifications.:

Table 7-3 — CableHome DHCP Server (CDS) Function System Design Guidelines

Number	CDS Function System Design Guidelines
CDS 1	CableHome will provide a means by which LAN IP Devices can acquire network address leases

EXHIBIT A

	and configuration information for the LAN-Trans realm.
CDS 2	The mechanism for allocating LAN-Trans IP addresses and configuration information will operate whether the PS has a WAN connection to the cable operator's data network or not.
CDS 3	The mechanism for allocating LAN-Trans IP address leases and configuration information will not allocate IP address leases or provide configuration information for LAN IP Devices in the LAN-Pass realm.

7.3.3.1.3 CDS Function System Description

The CDS is a standard DHCP server as defined in [RFC 2132], and responsibilities include:

- The CDS assigns addresses to and delivers DHCP configuration parameters to LAN IP Devices receiving an address in the LAN-Trans address realm. The CDS learns DHCP options from the NMS system and provides these DHCP options to LAN IP Devices. If DHCP options have not been provided by the NMS system (for example when the PS boots during a cable outage), the CDS relies on built-in default values (DefVals) for required options.
- The CDS is able to provide DHCP addressing services to LAN IP Devices, independent of the WAN connectivity state.
- The number of addresses supplied by the CDS to LAN IP Devices is controllable by the NMS system. The behavior of the CDS when a cable operator settable limit is exceeded is also configurable via the NMS. Possible CDS actions when the limit is exceeded include: (1) assign a LAN-Trans IP address and treat the WAN to LAN CAT interconnection as would normally occur if the limit had not been exceeded; and (2) do not assign an address to requesting LAN IP devices. An address threshold setting of 0 indicates the maximum threshold possible for the LAN-Trans IP address pool defined by the pool "start" (cabhCdpLanPoolStart) and "end" (cabhCdpLanPoolEnd) values.
- In the absence of time of day information from the Time of Day (ToD) server, the CDS uses the PS default starting time of 00:00.0 (midnight) GMT, January 1, 1970, updates the Expire Time for any active leases in the LAN-Trans realm to re-synchronize with DHCP clients in LAN IP Devices, and maintains leases based on that starting point until the PS synchronizes with the Time of Day server in the cable network.
- During the PS Boot process, the CDS remains inactive until activated by the PS.
- If the PS Primary Packet-handling mode (cabhCapPrimaryMode) has been set to Passthrough and the PS provisioning process has completed (as indicated by cabhPsDevProvState = pass(1)), then the CDS is disabled.

LAN IP Devices may receive addresses that reside in the LAN-Pass realm. As shown in Figure 7-2, LAN-Pass address requests are served by the WAN addressing infrastructure, not the PS. LAN-Pass addressing processes will occur when the PS is configured to operate in Passthrough Mode or Mixed Bridging/Routing Mode (see Section 8.3.4.3 Passthrough Requirements for more details). In these cases, DHCP interactions will take place directly between LAN IP Devices and cable data network servers, and CableHome does not specify the process.

Throughout this document, the terms Dynamic Allocation and Manual Allocation are used as defined in [RFC 2132]. The CDS Provisioned DHCP Options, cabhCdpServer objects in the CDP MIB, are DHCP Options that can be provisioned by the NMS, and are offered by the CDS to LAN IP devices assigned a LAN-Trans address. CDS Provisioned DHCP Options, cabhCdpServer objects, persist after a PS power cycle and the NMS system can establish, read, write and delete these objects. CDS Provisioned DHCP Options, cabhCdpServer objects, are retained during periods of cable outage and these objects are offered to LAN IP devices assigned a LAN-Trans address during periods of cable outage. The CDS persistent storage of DHCP options is consistent with [RFC 2132], Section 2.1. The default values of CDS Provisioned DHCP Options, cabhCdpServer objects, are defined (Table 7-4) and the NMS can reset the CDS Provisioned DHCP Options, cabhCdpServer objects, and cabhCdpLanAddrTable to their default values, by writing to the cabhCdpSetToFactory MIB object.

EXHIBIT A

The CDS Address Threshold (cabhCdpLanTrans) objects contain the event control parameters used by the CDS to signal the CMP to generate a notification to the Headend management system, when the number of LAN-Trans addresses assigned by the CDS exceeds the preset threshold.

The Address Count (cabhCdpLanTransCurCount) object is a value indicating the number of LAN-Trans addresses assigned by the CDS that have active DHCP leases.

The Address Threshold (cabhCdpLanTransThreshold) object is a value indicating when a notification is generated to the Headend management system. The notification is generated when the CDS assigns an address to the LAN IP Device that causes the Address Count (cabhCdpLanTransCurCount) to exceed the Address Threshold (cabhCdpLanTransThreshold).

The Threshold Exceeded Action (cabhCdpLanTransAction) is the action taken by the CDS while the Address Count (cabhCdpLanTransCurCount) exceeds the Address Threshold (cabhCdpLanTransThreshold). If the Threshold Exceeded Action (cabhCdpLanTransAction) allows address assignments after the count is exceeded, the notification is generated each time an address is assigned. The defined actions are a) assign a LAN-Trans address as normal, and b) do not assign an address to the next requesting LAN IP Device.

The Address Count (cabhCdpLanTransCurCount) continues to be updated during periods of cable outage.

The CDS MIB also contains the Address Pool Start (cabhCdpLanPoolStart) and Address Pool End (cabhCdpLanPoolEnd) parameters. These parameters indicate the range of addresses in the LAN-Trans realm that can be assigned by the CDS to LAN IP Devices.

The CDP LAN Address Table (cabhCdpLanAddrTable) contains the list of parameters associated with addresses allocated to LAN IP Devices with LAN-Trans addresses. These parameters include:

- The Client Identifiers , [RFC 2132], Section 9.14 (cabhCdpLanAddrClientID)
- The LAN IP address assigned to the client (cabhCdpLanAddrIp)
- An indication that the address was allocated either manually (via the CMP) or dynamically (via the CDP) (cabhCdpLanAddrMethod)

The CDS stores LAN IP Device identifying information in the cabhCdpLanAddrClientID MIB object. The CDS uses the value passed in the chaddr field of the DHCP REQUEST message sent by the LAN IP Device for this purpose.

The CDS creates a CDP Table (cabhCdpLanAddrTable) entry when it allocates an IP address to a LAN IP Device. The CDS can create CDP Table (cabhCdpLanAddrTable) entries during periods of cable outage.

The CDP Table (cabhCdpLanAddrTable) maintains a DHCP lease time for each LAN IP Device.

NMS-provisioned CDP Table (cabhCdpLanAddrTable) entries are retained during periods of cable outage and persist across a PS power-cycle.

7.3.3.1.4 CDS Function Requirements

The PS MUST comply with the Server requirements of [RFC 2131], section 4.3.

The PS MUST support Dynamic and Manual address allocation in accordance with [RFC 2131], section 1.

PS Manual IP address allocation MUST be supported using CDP MIB's cabhCdpLanAddrTable entries created via the NMS system or PS Configuration file.

EXHIBIT A

In support of Dynamic IP address allocation, the PS MUST be capable of creating, modifying and deleting cabhCdpLanAddrTable entries for devices allocated a LAN-Trans address.

The PS MUST retain Provisioned CDP LAN Address Management Table (cabhCdpLanAddrTable) entries during a cable outage and the entries MUST persist after a PS power cycle. The PS MUST be able to provide DHCP addressing services to LAN IP Devices when enabled by the PS, independent of the WAN connectivity state.

Upon PS reset or re-boot, the PS MUST NOT exchange DHCP messages with LAN IP Devices until the CDS is activated by the PS.

The PS MUST activate the CDS, i.e., the PS MUST begin responding to DHCP DISCOVER and DHCP REQUEST messages received through any PS LAN Interface, in any of the following conditions (see also Figure 13-2 CableHome Provisioning Modes):

- When the PS is operating in DHCP provisioning mode, after the CDC has received a PS WAN-Man IP address lease and the PS has received and properly processed a PS configuration file
- When the PS is operating in SNMP provisioning mode, after the CDC has received a PS WAN-Man IP address lease, has authenticated with the Key Distribution Center (KDC) server, and has successfully enrolled with the NMS
- When the first CDC attempt to acquire a PS WAN-Man IP address lease fails
- When the PS is operating in DHCP provisioning mode and the first attempt to download or to process the PS configuration file fails
- When the PS is operating in SNMP provisioning mode and the attempt to authenticate with the KDC server fails
- When the PS is operating in SNMP provisioning mode and is triggered to download a PS configuration file before CDS operation is initiated, and the first attempt to download or to process the PS configuration file fails

The PS MUST assign a unique, available IP address from the range of addresses beginning with cabhCdpLanPoolStart and ending with cabhCdpLanPoolEnd, to each LAN-IP Device in the LAN-Trans realm that requests an IP address using DHCP, if the number of IP addresses already assigned by the CDS is less than the value of cabhCdpLanTransThreshold.

If the value of cabhCdpLanTransThreshold is 0, the PS MUST treat the threshold as if it has been assigned the largest value possible for the current LAN-Trans IP address pool size (as defined by the LAN-Trans IP address pool start (cabhCdpLanPoolStart) and end (cabhCdpLanPoolEnd) values).

The PS MUST maintain the Address Count parameter (cabhCdpLanTransCurCount) indicating the number of active LAN-Trans address leases granted to LAN IP devices.

The PS MUST increase the Address Count each time a lease for a LAN-Trans address is granted to a LAN IP Device and MUST decrease the Address Count each time a LAN-Trans address is released or a LAN-Trans address lease expires.

The PS MUST compare the Address Count parameter (cabhCdpLanTransCurCount) to the Address Threshold parameter (cabhCdpLanTransThreshold) after assigning a LAN-Trans address. If the Address Count parameter (cabhCdpLanTransCurCount) exceeds the Address Threshold parameter (cabhCdpLanTransThreshold), the PS MUST generate a notification in accordance with the event reporting mechanism defined in Section 6.3.3.2 CMP Event Reporting Function and Appendix II. While the Address Count parameter (cabhCdpLanTransCurCount) exceeds the Address Threshold parameter (cabhCdpLanTransThreshold), the PS MUST be capable of the following threshold exceeded actions for the next DHCP DISCOVER from the LAN: assign a LAN-Trans addresses as normal or do not assign an address.

EXHIBIT A

If cabhCdpLanTranCurCount equals or exceeds cabhCdpLanTransThreshold and a LAN IP Device requests and additional IP address lease, the PS MUST take specific action as indicated by the Threshold Exceeded Action (cabhCdpLanTransAction) provisioned parameter.

The PS MUST assign IP addresses and deliver DHCP configuration parameters listed in Table 7-4 for which the CDS has a valid value, only to LAN IP Devices receiving an address in the LAN-Trans address realm.

If the cable operator provisions values for a row in the cabhCdpLanAddrTable, the PS (CDS) MUST offer a lease for (i.e., attempt to assign) the provisioned cabhCdpLanAddrIp IP address, to the LAN IP Device whose hardware address corresponds to the provisioned cabhCdpLanAddrClientID, in response to a DHCP DISCOVER received from that LAN IP Device.

When the CDS assigns an active lease for an IP address to a LAN IP Device, the PS MUST remove that address from the pool of IP addresses available for assignment to LAN IP Devices.

If the CDS receives a lease request from a LAN IP device that it cannot satisfy due to the unavailability of addresses from the IP address pool (defined by cabhCdpLanPoolStart and CabhCdpLanPoolEnd), the PS MUST notify the event in accordance to Appendix II and the event reporting mechanism defined in Section 6.3.3.2 CMP Event Reporting Function.

The PS MUST store the value passed in the chaddr field of the DHCP REQUEST message sent by the LAN IP Device when an active lease is created for the LAN IP Device.

The PS MUST support all CableHome CDP MIB objects, including all objects in the cabhCdpLanAddrTable, cabhCdpLanPool objects, cabhCdpServer objects, and cabhCdpLanTrans objects.

The CDS function of the PS MUST support the DHCP options indicated as mandatory in the CDS Protocol Support column of Table 7-4 CDS DHCP Options.

The CDS MUST include in DHCP OFFER and DHCP ACK messages it sends to its DHCP clients, the DHCP option code 43 sub-option 101 containing the string "CableHome1.1LAN-Trans" (with no spaces and without the quotation marks) as the sub-option information, only in response to DHCP DISCOVER and DHCP REQUEST messages that include DHCP option code 60 containing the string value "CableHome1.1BP" (with no spaces and without the quotation marks).[41]

The CDS MUST NOT include DHCP option code 43 sub-option 101 in the DHCP OFFER and DHCP ACK messages it sends to any DHCP client that did not provide the string value "*CableHome1.1BP*" in DHCP option code 60, in its DHCP DISCOVER and DHCP REQUEST messages.

The CDS function of the PS MUST support offering the default values indicated in the CDS Factory Defaults column of Table 7-4 CDS DHCP Options, if the DHCP option has not been provisioned with other values.

If the PS Primary Packet-handling mode (cabhCapPrimaryMode) has been set to Passthrough and the PS provisioning process has completed (as indicated b cabhPsDevProvState = pass(1)), then the CDS function of the PS MUST be disabled.

The CDS function of the PS MUST NOT respond to DHCP messages that are received through any WAN Interface, nor originate DHCP messages from any WAN Interface.

The CDS function of the PS MUST NOT deliver any DHCP option with null value to any LAN IP Device.

[41] Revised this paragraph per ECN CH1.1-N-03069 by GO on 10/28/03.

EXHIBIT A

The CDS MUST NOT offer a lease for IP address 192.168.0.1, i.e., the CDS MUST NOT transmit a DHCP offer or DHCP Ack message with the value 192.168.0.1 in the yiaddr field.[42]

Table 7-4 — CDS DHCP Options

Option Number	Option Function	CDS Protocol Support (M)andatory or (O)ptional	CDS Factory Defaults	MIB Object Name
0	Pad	M	N/A	N/A
255	End	M	N/A	N/A
1	Subnet Mask	M	255.255.255.0	cabhCdpServerSubnetMask
2	Time Offset	M	0	cabhCdpServerTimeOffset
3	Router Option	M	192.168.0.1	cabhCdpServerRouter
6	Domain Name Server	M	192.168.0.1	cabhCdpServerDnsAddress
7	Log Server	M	0.0.0.0	cabhCdpServerSyslogAddress
12	Host Name	M	N/A	N/A
15	Domain Name	M	Null String	cabhCdpServerDomainName
23	Default Time-to-live	M	64	cabhCdpServerTTL
26	Interface MTU	M	N/A	cabhCdpServerInterfaceMTU
43	Vendor Specific Information	M	Vendor Selected	cabhCdpServerVendorSpecific
43.101	Vendor Specific Information sub-option 101	M[1]	String: "CableHome 1.1LAN-Trans" (with no spaces)	N/A
50	Requested IP Address	M	N/A	N/A
51	IP Address Lease Time	M	3600 seconds	cabhCdpServerLeaseTime
54	Server Identifier	M	192.168.0.1	cabhCdpServerDhcpAddress
55	Parameter Request List	M	N/A	N/A
60	Vendor Class Identifier	M	N/A	N/A
61	Client-identifier	O	N/A	N/A

1. The CDS is required to include DHCP option code 43 sub-option 101 containing the string CableHome1.1LAN-Trans, with no spaces, in the DHCP OFFER and DHCP ACK messages it sends to CableHome compliant LAN IP Devices only. CableHome compliance of LAN IP Devices is indicated by the presence of the string CableHome1.1BP in the DHCP DISCOVER and DHCP REQUEST messages.

7.3.3.2 CDP CableHome DHCP Client (CDC) Function

7.3.3.2.1 CDC Function Goals

The goals of the CDP CDC Function include the following:

- acquire an IP address lease for the PS IP stack, used for management messaging and file transfer between the cable operator's network servers and the PS
- acquire configuration information from the cable operator's network DHCP server
- determine the Provisioning Mode in which the PS is to operate
- acquire one or more IP address lease(s) for mapping to LAN IP Devices in the LAN-Trans realm

[42] Revised Table 7-4 per ECN CH1.1-N-03069 by GO on 10/28/03.

EXHIBIT A

7.3.3.2.2 CDC Function System Design Guidelines

The guidelines listed in Table 7-5 were used to guide specification of the CDC function:

Table 7-5 — CableHome DHCP Client (CDC) Function System Design Guidelines

Number	CDC Function System Design Guidelines
CDC 1	CableHome will provide a means by which the PS can acquire a network address lease and configuration information for its WAN-Man interface.
CDC 2	CableHome will provide a means by which the PS can acquire one or more network address leases and configuration information for its WAN-Data interface.
CDC 3	The mechanism for allocating LAN-Trans IP address leases and configuration information will not allocate IP address leases or provide configuration information for LAN IP Devices in the LAN-Pass realm.

7.3.3.2.3 CDC Function System Description

The CDC is a standard DHCP client as defined in [RFC 2131], and responsibilities include:

- The CDC makes requests to Headend DHCP servers for the acquisition of addresses in the WAN-Man and may make requests to Headend DHCP servers for the acquisition of addresses in the WAN-Data address realms. The CDC also understands and acts upon a number of CableHome DHCP configuration parameters.
- The CDC makes a determination about which Provisioning Mode the PS is to operate in, based on information received in the DHCP ACKNOWLEDGE message from its DHCP server.
- The CDC supports acquisition of one WAN-Man IP address and zero or more WAN-Data IP addresses.
- The CDC supports the Vendor Class Identifier Option (DHCP option 60), the Vendor Specific Information option (DHCP Option 43), and the Client Identifier Option (DHCP option 61).
- In the default case, the CDC will acquire a single IP address for simultaneous use by the WAN-Man and WAN-Data IP interfaces. In order to minimize changes needed to existing Headend DHCP servers, the use of a Client Identifier (DHCP option 61) by the CDC is not required in this default case.

The CDP supports various DHCP Options and BOOTP Vendor Extensions, allowed by [RFC 2132].

The CDC determines the provisioning mode in which the PS is to operate based upon information received from the DHCP server in the DHCP ACK message, as introduced in Section 5.5 CableHome Operational Models.

DHCP Provisioning Mode of Operation:

The PS operates in DHCP provisioning mode if it receives a valid file name for the PS Configuration File in the *file* field and a valid IP address in the *siaddr* field of the DHCPACK message, and *does not* receive DHCP option 177 sub-options 3, 6, or 51.

Behavior of the PS when operating in DHCP Provisioning Mode is summarized below:

- requires a PS configuration file to be downloaded from a cable network file server
- defaults to using SNMPv1 and SNMPv2c for management messaging
- defaults to using the docsDevNmAccessTable of the DOCSIS Device MIB [RFC 2669] to control access to the PS Database via CableHome-specified MIBs
- can be configured to use Transport Layer Security (TLS) [RFC 2246] to authenticate and encrypt the PS Configuration File (ref.: Section 11.9 PS Configuration File Security in DHCP Provisioning Mode)

EXHIBIT A

- can be configured to operate in SNMPv3 Coexistence Mode, using Diffie-Hellman key management [RFC 2786], (ref.: Section 6.3.3.1.4.2.2)

SNMP Provisioning Mode of Operation:

The PS operates in SNMP provisioning mode if it receives DHCP option 177 with sub-option fields 3, 6, and 51, *does not* receive a valid file name in the *file* field and *does not* receive a valid IP address in the *siaddr* field of the DHCPACK message.

Behavior of the PS when operating in SNMP Provisioning Mode is summarized below:

- is not required to download a PS configuration file from the cable network file server. The PS can be triggered to download a PS configuration file at any time but will operate using factory default parameters without downloading a PS configuration file
- defaults to operating in SNMPv3 Coexistence Mode with SNMPv1 and SNMPv2 support *not* enabled (ref.: Section 11.4 Secure Management Messaging to the PS)
- defaults to using the User-based Security Model of SNMPv3 [RFC 3414] and View-based Access Control Model of SNMPv3 [RFC 3415] to control access to the PS Database via CableHome-specified MIBs (ref.: Section 11.4)
- uses Kerberos message exchanges with a Key Distribution Center server whose IP address is provided to the PS in DHCP Option 177 sub-option 51, and AP listener to authenticate SNMPv3 messages (ref.: Section 11.4.4.2 Security Algorithms for SNMPv3 in SNMP Provisioning Mode)
- can be configured to receive and process SNMPv1 and SNMPv2c messages as well as SNMPv3 messages

Dormant CableHome Mode:

The PS operates in Dormant CableHome Mode if it receives neither the combination of *file* field, *siaddr* field, or DHCP option code 177 sub-options to configure it for DHCP Provisioning Mode, nor the combination of these fields and sub-options to configure it for SNMP Provisioning Mode.

When the PS is operating in Dormant CableHome Mode, its behavior is required to be as described in Section 7.3.3.2.4, including the following. This mode of operation is designed to enable the PS to operate and perform residential gateway functions when connected to a cable data network that does not yet support CableHome provisioning and management systems:

- reject any SNMP messages received through any WAN interface
- disable the TFTP client function
- disable SYSLOG event reporting
- terminate the provisioning timer
- enable CNP, CAP, USFS, and CDS functionality

The PS is required to include certain DHCP option fields in DHCP DISCOVER and DHCP REQUEST messages it issues to cable network DHCP servers. The Vendor Class Identifier Option (DHCP option 60) defines a CableLabs device class. For CableHome 1.1 the Vendor Class Identifier Option will contain the string "CableHome1.1", to identify a CableHome 1.1-compliant Portal Services (PS) logical element, whenever the CDC requests a WAN-Man or WAN-Data address.

The Vendor Specific Information option (DHCP Option 43) further identifies the type of device and its capabilities. It describes the type of component that is making the request (embedded or standalone, CM or

EXHIBIT A

PS), the components that are contained in the device (CM, MTA, PS, etc.), the device serial number, and also allows device specific parameters. DHCP option 43 and its suboptions are defined in Section 7.2.3.3.[43]

Details of the requirements for supporting DHCP options 60 and 43 are in Table 7-6 and Table 7-7. Details related to other optional and mandatory DHCP options are provided in Table 7-8.

The WAN-Data IP Address count parameter of the CDP MIB (cabhCdpWanDataIpAddrCount) is the number of IP address leases the CDC is required to attempt to acquire for the WAN side of NAT and NAPT mappings. The default value of cabhCdpWanDataIpAddrCount is zero, which means that, by default, the CDC will acquire only a WAN-Man IP address.

7.3.3.2.3.1 CableHome DHCP Client Option 61

The CableHome PS element can have one or more WAN IP addresses associated with a one or more link layer (e.g. MAC) interfaces. Therefore, the CDC cannot rely solely on a MAC address as a unique client identifier value.

CableHome allows for the use of the Client Identifier Option (DHCP option 61), [RFC 2132] section 9.14, to uniquely identify the logical WAN interface associated with a particular IP address.

The PS is required to have two hardware addresses: one to be used to uniquely identify the logical WAN interface associated with the WAN-Man IP address (WAN-Man hardware address) and the other to be used to uniquely identify the logical WAN interface associated with WAN-Data IP addresses (WAN-Data hardware address).

7.3.3.2.3.2 WAN Address Modes

In order to enable compatibility with as many cable operator provisioning systems as possible, the CDC will support the following configurable WAN Address Modes:

WAN Address Mode 0:

The PS Element makes use of a single WAN IP Address, acquired via DHCP using the WAN-Man hardware address. The PS Element has one WAN-Man IP Interface and zero WAN-Data IP Interfaces. This Address Mode is only applicable when the PS Primary Packet-handling Mode (cabhCapPrimaryMode) is set to Passthrough (refer to Section 8.3.2). The cable operator's Headend DHCP server typically needs no software modifications to support this Address Mode. In WAN Address Mode 0, the value of cabhCdpWanDataIpAddrCount is zero.

WAN Address Mode 1:

The PS Element makes use of a single WAN IP Address, acquired via DHCP using the WAN-Man hardware address. The PS Element has one WAN-Man IP Interface and one WAN-Data IP Interface. These two Interfaces share a single, common IP address. This Address Mode is only applicable when the PS Primary Packet-handling Mode (cabhCapPrimaryMode) is set to NAPT. The cable operator's Headend DHCP server typically needs no software modifications to support this Address Mode. In WAN Address Mode 1, the value of cabhCdpWanDataIpAddrCount is zero.

WAN Address Mode 2:

The PS Element acquires a WAN-Man IP address using the unique WAN-Man hardware address, and is subsequently configured by the NMS to request one or more unique WAN-Data IP Address(es). The PS Element will have one WAN-Man and one or more WAN-Data IP Interface(s). All WAN-Data IP

[43] Added the last sentence in this paragraph per ECN CH1.1-N-03044, by GO on 10/27/03.

EXHIBIT A

addresses will share a common hardware address that is unique from the WAN-Man hardware address. The two or more Interfaces (one WAN-Man and one or more WAN-Data) each has its own, unshared IP address. The CDP is configured by the cable operator to operate in WAN Address Mode 2 by writing a nonzero value to cabhCdpWanDataIpAddrCount, via the PS Configuration File or an SNMP set-request. This Address Mode is applicable when the PS Primary Packet-handling Mode (cabhCapPrimaryMode) is set to NAPT or NAT. The cable operator's Headend DHCP server might need software modification to include support for Client IDs (DHCP Option 61) so that it can assign multiple IP addresses to the single WAN-Data hardware address.

There are four potential scenarios for WAN-Data IP addresses:

1. The PS is configured to request zero WAN-Data IP addresses. No WAN-Data Client IDs are needed.

2. The PS is configured to request one or more WAN-Data IP addresses and there are no MSO-configured cabhCdpWanDataAddrClientId entries in the CDP MIB. The PS is required to auto-generate as many unique WAN-Data Client IDs as the value of cabhCdpWanDataIpAddrCount.

3. The PS is configured to request one or more WAN-Data IP addresses and there are at least as many MSO-configured cabhCdpWanDataAddrClientId entries as the value of cabhCdpWanDataIpAddrCount, i.e., the MSO has provisioned enough WAN-Data Client ID values. The PS does not auto-generate any Client IDs.

4. The PS is configured to request one or more WAN-Data IP addresses and there are fewer MSO-configured cabhCdpWanDataAddrClientId entries than the value of cabhCdpWanDataIpAddrCount, i.e., the MSO has provisioned some but not provisioned enough WAN-Data Client ID values. The PS is required to auto-generate enough additional unique WAN-Data Client IDs to bring the total number of unique WAN-Data Client IDs to the value of cabhCdpWanDataIpAddrCount.

If the cable operator desires for the PS to acquire one or more WAN-Data IP addresses, that are distinct from the WAN-Man IP address, the procedure is as follows:

For all WAN Address Modes, the PS first requests a WAN-Man IP address using the WAN-Man hardware address.

The procedure described below assumes the PS has already acquired a WAN-Man IP address:

1. The cable operator optionally provisions the PS with unique specific Client IDs, by writing values to the cabhCdpWanDataAddrClientId entries of the CDP MIB's cabhCdpWanDataAddrTable, via the PS Configuration File or SNMP set-request message(s).

2. The cable operator configures the CDP to operate in WAN Address Mode 2 by writing cabhCdpWanDataIpAddrCount to a nonzero value through the PS Configuration File or SNMP set-request message.

3. After the CDP has been configured to operate in WAN Address Mode 2 as described in step 2), the PS checks to see if Client ID values have been provisioned by the NMS as described in step 1). If a number of Client ID values greater than or equal to the value of cabhCdpWanDataIpAddrCount have been provisioned, the PS uses these values in DHCP Option 61 when requesting the WAN-Data IP address(es). If Client ID values have not been provisioned, i.e., if the cabhCdpWanDataAddrClientId entries do not exist, or if the number of Client ID values provisioned is less than the value of cabhCdpWanDataIpAddrCount, the PS generates a number of unique Client ID values such that in combination with the provisioned Client IDs, the total number of unique Client IDs equals the value of cabhCdpWanDataIpAddrCount. The PS generates Client ID values by using the WAN-Data hardware

EXHIBIT A

address alone for the first requested WAN-Data IP address, and by concatenating the WAN-Data hardware address with a count that is 8 bits in length for the second and all subsequent WAN-Data IP addresses. If no Client IDs have been provisioned by the NMS, the first 8-bit count value is 0x02 (indicating the second requested WAN-Data IP address), the second count value is 0x03, and so on.

Example for the case when no Client IDs have been provisioned by the NMS:

Given WAN-Data hardware address 0xCDCDCDCDCDCD

PS-generated Client ID for the first requested WAN-Data IP address: 0xCDCDCDCDCDCD

PS-generated Client ID for the second requested WAN-Data IP address: 0xCDCDCDCDCDCD02

PS-generated Client ID for the third requested WAN-Data IP address: 0xCDCDCDCDCDCD03

PS-generated Client ID for the nth requested WAN-Data IP address: 0xCDCDCDCDCDCDn (n=<0xFF)

If some Client IDs have been provisioned by the NMS but the number is less than the value of cabhCdpWanDataIpAddrCount, the PS generates additional Client IDs as needed to bring the total number of Client IDs to the value of cabhCdpWanDataIpAddrCount. The PS will generate these additional Client IDs values by appending an 8-bit count value to the WAN-Data hardware address, starting with 0x02, unless that would duplicate a provisioned Client ID. If the Client IDs provisioned by the NMS follow the same format (hardware address with 8-bit count value), the PS is required to use a unique count value so as to not duplicate a provisioned Client ID.

Example for the case when Client IDs have been provisioned by the NMS (three provisioned Client ID values, cabhCdpWanDataIpAddrCount = 5):

Given WAN-Data hardware address 0xCDCDCDCDCDCD

First provisioned Client ID for the first WAN-Data IP address: 0x0A0A0A0A0A1A

Second provisioned Client ID for the second WAN-Data IP address: 0x0A0A0A0A0A2A

Third provisioned Client ID for the third WAN-Data IP address: 0x0A0A0A0A0A3A

First Client ID generated by the PS for the fourth requested WAN-Data IP address: 0xCDCDCDCDCDCD02

Second Client ID generated by the PS for the fifth requested WAN-Data IP address: 0xCDCDCDCDCDCD03

4. The PS adds the Client ID values it generates as cabhCdpWanDataAddrClientId entries to the end of the cabhCdpWanDataAddrTable.

5. The PS (CDC) requests (repeating the DHCP DISCOVER process as needed) as many unique WAN-Data IP addresses as the value of cabhCdpWanDataIpAddrCount specifies, using the WAN-Data hardware address in the chaddr field of the DHCP message and the Client ID value(s) from step 3) in DHCP Option 61, beginning with the first cabhCdpWanDataAddrClientId entry of the cabhCdpWanDataAddrTable. The CDC is not permitted to request more WAN-Data IP addresses than the value of cabhCdpWanDataIpAddrCount, even if the number of provisioned Client IDs is greater than the value of cabhCdpWanDataAddrTable.

EXHIBIT A

7.3.3.2.4 CDC Requirements[44]

The PS MUST implement a DHCP client function in accordance with the Client requirements of [RFC 2131].

In both the Embedded and Standalone configurations, the PS MUST implement two unique WAN hardware addresses: the PS WAN-Man hardware address and the PS WAN-Data hardware address. The numerical value of the PS WAN-Data hardware address MUST follow sequentially the numerical value of the PS WAN-Man hardware address. The PS WAN-Man and PS WAN-Data hardware addresses MUST persist once they are set at the factory. The PS MUST NOT permit the modification of its factory-set PS WAN-Man and PS WAN-Data hardware addresses.

In both the Embedded PS and Standalone PS cases, the PS element MUST have WAN interface hardware addresses that are distinct from the cable modem's hardware address.

The PS MUST broadcast DHCP DISCOVER in accordance with client requirements of [RFC 2131] and attempt to acquire a PS WAN-Man IP address lease during the PS boot process.

The PS MUST set cabhPsDevProvState to inProgress (2) when the PS broadcasts the DHCP DISCOVER message the first time following device reboot or PS reset. The PS ignores DHCP header fields and options used to determine Provisioning Mode and is not required to set cabhPsDevProvState to inProgress(2) when renewing its IP address lease via DHCP.[45]

As a result of the process of renewing its IP address lease, the PS sets the Provisioning State object (cabhPsDevProvState) to the value pass(1) or to the value fail(2). When it renews its WAN-Man or WAN-Data IP address lease(s), the PS MUST update its system time and related MIB objects (cabhPsDevDateTime) based on the value of DHCP Option 2 (Time Offset) of the DHCP ACK message. When it renews its WAN-Man or WAN-Data IP address lease(s), the PS MUST update its lease information, including updating the values of cabhCdpWanDataAddrLeaseCreateTime and cabhCdpWanDataAddrLeaseExpireTime as appropriate, based on the value of DHCP Option 51 (IP Address Lease Time). When it renews its WAN-Man or WAN-Data IP address lease(s), the PS MUST ignore DHCP Option 177 sub-options 3, 6, and 51, and DHCP header file and siaddr fields.[46]

The PS MUST use the PS WAN-Man hardware address in the *chaddr* field and in DHCP Option 61, in the DHCP DISCOVER and DHCP REQUEST messages, when requesting a WAN-Man IP address from the Headend DHCP server.

If the value of cabhCdpWanDataIpAddrCount is zero, the PS MUST use the WAN-Man IP Address for the WAN-Man and WAN-Data Interfaces.

If the value of cabhCdpWanDataIpAddrCount is greater than zero, the PS MUST request the same number of unique WAN-Data IP address(es) from the Headend DHCP server as the value of cabhCdpWanDataIpAddrCount.

The PS (CDC) MUST NOT attempt to acquire more WAN-Data IP addresses than the value of cabhCdpWanDataIpAddrCount.

The PS MUST use a unique cabhCdpWanDataAddrClientId in DHCP Option 61 for each WAN-Data IP address requested from the Headend DHCP server.

[44] Deleted the sentence referring to TFPT client functions per ECN CH1.1-N-03.0099-3 by GO on 12/10/03.
[45] Replaced this paragraph per ECN CH1.1-N-03046; superseded by CH1.1-N-03.0099-3 by GO on 12/10/03.
[46] Added this paragraph per ECN CH1.1-N-03.0099-3 by GO on 12/10/03.

EXHIBIT A

The PS MUST use the WAN-Data hardware address as the value in the DHCP message *chaddr* field for each WAN-Data IP address requested from the Headend DHCP server.

When the PS (CDC) requests WAN-Data IP addresses from the Headend DHCP server, the PS MUST use cabhCdpWanDataAddrClientId entries for DHCP Option 61 in the order the entries appear in the cabhCdpWanDataAddrTable, beginning with the first entry.

If a nonzero value is configured for cabhCdpWanDataIpAddrCount, and if the number of cabhCdpWanDataAddrClientId entries is less than the value of cabhCdpWanDataIpAddrCount, the PS MUST generate as many unique WAN-Data Client IDs as needed to bring the total number of cabhCdpWanDataAddrClientId entries to the value of cabhCdpWanDataIpAddrCount, and add each generated entry to the end of the cabhCdpWanDataAddrTable.

If the PS generates WAN-Data Client IDs, the first cabhCdpWanDataAddrClientId entry of the cabhCdpWanDataAddrTable MUST be the WAN-Data hardware address.

If the PS generates WAN-Data Client IDs, any cabhCdpWanDataAddrClientId entry generated by the PS other than the first entry of the cabhCdpWanDataAddrTable MUST be the WAN-Data hardware address with an 8-bit count value appended to the end, beginning with 0x02, unless that value already exists as a cabhCdpWanDataAddrClientId entry, in which case the PS MUST generate the Client ID as the WAN-Data hardware address appended with the next available 8-bit count value.[47]

The PS MUST implement the Vendor Specific Information Option (DHCP option 43) as specified in Table 7-7 and Table 7-8. Details of DHCP option 43 and its suboptions for CableHome 1.1 are further defined below. The definitions of DHCP Option 43 suboptions MUST conform to requirements imposed by [RFC 2132].[48]

The option begins with a type octet with the value of number 43, followed by a length octet. The length octet is followed by the number of octets of data equal to the value of the length octet. The value of the length octet does not include the two octets specifying the tag and length.

DHCP option 43 in CableHome 1.1 is a compound option. The content of option 43 is composed of one or more suboptions. Supported DHCP option 43 suboptions in CableHome 1.1 are: 1, 2, 3, 4, 5, 6, 11, 12, 13, and 14. A sub-option begins with a tag octet containing the sub-option code, followed a length octet which indicates the total number of octets of data. The value of the length octet does not include itself or the tag octet. The length octet is followed by "length" octets of sub-option data.

The encoding of each Option 43 suboption is defined below. See Table 7-7 and Table 7-8 for the intended purpose of each suboption.

The PS MUST encode DHCP Option 43 sub-option 1 by the number of octets equal to the value of the length octet of this suboption, with each octet codifying a requested suboption.

The PS MUST encode each of the DHCP Option 43 suboptions 2, 3, 4, 5, 6, 12, 13, and 14 as a character string consisting of characters from the NVT ASCII character set, with no terminating NULL.

A standalone PS MUST send DHCP Option 43 suboption 2 containing the character string "SPS" (without the quotation marks).

An embedded PS MUST send DHCP Option 43 suboption 2 containing the character string "EPS" (without the quotation marks).

[47] Deleted four paragraphs and 11 bullet statements below per ECN 02-02070 (mistakenly excluded from the I01 version) by GO on 07/31/03.

[48] Replaced this paragraph and the next 14 paragraphs per ECN CH1.1-N-03044, by GO on 10/27/03.

EXHIBIT A

A standalone PS MUST send DHCP Option 43 suboption 3 containing the character string "SPS" (without the quotation marks).

An embedded PS MUST send DHCP Option 43 suboption 3 containing a colon-separated list of all device types in the complete device, including at a minimum the colon-separated character string "ECM:EPS" (without the quotation marks).

If the PS is requesting a PS WAN-Man IP address lease, it MUST send DHCP Option 43 suboption 11 containing the value 0x01, encoded as a binary number, in its DHCP DISCOVER and DHCP REQUEST messages.

If the PS is requesting a PS WAN-Data IP address lease, it MUST send DHCP Option 43 suboption 11 containing the value 0x02, encoded as a binary number, in its DHCP DISCOVER and DHCP REQUEST messages.

Table 7-6 summarizes how the PS is required to set the values for DHCP Option 43, sub-option 11 for the WAN interfaces of the PS.

Table 7-6 — DHCP Option 43, Sub-option 11 Values

Element Id	Description & Comments
PS WAN-Man = 0x01	Identifies the request for a WAN-Man realm address.
PS WAN-Data = 0x02	Identifies the request for a WAN-Data realm address

The length limit of suboption 4, 5, 6, 12, 13, and 14 is each 255 octets. Thus the total length of option 43 could exceed 255 octets. If the total number of octets in all DHCP Option 43 suboptions exceeds 255 octets, the PS MUST follow RFC 3396 to split the option into multiple smaller options.

The PS MUST implement the Vendor Class Identifier Option (DHCP option 60) as specified in Table 7-7 and Table 7-8.

In the case of an Embedded PS with cable modem, the cable modem and PS element each send separate DHCP requests. Table 7-7 describes how the PS MUST set the contents of options 60 and 43 for the CableHome PS when the CableHome PS element is embedded with a cable modem, and separate PS WAN Management and PS WAN Data addresses are requested.

Table 7-7 — DHCP Options for Embedded PS WAN-Man and WAN-Data Address Requests

DHCP Request Options	Value	Description
Embedded CableHome Portal Services DHCP Request for WAN Management Address		
CPE Option 60	"CableHome1.1"	
CPE Option 43 sub-option 1	request sub-option vector	List of sub-options (within option 43) to be returned by server. None defined.
CPE Option 43 sub-option 2	"EPS"	Embedded PS
CPE Option 43 sub-option 3	"ECM:EPS"	List of embedded devices (Embedded CM and embedded PS)
CPE Option 43 sub-option 4	e.g.,"123456"	CM/PS Device serial number
CPE Option 43 sub-option 5	e.g., "v3.2.1"	CM/PS Hardware Version Number
CPE Option 43 sub-option 6	e.g., "1.0.2"	CM/PS Software Version Number

EXHIBIT A

DHCP Request Options	Value	Description
CPE Option 43 sub-option 11	PS WAN-Man (0x01)	Defines that an address is being requested in the PS WAN Management realm
CPE Option 43 sub-option 12	e.g., "ABC Inc. CM-PS123..."	CM/PS System Description from sysDescr
CPE Option 43 sub-option 13	e.g., "CM-PS123-1.0.2...."	CM/PS Fireware Rev from docsDevSwCurrentVers
CPE Option 43 sub-option 14	e.g., "1.2.3..."	Firewall Policy File Version from cabhSec2FirewallPolicyCurrentVersion[49]
Embedded CableHome Portal Services DHCP Request for WAN-Data Address		
CPE Option 60	"CableHome1.1"	
CPE Option 43 sub-option 1	request sub-option vector	List of sub-options (within option 43) to be returned by server. None defined.
CPE Option 43 sub-option 2	"EPS"	Embedded PS
CPE Option 43 sub-option 3	"ECM:EPS"	List of embedded devices (Embedded CM and embedded PS)
CPE Option 43 sub-option 4	e.g.,"123456"	CM/PS Device serial number
CPE Option 43 sub-option 11	PS WAN-Data (0x02)	Defines that an address is being requested in the PS WAN-Data realm

Table 7-8 describes to what the PS MUST set the contents of options 60 and 43, when the CableHome PS is a standalone device.

Table 7-8 — DHCP Options for Stand-alone PS WAN-Man and WAN-Data Address Requests

DHCP Request Options	Value	Description
Stand-alone CableHome Portal Services DHCP Request for WAN Management Address		
CPE Option 60	"CableHome1.1"	
CPE Option 43 sub-option 1	request sub-option vector	List of sub-options (within option 43) to be returned by server. None defined.
CPE Option 43 sub-option 2	"SPS"	Stand-alone PS
CPE Option 43 sub-option 3	"SPS"	List of Embedded devices (Standalone PS only)
CPE Option 43 sub-option 4	e.g., "123456"	Device serial number
CPE Option 43 sub-option 5	e.g., "v3.2.1"	CM/PS Hardware Version Number
CPE Option 43 sub-option 6	e.g., "1.0.2"	CM/PS Software Version Number
CPE Option 43 sub-option 11	PS WAN-Man (0x01)	Defines that an address is being requested in the PS WAN Management realm
CPE Option 43 sub-option 12	e.g., "ABC Inc. CM-PS123..."	CM/PS System Description from sysDescr
CPE Option 43 sub-option 13	e.g., "CM-PS123-1.0.2..."	CM/PS firmware revision from docsDevSwCurrentVers

[49] Revised this cell per ECN CH1.1-N-04.0123-2 by KB on 4/5/04.

EXHIBIT A

DHCP Request Options	Value	Description
CPE Option 43 sub-option 14	e.g., "1.2.3..."	Firewall Policy File Version from cabhSec2FirewallPolicyCurrentVersion[50]
Standalone CableHome Portal Services DHCP Request for WAN-Data Address		
CPE Option 60	"CableHome1.1"	
CPE Option 43 sub-option 1	request sub-option vector	List of sub-options (within option 43) to be returned by server. None defined.
CPE Option 43 sub-option 2	"SPS"	Stand-alone PS
CPE Option 43 sub-option 3	"SPS"	List of Embedded devices (Stand-alone PS only)
CPE Option 43 sub-option 4	e.g., "123456"	Device serial number
CPE Option 43 sub-option 11	PS WAN-Data (0x02)	Defines that an address is being requested in the PS WAN-Data realm

For a detailed description of the contents of the PS sysDescr object, see Section 6.3.3.1.4 SNMP Agent Function Requirements.[51]

The PS MUST support the DHCP Options indicated as mandatory in the CDC Protocol Support column in Table 7-9. Table 7-9 lists the DHCP Options that are mandatory and optional for the CDC to support.[52]

Table 7-9 — DHCP Options Supported by CDC

Option Number	Option Function	CDC Protocol Support (M)andatory
0	Pad	M
255	End	M
1	Subnet Mask	M
2	Time Offset Option	M
3	Router Option	M
4	Time Server Option	M
6	Domain Name Server	M
7	Log Server (syslog)	M
12	Host Name	M
15	Domain Name	M
23	Default Time-to-live	M
26	Interface MTU	M
43	Vendor Specific Information	M
50	Requested IP Address	M
51	IP Address Lease Time	M
54	Server Identifier	M

[50] Revised this cell per ECN CH1.1-N-04.0123-2 by KB on 4/5/04.

[51] Remove a subsequent paragraph per ECN CH1.1-N-03029 by GO on 06/03/03.

[52] Revised this paragraph, Table 7-9, added Table 7-10 and 7-11, along with text between these tables per ECN CH1.1-N-03048 by GO on 07/07/03.

EXHIBIT A

Option Number	Option Function	CDC Protocol Support (M)andatory
55	Parameter Request List	M
60	Vendor Class identifier	M
61	Client-identifier	M
177	Suboption 3 - Service Provider's SNMP Entity Address	M
177	Suboption 6 - Kerberos Realm Name of the Provisioning Realm	M
177	Suboption 51 - Kerberos Server IP address	M

The PS MUST include DHCP Options listed as mandatory in Table 7-10 in DHCP DISCOVER and DHCP REQUEST messages sent to the cable network DHCP server.[53]

Table 7-10 — CDC DHCP Options in DISCOVER and REQUEST Messages

Option Number	Option Function	CDC Protocol Inclusion (M)andatory
255	End	M
43	Vendor Specific Information	M
50	Requested IP Address	M (DHCP REQUEST Only)
55	Parameter Request List	M
60	Vendor Class Identifier	M
61	Client-identifier	M

The PS MUST request DHCP options listed as mandatory in Table 7-11, within the DHCP Option 55 (Parameter Request List) [RFC 2132] sent in the DHCP DISCOVER and DHCP REQUEST messages.

Table 7-11 — CDC DHCP Options Requested within Option 55

Option Number	Option Function	CDC Protocol Inclusion (M)andatory
1	Subnet Mask	M
2	Time Offset Option	M
3	Router Option	M
4	Time Server Option	M
6	Domain Name Server	M
7	Log Server (syslog)	M
15	Domain Name	M
23	Default Time-to-live	M
26	Interface MTU	M
51	IP address Lease Time	M
54	Server Identifier	M
177	PacketCable Compatible Client Configuration Option	M

[53] Revised Table 7-10 per ECN CH1.1-N-03065 by GO on 10/28/03.

EXHIBIT A

The PS MUST support a Service Provider's SNMP Entity Address (DHCP Option 177 sub-option 3) configured as an IPv4 address. The format of DHCP Option 177 sub-option 3 is described below:

The sub-option length MUST be 5 octets. The length octet MUST be followed by a single octet that indicates the specific address type that follows. This type octet MUST be set to 1 to indicate an IPv4 address. The type octet MUST be followed by 4 octets of IPv4 address.[54]

Code	Length	Type	Address			
3	5	1	a1	a2	a3	a4

The PS MUST support a Kerberos Realm Name (DHCP Option 177 sub-option 6). A Kerberos realm name is required by the PS to permit a DNS lookup for the address of the service provider's Key Distribution Center (KDC) entity. The format of DHCP Option 177 sub-option 6 is described below:

The realm name MUST be encoded per the domain style realm name described in [RFC 1510]. The realm name MUST be all capital letters and conform to the syntax described in [RFC 1035] section 3.1. The sub-option is encoded as follows:

Code	Length	Kerberos Realm Name			
6	n	k1	k2	. . .	k_n

The PS MUST support a Kerberos server IP address (DHCP Option 177 sub-option 51). The Kerberos server IP address sub-option informs the PS of the network address of one or more Key Distribution Center servers.

The encoding of the KDC Server Address sub-option will adhere to the format of an IPv4 address using the default port. The minimum length for this option is 4 octets, and the length MUST always be a multiple of 4. If multiple KDC servers are listed they MUST be listed in decreasing order of priority. The KDC Server Address sub-option is encoded as follows:

Code	Length	Address 1				Address 2		
51	n	a1	a2	a3	a4	a1	a2	. . .

Whenever the first PS WAN-Data interface does not have a current DHCP lease, that first PS WAN-Data interface MUST default to the following IP parameters:

"Fallback" WAN-Data IP address: 192.168.100.5

Netmask: 255.255.255.0

Default Gateway: 192.168.100.1

The purpose for the "Fallback" WAN-Data IP address is to enable access to the cable modem's diagnostic IP address (192.168.100.1) from a LAN IP Device. The "Fallback" WAN-Data IP address MUST only be used as the WAN IP address portion of the Dynamic NAT or NAPT tuple of a C-NAT and C-NAPT address mapping, respectively. If the PS is operating in WAN Address Mode 2 and is required to attempt to acquire multiple WAN-Data IP address leases and the PS is unable to acquire the leases after issuing three

[54] Revised type octet from '0' to '1', in this paragraph and the matrix below per ECN CH1.1-N-03039 by GO on 06/23/03.

EXHIBIT A

acquire multiple WAN-Data IP address leases and the PS is unable to acquire the leases after issuing three DHCP DISCOVER messages (in accordance with DHCP retry procedures specified in Section 7.3.3.2.4, CDC Requirements), the PS MUST use the "Fallback" WAN-Data IP address as the WAN portion of each Dynamic NAT tuple, until the PS acquires the necessary WAN-Data IP address lease(s) from a DHCP server through a PS WAN interface.

The PS MUST NOT use the "Fallback" WAN-Data IP address when the PS is configured to operate in Passthrough Primary Packet-handling mode.

The PS MUST NOT use the "Fallback" WAN-Data IP address for any C-NAT or C-NAPT mappings when the PS has a current PS WAN-Man and PS WAN-Data IP address lease. If a DHCP server on the PS WAN interface offers a lease to the PS (CDC) for the IP address 192.168.100.5, i.e., the same address as the "Fallback" WAN-Data IP address, the PS (CDC) MAY accept the lease and use the address as the WAN-Data IP address for a C-NAT or C-NAPT mapping.

Even when using the 192.168.100.5 default WAN-Data IP address, the PS MUST continue to perform a DHCP DISCOVER every 10 seconds until a valid DHCP lease is granted to that PS WAN-Data interface (or the WAN- Man interface, if the WAN-Man and WAN-data are sharing one IP address).

When a PS is acquiring a WAN-Management IP address for its WAN-Man interface, the PS MUST always insert its WAN hardware address into the Client ID (DHCP option 61) field in the DHCP Discover message.

If during its attempt to acquire a lease for the PS WAN-Man IP address the CDC receives no DHCP OFFER, the PS MUST log Event ID 68000100 in the local log and re-broadcast a DHCP DISCOVER message (i.e., restart the provisioning sequence in the event of this failure condition) - repeating the DHCP lease acquisition attempt up to 5 times. If on its fifth attempt to acquire a PS WAN-Man IP address lease the CDC receives no DHCP OFFER, the PS MUST use the "Fallback" WAN IP address, netmask, and default gateway as described above and continue to attempt to acquire a valid WAN-Man IP address by broadcasting DHCP DISCOVER out its WAN interface every 10 seconds until a valid DHCP lease is granted for the WAN-Man IP address.

If during the process of acquiring a lease for the PS WAN-Man IP address the CDC receives, in the DHCP ACK [RFC 2131] from the DHCP server in the cable network, a valid IP address in the 'siaddr' field and a valid file name in the 'file' field and does not receive DHCP Option 177 sub-option 3, sub-option 6, or sub-option 51 (valid combination 1), the PS MUST set cabhPsDevProvMode to dhcpmode(1) and attempt to synchronize time of day with the ToD server as described in Section 7.5.4 Time of Day Client Function Requirements.

If during the process of acquiring a lease for the PS WAN-Man IP address the CDC receives a DHCP ACK from the DHCP server in the cable network containing DHCP Option 177 with a valid IP address (SNMP Entity's address) in sub-option 3, a valid Kerberos realm name in sub-option 6, and a valid IP address (Kerberos server IP address) in sub-option 51, and does not receive a valid IP address in the 'siaddr' field and does not receive a valid file name in the 'file' field (valid combination 2), the PS MUST set cabhPsDevProvMode to snmpmode(2) and the PS MUST initiate operation of the CDS and attempt to synchronize time of day with the ToD server and to authenticate with the KDC server as described in Section 11.3.4 Authentication Infrastructure Requirements.

If during the process of acquiring a lease for the PS WAN-Man IP address the CDC receives, in the DHCP ACK from the DHCP server in the cable network, any combination of DHCP Option 177 sub-options 3, 6, and 51, 'siaddr' field, and 'file' field other than the two valid combinations described above, the PS has received an invalid DHCP configuration, and the PS MUST log the appropriate event and re-broadcast a DHCP DISCOVER message (i.e., restart the provisioning sequence in the event of this invalid condition) - repeating the entire DHCP lease acquisition process up to 5 times.

EXHIBIT A

If on its fifth attempt to acquire a lease for the PS WAN-Man IP address the CDC receives, in the DHCP ACK from the DHCP server in the cable network, any combination of DHCP Option 177 sub-options 3, 6, and 51, 'siaddr' field, and 'file' field other than the two valid combinations described above, the PS MUST do the following on the assumption that it is connected via cable modem to a cable data network that does not support CableHome provisioning (Dormant CableHome mode):

- Disable the SNMP agent (CMP) for WAN interface access. Leave the SNMP agent enabled for message received through the LAN interface (i.e., for SNMP messages addressed to the PS Server Router address).
- Disable the TFTP client
- Disable SYSLOG event reporting
- Accept the offered (CPE) IP address lease and use it as the PS WAN-Data address in the CAP Mapping Table, including assigning the address to cabhCdpWanDataAddrIp and populating the other entries of the CDP WAN-Data Address Table (cabhCdpWanDataAddrTable). The PS will be operating without a WAN-Man IP address, which is different from any of the WAN Address Modes described in Section 7.3.3.2.3.2.
- Terminate the provisioning timer
- Set the value of cabhPsDevProvMode to dormantCHmode(3)
- Set the value of cabhPsDevProvState to fail(3)
- Enable the CDS
- Enable the CAP and USFS functionality
- Enable the CNP
- Enable the firewall
- Operate with parameters that have been provisioned in the past, including those values of persistent MIB objects. The PS operating in Dormant CableHome Mode MUST NOT reset its MIB objects to factory default settings.

When a PS operating in WAN Address Mode 2 (as described in Section 7.3.3.2) is acquiring a WAN-Data IP address for a WAN-Data interface that will use an IP address distinct from the WAN-Man interface, the PS MUST include the Client Identifier option (cabhCdpWanDataAddrClientId) in the DHCP Discover message. To enable these unique WAN-Data Client IDs, the CDC MUST enable the NMS system to create cabhCdpWanDataAddrClientId entries in the cabhCdpWanDataAddrTable.

If a PS is operating in WAN Address Mode 2 (as described in Section 7.3.3.2) the PS MUST attempt to obtain an IP address, via DHCP, for each unique client ID (cabhCdpWanDataAddrClientId) in the cabhCdpWanDataAddrTable, up to the limit defined by cabhCdpWanDataIpAddrCount.

The PS MUST continue to retransmit the broadcast DHCP DISCOVER message implementing a randomized exponential backoff algorithm, consistent with that described in [RFC 2131], until it acquires a valid PS WAN-Man IP and/or PS WAN-Data IP address lease, as needed.[55]

If the PS (CDC) is successful in acquiring the WAN-Man IP address (i.e., receives a DHCP ACK from a DHCP server via the PS WAN-Man Interface) on its first attempt, and if the PS is operating in DHCP Provisioning Mode, the PS MUST attempt Time of Day time synchronization with the ToD server by issuing a ToD request as described in Section 7.5.4, before attempting to download the PS Configuration File.

If the PS (CDC) is unsuccessful in acquiring the WAN-Man IP address (i.e., the DHCP request times out in accordance with [RFC 2131]) on its first attempt, the PS MUST trigger the CDS (i.e., initiate CDS operation), so that the CDS can serve DHCP requests from LAN IP Devices in the LAN-Trans realm.

[55] Replaced this paragraph per ECN CH1.1-N-03030 by GO on 06/03/03.

EXHIBIT A

The PS CDC Function MUST only respond to DHCP messages that are received through, or send DHCP messages through, a WAN Interface.

When the WAN-Man DHCP lease expires, the PS MUST clear all row entries from the cabhCdpWanDnsServerTable.

7.4 PS Function - Bulk Portal Services Configuration (BPSC)

7.4.1 Bulk Portal Services Configuration Function Goals

The primary goals of the BPSC function are to request, receive, and process PS and firewall configuration parameters.

7.4.2 Bulk Portal Services Configuration Function System Design Guidelines

The guideline identified in Table 7-12 guided specification of capabilities for the Bulk PS Configuration function:

Table 7-12 — Bulk Portal Services System Design Guidelines

Number	Bulk PS Configuration System Design Guidelines
BPSC 1	CableHome will provide a mechanism by which the PS can download and process CableHome PS and Firewall Configuration Files.

7.4.3 Bulk Portal Services Configuration Function System Description

Bulk Portal Services configuration is typically carried out during the provisioning of the PS element, via the processing of configuration settings contained within a configuration file. However, this process may be initiated at any time. Within this section the term "configuration file" is used to mean either the PS Configuration File or the Firewall Configuration File. Specific requirements for either type of configuration file will be labeled with the appropriate file label, i.e., PS Configuration File or Firewall Configuration File. The Bulk PS Configuration tool consists of the following components:

- The format of the Configuration File
- Modes of triggering the download process
- Means of authenticating the file
- Means of reporting back the status of the configuration file download and other considerations

Bulk PS Configuration (BPSC) is a tool that MSOs can use to change PS and Firewall configuration settings in bulk, via a Configuration File. Typically, the Configuration File will contain many settings, since the primary usefulness afforded by Configuration Files use is the ability to change a number of configuration settings with minimal cable operator intervention. However, it is expected that the Firewall Configuration File will only be used for firewall-specific settings.

The Bulk PS Configuration process can behave the same as successive SNMP sets executed by an operator manually. The Configuration File is a tool meant to make operators more productive and to make large configuration changes less error prone.

It is significant to note that a PS operating in SNMP Provisioning Mode does not need a PS Configuration File loaded before it can operate. It is expected that a PS operating in SNMP Provisioning Mode will initialize itself to a known state and a PS could run for a lifetime without having a PS Configuration File loaded. However, a PS will accept and process a PS Configuration File when one is provided.

EXHIBIT A

7.4.4 Bulk Portal Services Configuration Function Requirements

A PS operating in DHCP Provisioning Mode MUST download and process a PS Configuration File.

A PS operating in SNMP Provisioning Mode MUST be capable of operating without a PS Configuration File, but MUST be capable of downloading and processing a PS Configuration File if triggered as described in Section 7.3.3.2. The PS is not required to download a Firewall Configuration File in either DHCP or SNMP Provisioning Mode.

MIB object settings passed in the PS Configuration File take precedence over and MUST over-write existing MIB object settings.

7.4.4.1 Configuration File Format Requirements

PS or firewall configuration data MUST be contained in a file, which is downloaded via TFTP or HTTPS. The Configuration File MUST consist of a number of configuration settings (1 per parameter), each of the form "Type Length Value (TLV)". Definitions of these terms are provided in Table 7-13.

Table 7-13 — TLV Definitions

Type	A single-octet identifier which defines the parameter
Length	A two-octet field specifying the length of the Value field (not including Type and Length fields)
Value	A set of octets Length long containing the specific value for the parameter

The configuration settings MUST follow each other directly in the file, which is a stream of octets (no record markers). The PS MUST be capable or properly receiving and processing a configuration file that is padded to an integral number of 32-bit words, and be able to properly receive and process a configuration file that is not padded to an integral number of 32-bit words. See Section 7.3.3.1.1 for a definition of the pad. Configuration settings are divided into three types:

- CableHome-specified Configuration settings which are required to be present
- Additional or optional CableHome-specified configuration settings which MAY be present
- Vendor-specific configuration settings.

A PS Configuration File MAY contain many different parameters, but the only parameters that MUST be included in the PS configuration file are the PS Message Integrity Check (MIC) (Type 53) and the End of Data Marker (Type 255). A Firewall Configuration File MAY contain many different Type 28 TLV parameters for configuring the firewall, but the only parameter that MUST be included in the Firewall Configuration File is the End of Data Marker (Type 255). If the Firewall Configuration File contains a PS Message Integrity Check (MIC) (Type 53), the PS MUST ignore it.[56]

To allow uniform management of the PS, the PS MUST support a Configuration File that is up to 64K-bytes long.

Each CableHome Portal Services element MUST support configuration parameter Types 0, 9, 10, 21, 28, 32, 33, 34, 38, 43, 53 and 255, which are described in this section. Each TLV parameter in the Firewall Configuration File describes a firewall attribute. Since the CableHome firewall is configured via access to the CableHome Security MIB (ref: Section 11.6.4 Firewall Requirements), a Firewall Configuration File typically includes TLV type 28 configuration settings, which contain SNMP MIB objects. Vendor-specific firewall configuration information is permitted to be passed to the PS in the Firewall Configuration File using the vendor-specific configuration setting type 43 (TLV-43). If the configuration file does not contain the required attributes, the PS MUST reject the file.

[56] Revised this paragraph per ECN CH1.1-N-03.0097-5 by GO on 12/9/03.

EXHIBIT A

The size of the value in the Length field for any configuration parameter included in a CableHome configuration file MUST be 2 octets.

The Length value for each Type described in the TLV descriptions in this section is the actual length in octets of the Value field.

7.4.4.1.1 Pad Configuration Setting

This has no Length or Value fields and is only used following the end of data marker to pad the file to an integral number of 32-bit words.

Type	Length	Value
0	—	—

7.4.4.1.2 Software Upgrade Filename

The filename of the software upgrade file for the CableHome device. The filename is a fully qualified directory- path name. The file is expected to reside on a TFTP server identified in a configuration setting option.

Type	Length	Value
9	Variable	filename

7.4.4.1.3 SNMP Write-Access Control

This object makes it possible to disable SNMP "Set" access to individual MIB objects. Each instance of this object controls access to all of the writeable MIB objects whose Object ID (OID) prefix matches. This object may be repeated to disable access to any number of MIB objects.

Type	Length	Value
10	n	OID prefix plus control flag

Where n is the size of the ASN.1 Basic Encoding Rules [ISO8025] encoding of the OID prefix plus one byte for the control flag.

The control flag may take values:

0 - allow write-access

1 - disallow write-access

Any OID prefix may be used. The Null OID 0.0 may be used to control access to all MIB objects. (The OID 1.3.6.1 will have the same effect.)

When multiple instances of this object are present and overlap, the longest (most specific) prefix has precedence.

Thus, one example might be

someTable disallow write-access

someTable.1.3 allow write-access

EXHIBIT A

This example disallows access to all objects in someTable except for someTable.1.3.

7.4.4.1.4 Software Upgrade TFTP Server

The IP address of the TFTP server, on which the software upgrade file for the CableHome device resides.

Type	Length	Value
21	4	ip1, ip2, ip3, ip4

7.4.4.1.5 First-phase SNMP MIB Object with Extended Length[57]

This object allows SNMP MIB objects to be Set via the TFTP-Registration process prior to SNMP Sets done with TLV-28. The intent of this TLV is to include only those SNMP Sets that have to occur prior to other SNMP Sets to ensure correct operation, such as SetToFactory objects (e.g., cabhPsDevSetToFactory) that clear persistent MIB objects. Non-priority SNMP Sets are expected to be included in TLV-28.

The value of this parameter is an SNMP variable binding (VarBind) as defined in [RFC 3416]. The VarBind is encoded in ASN.1 Basic Encoding Rules, just as it would be if part of an SNMP Set Request PDU.

Type	Length	Value
27	Variable	variable binding

The PS MUST treat the variable binding, in a Type 27 TLV, as if it were part of an SNMP Set Request with the following caveats:

- It MUST treat the request as fully authorized (it cannot refuse the request for lack of privilege).
- SNMP Write-Control provisions do not apply.
- No SNMP response is generated by the PS.
- This object MAY be repeated with different VarBinds to "Set" a number of MIB objects. All SNMP Sets in a Configuration File that occur within Type 27 TLVs MUST be treated as if simultaneous. Each VarBind MUST be limited to 65535 bytes.
- This object MUST be processed before any Type 28 TLV present in the Configuration File are processed.

7.4.4.1.6 SNMP MIB Object with extended Length

This object allows arbitrary SNMP MIB objects to be Set via the TFTP-Registration process, where the value is an SNMP variable binding (VarBind) as defined in [RFC 3416]. The VarBind is encoded in ASN.1 Basic Encoding Rules, just as it would be if part of an SNMP Set request.

Type	Length	Value
28	Variable	variable binding

The PS MUST treat the variable binding, in a Type 28 TLV, as if it were part of an SNMP Set Request with the following caveats:

- It MUST treat the request as fully authorized (it cannot refuse the request for lack of privilege).
- SNMP Write-Control provisions (see previous section) do not apply.
- No SNMP response is generated by the PS.

[57] Added this section per ECN CH1.1-N-03.0103-3 by GO on 12/5/03.

EXHIBIT A

- This object MAY be repeated with different VarBinds to "Set" a number of MIB objects. All SNMP Sets in a Configuration File that occur within Type 28 TLVs MUST be treated as if simultaneous. Each VarBind MUST be limited to 65535 bytes.

7.4.4.1.7 Manufacturer Code Verification Certificate

The Manufacturer's Code Verification Certificate (M-CVC) for Secure Software Downloading. Refer to Section 11.8.4.4.2 Network Initialization.[58]

Type	Length	Value
32	Variable	Manufacturer CVC (DER-encoded ASN.1)

7.4.4.1.8 Co-signer Code Verification Certificate

The Co-signer's Code Verification Certificate (C-CVC) for Secure Software Downloading. Refer to Section 11.8.4.4.2 Network Initialization.[59]

Type	Length	Value
33	Variable	Co-signer CVC (DER-Encoded ASN.1)

7.4.4.1.9 SNMPv3 Kickstart Value

(ref.: Section C.1.2.8 DOCSIS 1.1 RFI Specification [DOCSIS])

Compliant Portal Services elements MUST understand the following TLV and its sub-elements and be able to kickstart SNMPv3 access to the PS regardless of whether the PS is operating in NmAccess Mode or Coexistence Mode (see Section 6.3.3 CMP System Description and Section 6.3.3.1.4.2 Network Management Mode Requirements).

Type	Length	Value
34	n	Composite

Up to 5 of these objects may be included in the configuration file. Each results in an additional row being added to the usmDHKickstartTable and the usmUserTable and results in an agent public number being generated for those rows.

7.4.4.1.9.1 SNMPv3 Kickstart Security Name

Type	Length	Value
34.1	2-16	UTF8 Encoded security name

For the ASCII character set, the UTF8 and the ASCI I encodings are identical. Normally, this will be specified as one of the CableHome built-in USM users, e.g., "CHAdministrator".

The security name is NOT zero terminated. This is reported in the usmDHKickStartTable as usmDHKickStartSecurityName and in the usmUserTable as usmUserName and usmUserSecurityName.

[58] Revised this section per ECN CH1.1-N-03032 by GO on 06/06/03.
[59] Revised this section per ECN CH1.1-N-03032 by GO on 06/06/03.

EXHIBIT A

7.4.4.1.9.2 SNMPv3 Kickstart Manager Public Number

Type	Length	Value
34.2	n	Manager's Diffie-Hellman public number expressed as an octet string.

This number is the Diffie-Hellman public number derived from a privately (by the manager or operator) generated random number and transformed according to [RFC 2786]. This is reported in the usmDHKickStartTable as usmKickstartMgrPublic. When combined with the object reported in the same row as usmKickstartMyPublic, it can be used to derive the keys in the related row in the usmUserTable.

7.4.4.1.10 SNMP Notification Receiver

(ref: [DOCSIS9])

Type	Length	Value
38	n	Composite

This PS Configuration File element specifies a Network Management Station that will receive notifications from the PS when it is in Coexistence network management mode. This TLV (38) consists of several sub-TLVs inside the TLV configuration file element. Up to 10 of these elements may be included in the PS Configuration File. Section 6.3.3.1.4.6 Mapping TLV Fields Into Created SNMPv3 Table Rows provides detail about how this configuration file element is mapped into SNMPv3 functional tables.

All multi-byte fields of this sub-TLV MUST be placed in the network byte order.

7.4.4.1.10.1 Sub-TLV 38.1 - IP Address of trap receiver

IPv4 address of the trap receiver, in binary.

Type	Length	Value
38.1	4	IP address

7.4.4.1.10.2 Sub-TLV 38.2 - UDP Port number of the trap receiver

UDP Port number of the trap receiver, in binary.

Type	Length	Value
38.2	2	UDP Port

If this sub-TLV is not present in a configuration file, the default value 162 is used.

7.4.4.1.10.3 Sub-TLV 38.3 - Type of trap sent by the PS (Note 2)

Trap type.

Type	Length	Value
38.3	2	Trap type

The PS MUST support the following trap type values:

EXHIBIT A

1 = SNMP v1 trap in an SNMP v1 packet

2 = SNMP v2c trap in an SNMP v2c packet

3 = SNMP inform in an SNMP v2c packet

4 = SNMP v2c trap in an SNMP v3 packet

5 = SNMP inform in an SNMP v3 packet

7.4.4.1.10.4 Sub-TLV 38.4 - Timeout

Timeout, in milliseconds, used for sending SNMP inform messages.

Type	Length	Value
38.4	2	0 - 65535

7.4.4.1.10.5 Sub-TLV 38.5 - Retries

Number of retries when sending an inform, after sending the inform the first time.

Type	Length	Value
38.5	2	0 - 65535

7.4.4.1.10.6 Sub-TLV 38.6 - Notification Filtering Parameters

Type	Length	Value
38.6	n	Filter OID

Where n is the size of the ASN.1-encoded Filter Object Identifier.

Filter OID is an ASN.1-formatted Object Identifier of the snmpTrapOID value that identifies the notifications to be sent to the notification receiver. This notification and all below it will be sent.

If this Sub-TLV is not present, the notification receiver will receive all notifications generated by the SNMP agent.

7.4.4.1.10.7 Sub-TLV 38.7 - Security Name to use when sending SNMP V3 Notification

Type	Length	Value
38.7	2 - 16	UTF8-encoded security name

This sub-TLV is not required for Trap type = 1, 2, or 3. The PS MUST ignore sub-TLV 38.7 if the trap type in sub-TLV 38.3 is 1, 2, or 3. If sub-TLV 38.7 is not supplied for a Trap type of 4 or 5, the PS MUST send the SNMPv3 Notification in the noAuthNoPriv security level using the security name "@PSconfig". (Note 2)

SecurityName

The SNMPv3 Security Name to use when sending an SNMPv3 Notification. Only used if Trap Type is set to 4 or 5. This name MUST be a name specified in a Config File TLV Type 34 as part of the DH Kickstart

EXHIBIT A

procedure. The notifications MUST be sent using the Authentication and Privacy Keys calculated by the PS during the DH Kickstart procedure.

Notes:[60]

1. Upon receiving one of these TLV elements, the PS MUST make entries to the following tables in order to cause the desired trap transmission: snmpNotifyTable, snmpTargetAddrTable, snmpTargetParamsTable, snmpNotifyFilterProfileTable, snmpNotifyFilterTable, snmpCommunityTable, usmUserTable, vacmSecurityToGroupTable, vacmAccessTable, and vacmViewTreeFamilyTable

2. Trap Type: The community String for traps in SNMP V1 and V2 packets MUST be "public". The Security Name in traps and informs in SNMP V3 packets where no security name has been specified MUST be "@PSconfig" and in that case the security level MUST be NoAuthNoPriv.

3. Filter OID: SNMP V3 allows the specification of which Trap OID's are to be sent to a trap receiver. The filter OID in the config element specifies the OID of the root of a trap filter sub-tree. All Traps with a Trap OID contained in this trap filter sub-tree MUST be sent to the trap receiver.

4. The PS Configuration File is permitted to also contain TLV MIB elements (TLV-28) that make entries to any of the 10 tables listed in Note 1. The PS MUST ignore TLV MIB elements that use index columns that start with the characters "@PSconfig".

7.4.4.1.11 Vendor-specific Information[61]

If vendor-specific information is provided to the PS, it MUST be encoded in the vendor-specific information field (VSIF) (code 43) using the Vendor ID field to specify which TLV tuples apply to which vendors' products. A properly-formed VSIF has a single Vendor ID Sub-TLV (code 43.1) as the first sub-TLV. The PS MUST reject the PS Configuration File if any VSIF (Type 43) TLV is not correctly formed.

A PS configuration file can have multiple VSIFs with either different or the same Vendor ID Sub-TLVs present. The PS will process only those VSIFs that have a Vendor ID Sub-TLV matching Vendor ID and will ignore the VSIF's that have Vendor ID Sub-TLVs which do not match.

Vendor-specific sub-types are allowed to be added after Type 43.1.

Type	Length	Value
43	N	vendor-specific settings

Sub-TLV 43.1 - Vendor ID type

Vendor identification specified by the three-byte Organization Unique Identifier of the PS vendor.

Type	Length	Value
43.1	3	v1, v2, v3

7.4.4.1.12 PS Message Integrity Check (PS MIC)

Type	Length	Value

[60] Removed Note 5 from this section per ECN CH1.1-N-03063 by GO on 10/28/03.
[61] Revised the first two paragraphs of this section per ECN CH1.1-N-03.0093-2 by GO on 12/5/03.

EXHIBIT A

53	20	A 160-bit (20 octet) SHA hash

This parameter contains a hash (PS MIC) calculated by a Secure Hash Algorithm (SHA-1) [SHA], defined in NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995 [FIPS 180-1]. This TLV is only used in the configuration file immediately before the end of data marker.

EXHIBIT A

7.4.4.1.13 End-of-Data Marker

This is a special marker for end of data. It has no Length or Value fields.

Type	Length	Value
255	---	---

7.4.4.2 BPSC Triggering Requirements

Transfer of the configuration file, from the TFTP server or HTTPS server in the cable data network to the PS, is initiated by an event referred to as a trigger. Requirements for triggering the transfer of a CableHome PS Configuration File or Firewall Configuration File from the TFTP server or HTTPS server to the PS follow.

The mode of triggering the PS Configuration File download is dependent upon the Provisioning Mode in which the PS is operating. The CMP MUST read the value of cabhPsDevProvMode (see Section 7.3.3.2.4) prior to initiating any PS Configuration File download. The method of triggering for the Firewall Configuration File download is not dependent upon the Provisioning Mode.

7.4.4.2.1 PS Configuration File Download Trigger for DHCP Provisioning Mode

If the PS receives the TFTP or HTTPS server address in the 'siaddr' field and the PS Configuration File name in the 'file' field of the DHCP ACK, AND the value of cabhPsDevProvState = inProgress(2), the PS MUST combine the server address and PS Configuration File name to form a URL-encoded value and write that value into PSDev MIB object cabhPsDevProvConfigFile. The PS MUST use the following format for the URL-encoded value for the TFTP server IP address and PS Configuration File name:[62]

tftp://IPv4_address_of_the_TFTP_server/full_path_ to_the_PS_Configuration_File/PS_Configuration_File_name

The PS MUST use the following format for the URL-encoded value for the HTTPS server IP address and PS Configuration File name:

https://IPv4_address_of_the_HTTPS_server/full_path_ to_the_PS_Configuration_File/PS_Configuration_File_name

Download of the PS Configuration File, by a PS operating in DHCP Provisioning Mode, is triggered by the presence of the PS Configuration File location (TFTP or HTTPS server IP address) and name in the DHCP message issued to the PS (CDC) by the DHCP server in the cable network. Refer to Section 7.3.3.2.4 CDC Requirements.

If the PS is operating in DHCP Provisioning Mode (as indicated by the value of cabhPsDevProvMode), after the PS (CDC) receives a DHCP ACK from the DHCP server in the cable network, and the IP address in the 'siaddr' field does not match the first IP address in DHCP option 72, AND the value of cabhPsDevProvState = inProgress(2), then the PS MUST issue a TFTP Get request to the server identified in the DHCP message 'siaddr' field to download the configuration file.[63]

If the PS is operating in DHCP Provisioning Mode (as indicated by the value of cabhPsDevProvMode), after the PS (CDC) receives a DHCP ACK from the DHCP server in the cable network, and the IP address in the 'siaddr' field matches the first IP address in DHCP option 72, and the cabhPsDevTodSyncStatus MIB object has a value of '1' (ToD access succeeded), then the PS MUST establish a TLS session as defined in Section 11, and issue a HTTP Get request to the server identified in the DHCP message 'siaddr' field, to download the configuration file.

[62] Revised the first sentence of this paragraph per ECN CH1.1-N-03.0099-3 by GO on 12/10/03.

[63] Revised the first sentence of this paragraph per ECN CH1.1-N-03.0099-3 by GO on 12/10/03.

EXHIBIT A

If the PS is operating in DHCP Provisioning Mode (as indicated by the value of cabhPsDevProvMode), after the PS (CDC) receives a DHCP ACK from the DHCP server in the cable network, and the IP address in the 'siaddr' field matches the first IP address in DHCP option 72, and the cabhPsDevTodSyncStatus MIB object has a value of '2' (ToD access failed), the PS MUST wait until the cabhPsDevTodSyncStatus MIB object has a value of '1' (ToD access succeeded), before establishing a TLS session as defined in Section 11, and issuing an HTTP Get request to the server identified in the DHCP message 'siaddr' field, to download the configuration file.

Modification of cabhPsDevProvConfigFile MUST NOT trigger a PS operating in DHCP Provisioning Mode to download a configuration file. A PS operating in DHCP Provisioning Mode MUST treat cabhPsDevProvConfigFile as a read-only object.

7.4.4.2.2 PS Configuration File Download Trigger for SNMP Provisioning Mode

If the PS is operating in SNMP Provisioning Mode (as indicated by the value of cabhPsDevProvMode), PS Configuration File download MUST NOT occur before completion of the SNMP v3 setup process (refer to Section 11.4 Secure Management Messaging to the PS, for details about the SNMP setup process).

If the PS is operating in SNMP Provisioning Mode (as indicated by the value of cabhPsdevProvMode), the PS element MUST NOT initiate a PS Configuration File download if the cabhPsDevTodSyncStatus MIB object has a value of '2' (ToD access failed).

Once the PS, operating in SNMP Provisioning Mode (as indicated by the value of cabhPsDevProvMode), issues a TFTP request to download a PS Configuration file (subject to conditions described in other requirements, below), the PS MUST complete the download phase. When the PS (CMP) has successfully downloaded the requested PS Configuration File, it MUST process the file before issuing a TFTP request for another PS Configuration File.

The PS MUST attempt to download and process the configuration file whose name and address are specified in cabhPsDevProvConfigFile when it receives an SNMP Set command for the cabhPsDevProvConfigFile object, if the following conditions are true:

- the PS is operating in SNMP Provisioning Mode
- the cabhPsDevTodSyncStatus MIB object has a value of '1' (ToD access succeeded), and
- cabhPsDevProvConfigFileStatus = idle(1)

The format of cabhPsDevProvConfigFile MUST be a URL- encoded TFTP server IP address and configuration file name.

If the PS (CMP) operating in SNMP Provisioning Mode receives an SNMP set request from the NMS to update the value of cabhPsDevProvConfigFile and cabhPsDevProvConfigFileStatus = busy(2), or if the cabhPsDevProvConfigHash object does not have a valid value, then the PS MUST reject the set request.

7.4.4.2.3 Firewall Configuration File Trigger

The Firewall Configuration File download is triggered when the value used to SET the cabhSec2FwPolicyFileURL MIB object, by either the PS Configuration File or by a SNMP SET command, is different than the value of the cabhSec2FwPolicySuccessfulFileURL MIB. If the value used to SET the cabhSec2FwPolicyFileURL MIB object, by either the PS Configuration File or by a SNMP SET command, is the same as the value of the cabhSec2FwPolicySuccessfulFileURL MIB, the Firewall Configuration File download MUST NOT be triggered.[64]

[64] Replaced paragraph per ECN CH1.1-N-03035 by GO on 07/03/03. Superseded and replaced by ECN CH1.1-N-03069 on 10/28/03.

EXHIBIT A

When a download as been triggered, the PS MUST use the prefix of the cabhSecFwPolicyFileURL MIB object value to determine whether to use TFTP (tftp://) or a TLS session (https://) as defined in Section 11 for Firewall Configuration File download.[65]

7.4.4.2.4 Post-trigger Operation

Once triggered, the PS MUST use an [RFC 1350] and [RFC 2349] compliant TFTP or [RFC 2616] HTTP client to download the configuration files[66]

A signaling mechanism is necessary to inform the management entity that the PS is currently processing a configuration file. The PS Dev MIB object cabhPsDevProvConfigFileStatus is defined to serve as this signaling mechanism.

If a PS is not currently requesting, downloading, or processing a configuration file, it MUST set cabhPsDevProvConfigFileStatus = idle(1). When the PS has issued a TFTP request for a configuration file specified in cabhPsDevProvConfigFile, it MUST set cabhPsDevProvConfigFileStatus = busy(2).When the PS completes the processing of the PS Configuration File, the PS MUST set cabhPsDevProvConfigFileStatus = idle(1).

Once triggered to download a configuration file, the PS element MUST continue to attempt to download the specified configuration file from the specified location until the configuration file is successfully downloaded and the hash successfully computed as described in Section 7.4.4.3 Configuration File Check and SNMP Provisioning Mode Authentication Requirements. The PS MUST use an adaptive timeout for TFTP and HTTPS based on binary exponential backoff as described below, if the first attempt is not successful, until the PS successfully receives the requested file from the server in the cable data network:

- each retry is 2^n second(s) following the previous attempt, where the PS Configuration File Retry Counter or the Firewall Configuration File Retry Counter, n = [0, 1, 2, 3, 4, or 5]
- n = 0 for the first retry, then is incremented by one for each subsequent attempt until n = 5
- if the PS does not successfully acquire the requested PS Configuration File following the attempt with n = 5, n is to be reset to 0 and the PS is to restart the WAN-Man IP address acquisition process via DHCP.
- if the PS does not successfully acquire the requested Firewall Configuration File following the attempt with n = 5, n is to be reset to 0 and the PS is to continue normal operation, i.e., the PS is not to restart the WAN-Man IP address acquisition process.

The PS MUST exchange TFTP and HTTPS messages only through the PS WAN-Man Interface. The PS MUST reject any configuration file not received through the PS WAN-Man Interface.

When the download of the configuration file is complete and the configuration file is properly authenticated as described in Section 7.4.4.3 PS Configuration File Check and SNMP Provisioning Mode Authentication Requirements, the PS MUST process the TLVs contained within the file as defined below. See Section 7.4.4.4 Configuration File Processing and Status Reporting Requirements, for specifics of error handling and event generation while processing the configuration file.

The PS MUST use parameters extracted from the configuration file to set the managed objects in the PS database. This process is functionally equivalent to an SNMP SET operation, but it does not rely on the user or view-based access permissions. The PS MUST unconditionally update managed objects in the PS database corresponding to recognized OIDs.

The PS MUST translate Configuration File TLV-27 elements into a single SNMP PDU containing (n) MIB OID/instance and value components (SNMP varbinds) and translate TLV-28 elements into a single SNMP

[65] Added this paragraph per ECN CH1.1-N-03.0097-5 by GO on 12/9/03.
[66] Revised this sentence per ECN CH1.1-N-03.0099-3 by GO on 12/10/03.

EXHIBIT A

PDU containing (n) MIB OID/instance and value components (SNMP varbinds). In accordance with [RFC 3416], the single TLV-27 Configuration File-generated SNMP PDU will be treated "as if simultaneous", the single TLV-28 Configuration File generated SNMP PDU will be treated "as if simulataneous", and the PS MUST behave consistently, regardless of the order in which TLV-27 or TLV-28 elements appear in the Configuration File or SNMP PDUs. The single configuration file-generated SNMP PDU requirement is consistent with SNMP PDU packet behaviors received from an SNMP manager: SNMP PDU varbind order does not matter, and there is no defined MAX SNMP PDU limit. Once a single SNMP PDU is constructed, the PS processes the SNMP PDU and determines the PS configuration acceptance/rejection based on the rules for configuration file processing, described in Section 7.4.4.4 PS Configuration File Processing and Status Reporting Requirements. In processing the SNMP PDU, the PS MUST support CreateAndGo for row creation.[67]

The PS MUST update the size of the PS Configuration file in the MIB object cabhPsDevProvConfigFileSize.

The PS MUST update the number of TLVs processed (i.e., the TLVs that are intended to change the PS configuration per their own Value field) and the number of TLVs ignored (i.e., the TLVs intended to change the PS configuration per their own Value fields that are not successful) from a PS Configuration File, in the MIB objects cabhPsDevProvConfigTLVProcessed and cabhPsDevConfigTLV Rejected, respectively[68]. Configuration parameter Types 255 (End-of-Data Marker), 53 (PS MIC), 0 (Pad Configuration Setting), and Type and Length field pairs that encompass sub-TLVs do not specify values in Value fields intended to change PS configuration and thus MUST NOT be counted in the values of cabhPsDevProvConfigTLVProcessed and cabhPsDevConfigTLVRejected.

7.4.4.3 Configuration File Check and SNMP Provisioning Mode Authentication Requirements

The algorithm used to authenticate the configuration file depends upon the provisioning mode in which the PS is operating (see Section 5.5 CableHome Operational Models). The PS supports two provisioning modes: DHCP Provisioning Mode and SNMP Provisioning mode. Two methods of configuration file authentication are supported for DHCP Provisioning Mode, depending upon the information received in the 'siaddr' field of the DHCP ACK message.

The following sections describe the security algorithms and requirements needed to check the configuration file Hash based on the provisioning mode of the PS element. The PS element MUST support both security algorithms specified in Sections 7.4.4.3.1 PS Configuration File Check for DHCP Provisioning Mode and 7.4.4.3.2 PS Configuration File Authentication Algorithm for SNMP Provisioning Mode.

7.4.4.3.1 PS Configuration File Check for DHCP Provisioning Mode

When operating the DHCP Provisioning Mode, the PS will use a hash-based check of the configuration file, or it will authenticate the message in which the file is transferred, depending upon the configuration of the cable operator's provisioning system.

The PS MUST conduct the hash-based configuration file check described below:

1. When the configuration file Generator of the Provisioning System creates a new PS Configuration File or modifies an existing file, the Config File Generator will create a SHA-1 hash of the contents of the PS Configuration File, taken as a byte string. The end of data marker and any padding that follow it are

[67] Revised this paragraph per ECN CH1.1-N-03.0103-3 by GO on 12/5/03.

[68] Per these definitions a TLV that does not successfully configure the PS is counted twice, once by each of cabhPsDevProvConfigTLVProcessed and cabhPsDevProvConfigTLVRejected. A TLV that successfully configures the PS is counted only by cabhPsDevProvConfigTLVProcessed.

EXHIBIT A

not included in the hash calculation.

2. The Config File Generator adds the hash value, calculated in Step 1, to the PS Configuration File as the last TLV setting (immediately before the end of data marker) using a type 53 TLV. The PS Configuration File is then made available to the appropriate TFTP server.

3. The PS element downloads the PS Configuration File.

4. The PS MUST update the cabhPsDevProvConfigHash MIB object with the hash value from the hash TLV created in steps 1 and 2.

5. The PS element MUST compute a SHA-1 hash over the contents of the PS Configuration File excluding the hash TLV (used to configure the cabhPsDevProvConfigHash MIB object), the end of data marker, and any padding that follows. If the computed hash and the value of the cabhPsDevProvConfigHash MIB object are the same, the PS Configuration File integrity is verified and the configuration file MUST be processed; otherwise, the file MUST be rejected.

7.4.4.3.2 PS Configuration File Authentication Algorithm for SNMP Provisioning Mode

The procedure for checking the PS Configuration File Hash by the PS element in SNMP Provisioning Mode follows:

1. When the Config File Generator of the Provisioning System creates a new PS Configuration File or modifies an existing file, the Config File Generator will create a SHA-1 hash of the entire content of the PS Configuration File, taken as a byte string. The end of data marker and any padding that follow it are not included in the hash calculation.

2. The NMS sends the hash value calculated in step 1 to the PS element via SNMP SET. The PS updates its cabhPsDevProvConfigHash MIB object with the new value.

3. The NMS sends the Name and location of the PS Configuration File via SNMP SET. The PS updates its cabhPsDevProvConfigFile MIB object with the new value.

4. The PS element downloads the named file from the configured TFTP server. If the PS Configuration File contains TLV type 53 the PS MUST ignore it.

5. The PS element MUST compute a SHA-1 hash over the contents of the PS Configuration File excluding the TLV 53 if it exists, the end of data marker and any padding that follows. If the computed hash and the value of the cabhPsDevProvConfigHash MIB object are the same, the PS Configuration File integrity is verified and the configuration file MUST be processed; otherwise, the file MUST be rejected.

7.4.4.3.3 Firewall Configuration File Check

The PS is required to use the Firewall Configuration File check on the Firewall Configuration File as described in this section if the file is provided in SNMP Provisioning Mode or DHCP Provisioning Mode without the use of HTTPS/TLS as defined in Section 11.9 PS Configuration File Security in DHCP Provisioning Mode.

If the Firewall Configuration File was downloaded without the use of HTTP/TLS, the PS MUST follow the procedure defined in steps 1) through 5) below to check the integrity of the Firewall Configuration File:

1. The Firewall Configuration File generator will create a SHA-1 hash of the entire contents of the

EXHIBIT A

Firewall Configuration File, taken as a byte string.

2. The provisioning system sends the hash value calculated in step 1 to the PS element in one of two ways:
   a) modifies the cabhSec2FwPolicyFileHash MIB object via a type 28 TLV in the PS Configuration File
   b) sends an SNMP Set command to update the cabhSec2FwPolicyHash MIB object

3. The provisioning system sends the name and location of the Firewall Configuration File to trigger the download of the Firewall Configuration File in one of two ways:
   a) modifies the cabhSec2FwPolicyFileURL MIB object via a type 28 TLV in the PS Configuration File
   b) sends an SNMP Set command to update the cabhSec2FwPolicyURL MIB object

4. If the cabhSecFwPolicyFileOperStatus is not inProgress(1) and the value used to SET the cabhSec2FwPolicyFileURL MIB object is different than the value of the cabhSec2FwPolicySuccessfulFileURL MIB, then the PS element MUST immediately download the named file from the configured server.[69]

5. The PS MUST compute a SHA-1 hash over the entire contents of the Firewall Configuration File and compare the computed hash to the hash represented by the value of the cabhSec2FwPolicyFileHash MIB object. If the computed hash and the value of the cabhSec2FwPolicyFileHash MIB object are the same, the integrity of the Firewall Configuration File is verified and the PS MUST use Firewall Configuration File to configure the firewall, otherwise the PS MUST reject the file.

7.4.4.4 Configuration File Processing and Status Reporting Requirements

The PS MUST report configuration file download status and error conditions using the Event Reporting process described in Section 6.3.3.2 CMP Event Reporting Function.

Table 7-14 identifies success and failure modes that might be encountered with PS Configuration File download and processing, and the action that the PS MUST take when it detects these modes.[70]

Table 7-14 — Configuration File Processing Conditions

Configuration File Processing Condition	Action
TFTP failed - Get Request sent, no response received	Report an event (Event ID 68000500) and retry TFTP.
HTTPS failed - Get Request sent, no response received or failed to connect with HTTPS server.	Report an event (Event ID 68002000) and retry HTTPS.
TFTP failed - configuration file not found	Report an event (Event ID 68000600) and retry TFTP.
HTTPS failed - configuration file download attempt failed and maximum number of retries not exceeded.	Report an event (Event ID 68003000) and retry HTTPS.
TFTP failed - out of order packets	Report an event (Event ID 68000700) and retry TFTP.
TFTP download failed - configuration file download attempt failed and maximum allowable number of retries have been done.	Report an event (Event ID 68000900) and reset.
HTTPS failed - configuration file download attempt failed and maximum allowable number of retries have been done.	Report an event (Event ID 68003100) and reset.
Configuration file download successful	Report an event (Event ID 68001000 if download was done using TFTP (TLS was not used) or Event ID 68003200 if download was done using HTTPS/TLS), and begin configuration file check or authentication.

[69] Revised this step per ECN CH1.1-N-03035 by GO on 07/03/03.
[70] Revised Table 7-14 per ECN CH1.1-N-03063 and CH1.1-N-03.0099-3 by GO on 10/28/03 and 12/9/03.

EXHIBIT A

Configuration File Processing Condition	Action
Configuration file fails authentication check	Report an event (Event ID 68000800) and reset. Do not attempt to process the file.
Configuration File is too large	Report an event (Event ID 73040102) and reset. Do not attempt to process the file.
No End Of Data marker	Report an event (Event ID 7340102) and reset. Do not attempt to process the file.
Duplicate TLV-27 or TLV-28 OID	Report an event (Event ID 73040102), reject the configuration file, and reset. Preserve all object values that existed before the attempt to process this bad configuration file. The PS is not required to restore MIB objects to the values they were assigned before the attempt to process the configuration file if the single SNMP PDU created from TLV-27 parameters has been set. Refer to the Post-trigger Operation section.
Duplicate TLV-9, TLV-21, TLV-32, TLV-33 or duplicate Sub-TLV in a single TLV-34, TLV-38, TLV-43.	Report an event (73040102), reject the configuration file, and reset. Preserve all objects that existed before the attempt to process this bad configuration file.
Recognized Type but bad Value or valid TLV-27 or TLV-28 OID but bad MIB value	Report an event (Event ID 73040102), reject the configuration file, and reset. Preserve all object values that existed before the attempt to process this bad configuration file. The PS is not required to restore MIB objects to the values they were assigned before the attempt to process the configuration file if the single SNMP PDU created from TLV-27 parameters has been set. Refer to the Post-trigger Operation section.
An unrecognized SNMP OID is encountered	Disregard the subject TLV and report an event (Event ID 73040100). Continue to process the file.
Type field is not valid for CableHome PS	Disregard the subject TLV and report an event (Event ID 73040101). Continue to process the file.

Refer to Appendix II for a list of events including those listed in Table 7-14 and for information about how events are reported.

7.4.4.4.1 Unsuccessful Configuration File Download Attempt - TFTP or HTTPS Retries Permitted

If the PS Configuration File Retry Counter is less than 5 and the TFTP or HTTPS Get Request times out, the PS Configuration File is not found on the server, or the TFTP or HTTPS Get failed due to out of order packets, the PS MUST initiate operation of the CDS and CNP functions, report the appropriate event, and retry the attempt to download the PS Configuration File, in accordance with the retry algorithm described in Section 7.4.4.2.4 Post-trigger Operation.

If the Firewall Configuration File Retry Counter is less than 5 and the TFTP or HTTP Get Request times out, the Firewall Configuration File is not found on the server, or the TFTP or HTTP Get failed due to out of order packets, the PS MUST continue normal operations, report the appropriate event, and retry the attempt to download the Firewall Configuration File, in accordance with the retry algorithm described in Section 7.4.4.2.4 Post-trigger Operation.

7.4.4.4.2 Unsuccessful Configuration File Download Attempt - TFTP or HTTPS Retries Exhausted

If the PS Configuration File Retry Counter is equal to 5 and the PS has not successfully downloaded the PS Configuration File, the PS MUST report the event identified in Table 7-14, "Configuration File Processing Conditions," on page 135 for indicating failure of the PS Configuration File download process and release

EXHIBIT A

its PS WAN-Man IP address in accordance with [RFC 2131], and restart the WAN-Man IP address acquisition process via DHCP.

If the Firewall Configuration File Retry Counter is equal to 5 and the PS has not successfully downloaded the PS Configuration File, the PS MUST report the event identified in Table 7-14 Configuration File Processing Modes for indicating failure of the Firewall Configuration File download process and continue normal operations. If the Firewall Configuration File is not successfully downloaded the PS MUST function as it did prior to the failed Firewall Configuration File download attempt.

7.4.4.4.3 Successful PS Configuration File Download

Successful download of the PS Configuration File is defined as complete and correct reception by the PS element the contents of the PS Configuration File within the TFTP timeout period and computation by the PS the hash values for the PS Configuration File with no errors resulting from the computation.

If the PS successfully downloads the PS Configuration File, the PS MUST reset the PS Configuration File Retry Counter to zero and report the event identified for 'Failure Mode' TFTP Download Successful in Table 7-14 Configuration File Processing Modes.

7.4.4.4.4 Unsuccessful PS Configuration File Download[71]

If the PS Configuration File fails the Configuration File Check as specified in Section 7.4.4.3 Configuration File Check and SNMP Provisioning Mode Authentication Requirements or in Section 11.9 PS Configuration File Security in DHCP Provisioning Mode, the PS MUST stop the provisioning process, reject the PS Configuration File, report the appropriate event, and restart the WAN-Man IP acquisition process via DHCP.

If the PS Configuration File contains no End-of-Data TLV (TLV-255), no PS MIC TLV (TLV-53), or is too large to process, the PS MUST stop the provisioning process, reject the PS Configuration File, report the appropriate event, and restart the WAN-Man IP address acquisition process via DHCP.

If the PS Configuration File contains duplicate TLV-27 or TLV-28 elements (duplicate means two or more SNMP MIB objects have an identical object identifier (OID)), the PS MUST stop the provisioning process, reject the PS Configuration File, report the appropriate event, and restart the WAN-Man IP address acquisition process via DHCP.

If the PS Configuration File contains a recognized Type field but bad Value field or a valid TLV-27 or TLV-28 OID with a bad MIB value, the PS MUST stop the provisioning process, reject the PS Configuration File, report the appropriate event, and restart the WAN-Man IP address acquisition process via DHCP.

If the PS Configuration File contains an unrecognized Type field or aTLV-27 or TLV-28 element with an unrecognized OID, the PS MUST ignore that TLV, report the appropriate event, and continue processing the PS Configuration File.

If the PS completes the processing of the single SNMP PDU created from the TLV-27 parameter then discovers duplicate TLV-28 elements, or TLV-28 elements with bad Value, the PS is not required to restore the MIB objects changed by the TLV-27 parameter back to their previous values, before rejecting the configuration file, reporting the event, and resetting the PS.

[71] Revised paragraphs 3, 4, and 5; added paragraph 6 per ECN CH1.1-N-03.0103-3 by GO on 12/5/03.

EXHIBIT A

7.4.4.4.5 Successful Firewall Configuration File Download

Successful download of the Firewall Configuration File is defined as complete and correct reception of the file by the PS element within the TFTP or HTTPS timeout period and error-free file validation as defined by the integrity check procedure described in Section 7.4.4.3 Configuration File Check and SNMP Provisioning Mode Authentication Requirements . After the PS successfully downloads the Firewall Configuration File, the PS MUST update the cabhSec2FwPolicySuccessfulFileURL MIB with the same value as the cabhSec2FwPolicyFileURL MIB.[72]

If the PS successfully downloads the Firewall Configuration File, the PS MUST reset the Firewall Configuration File Retry Counter to zero and report Event ID 80013500 (ref.: Table II-1 Defined Events for CableHome). After the PS successfully downloads and processes the Firewall Configuration File, the firewall MUST function as configured by the downloaded file.[73]

7.4.4.4.6 Unsuccessful Firewall Configuration File Download[74]

If the Firewall Configuration File fails the Configuration File Check as specified in Section 7.4.4.3 Configuration File Check and SNMP Provisioning Mode Authentication Requirements, the PS MUST continue normal operations, reject the Firewall Configuration File and report the appropriate event identified in Table II-1 Defined Events for CableHome.

If the Firewall Configuration File contains duplicate TLV-27 or TLV-28 elements (duplicate means two or more SNMP MIB objects have an identical object identifier (OID)), the PS MUST continue normal operations, reject the Firewall Configuration File and report the appropriate event identified in Table II-1 Defined Events for CableHome.

If the Firewall Configuration File contains a recognized Type field but bad Value field or a valid TLV-27 or TLV-28 OID with a bad MIB value, the PS MUST continue normal operations, reject the Firewall Configuration File and report the appropriate event identified in Table II-1 Defined Events for CableHome.

If the Firewall Configuration File contains an unrecognized Type field or a TLV-28 element with an unrecognized OID, the PS MUST ignore that TLV, report the appropriate event identified in Table II-1 Defined Events for CableHome, and continue processing the Firewall Configuration File.

If the download of the Firewall Configuration File fails for any reason, the firewall MUST function as configured prior to the failed download attempt.

7.5 PS Function - Time of Day Client

7.5.1 Time of Day Client Function Goals

The goal of the Time of Day client function of the PS is to acquire the current time of day from the Time of Day server in the cable operator's network.

7.5.2 Time of Day Client Function System Design Guidelines

The guideline identified in Table 7-15 guided specification of the capabilities defined for the PS Time of Day Client function:

[72] Revised this paragraph per ECN CH1.1-N-03035 by GO on 07/03/03.

[73] Revised the first sentence of this paragraph per ECN CH1.1-N-03069 by GO on 10/28/03.

[74] Revised paragraph 2 and 3 per ECN CH1.1-N-03.0103-3 by GO on 12/5/03.

EXHIBIT A

Table 7-15 — Time of Day Client System Design Guidelines

Number	Time of Day Client System Design Guidelines
TOD 1	CableHome will provide a mechanism by which the PS can achieve time synchronization with the Headend network

7.5.3 Time of Day Client Function System Description

The Portal Services element makes use of an [RFC 868] compliant Time of Day client, in order to achieve time synchronization with a time server on the Headend network. Time synchronization is essential for PS security functions as well as event messaging.

When the CDC DHCP client requests an IP Address - from the Headend DHCP server - for the WAN-Man interface, the DHCP client will receive the IP address of the Headend ToD server within DCHP Option 4. The DHCP client will also receive the Time Offset (from UTC), within DHCP Option 2.

Once the WAN-Man IP stack begins use of the IP address it received from DHCP, it should send an[RFC 868] time query to the ToD Server. If the ToD server responds with a valid response, the PS will begin using this time of day for event message time stamps and security functions.

7.5.4 Time of Day Client Function Requirements[75]

The Portal Services element MUST implement a Time of Day Client.

The Portal Services Time of Day Client MUST comply with the Time of Day Protocol [RFC 868] and make use of the UDP Protocol only.

Upon reset, before the PS synchronizes with a Time of Day server, the Portal Services Element MUST initialize its time to 00:00.0 (midnight) GMT, January 1, 1970.

If the PS receives DHCP Option 4 (Time Server Option) in the DHCP ACK, the PS MUST save the IP address of the Time Server from which the PS accepted a response as the value of cabhPsDevTimeServerAddr.

An Embedded PS MUST use the most recent valid time of day acquired from the ToD server for the system time of day clock, even if this means overwriting the system time acquired by the CM or overwriting the system time originally initialized to epoch time (00:00.0 (midnight) GMT, January 1, 1970).

If the value of cabhPsDevTodSyncStatus is true(1), i.e., if local time has already been established, it is not necessary for the Time of Day client to issue a ToD request.

The PS MUST send and receive ToD messages only through its WAN-Man Interface.

The PS MUST use the value of cabhPsDevDateTime for any functions requiring time of day, and which need only be accurate to the nearest second.

The CableHome Time of Day acquisition process is comprised of two phases: the Initial Time of Day Synchronization Attempt (Initial Attempt) phase and the Time of Day Synchronization Retry (Retry) phase. If the PS is successful synchronizing Time of Day with the Time of Day server during the Initial Attempt phase, it does not initiate the Retry phase. The PS is required to enter the Initial Attempt phase and attempt synchronization with a Time of Day server upon receipt of a DHCP ACK message, if the value of

[75] Revised this section per ECN CH1.1-N-03.0097-3 by GO on 12/9/03.

EXHIBIT A

cabhPsDevTodSyncStatus is false(2). Section 7.5.4.1 describes the required Initial Attempt behavior for the PS. Section 7.5.4.2 describes the required behavior for the PS if it is required to initiate the ToD Retry phase.

7.5.4.1 Initial Time of Day Synchronization Attempt Requirements

If the PS is operating in DHCP Provisioning Mode or SNMP Provisioning Mode (cabhPsDevProvMode = dhcpmode(1) or snmpmode(2)), the PS MUST attempt to synchronize with a Time of Day server whose address was passed to the PS in DHCP Option 4 of the DHCP ACK message, in accordance with [RFC 868]. A PS operating in Dormant CableHome Mode is not required to attempt to synchronize with a Time of Day server.

If the PS is not successful in synchronizing with a Time of Day (ToD) server on its first attempt, the PS MUST attempt to synchronize with the next ToD server in the order listed in DHCP Option 4, until it successfully synchronizes with a server, OR until it makes an unsuccessful attempt with each listed ToD server.

If the PS successfully synchronizes with a Time of Day server, the PS MUST do the following:

- set the value of cabhPsDevTodSyncStatus to true(1)
- set the value of cabhCdpServerTimeOffset with the value of DHCP Option 2 (Time Offset) from the DHCP ACK message
- set the value of cabhPsDevDateTime equal to the acquired time, plus the value of DHCP Option 2 from the DHCP ACK message (local time)
- set the value of cabhPsDevTimeServerAddr with the IP address of the Time of Day server with which the PS synchronized its time
- if the PS CDS function has current LAN IP address leases, update cabhCdpLanAddrCreateTime with the value of cabhPsDevDateTime and set the value of cabhCdpLanAddrExpire time equal to cabhCdpLanAddrCreateTime, plus the value of cabhCdpServerLeaseTime, for each active lease
- continue with the Provisioning Process as defined in Section 13

If an embedded PS operating in DHCP Provisioning Mode is not successful in synchronizing with any of the Time of Day servers listed in DHCP Option 4 of the DHCP ACK message, after attempting to do so once with each listed ToD server, the embedded PS MUST attempt to acquire system time from the cable modem. The embedded PS operating in SNMP Provisioning Mode is not required to attempt to acquire system time from the cable modem.

If the embedded PS operating in DHCP Provisioning Mode is not successful in synchronizing with any Time of Day servers on its first attempt with each AND is successful acquiring system time from the cable modem, the embedded PS MUST do the following:

- set the value of cabhPsDevTodSyncStatus to false(2)
- set the value of cabhPsDevDateTime to the cable modem's system time
- if the embedded PS CDS function has current LAN IP address leases, update cabhCdpLanAddrCreateTime with the value of cabhPsDevDateTime (cable modem's time) and set the value of cabhCdpLanAddrExpire time equal to cabhCdpLanAddrCreateTime, plus the value of cabhCdpServerLeaseTime, for each active lease
- initiate the Time of Day Synchronization Retry process defined in Section 7.5.4.2 AND continue with the Provisioning Process defined in Section 13.

An embedded PS operating in DHCP Provisioning Mode that is not successful in synchronizing with any Time of Day server on its first attempt with each and is not successful in acquiring system time from the cable modem, MUST do the following:

EXHIBIT A

- set the value of cabhPsDevTodSyncStatus to false(2)
- set the value of cabhPsDevDateTime to epoch time (00:00.0 (midnight) GMT, January 1, 1970)
- if its CDS function has current LAN IP address leases, update cabhCdpLanAddrCreateTime with the value of cabhPsDevDateTime (epoch time) and set the value of cabhCdpLanAddrExpire time equal to cabhCdpLanAddrCreateTime plus the value of cabhCdpServerLeaseTime, for each active lease
- initiate the Time of Day Synchronization Retry process defined in Section 7.5.4.2 AND continue with the Provisioning Process defined in Section 13.

A standalone PS operating in DHCP Provisioning Mode that is not successful in synchronizing with any Time of Day server on its first attempt with each, MUST do the following:

- set the value of cabhPsDevTodSyncStatus to false(2)
- set the value of cabhPsDevDateTime to epoch time (00:00.0 (midnight) GMT, January 1, 1970)
- if its CDS function has current LAN IP address leases, update cabhCdpLanAddrCreateTime with the value of cabhPsDevDateTime (epoch time), and set the value of cabhCdpLanAddrExpire time equal to cabhCdpLanAddrCreateTime, plus the value of cabhCdpServerLeaseTime, for each active lease
- initiate the Time of Day Synchronization Retry process defined in Section 7.5.4.2 AND continue with the Provisioning Process defined in Section 13.

A PS operating in SNMP Provisioning Mode that is not successful in synchronizing with any Time of Day server listed in DHCP Option 4 of the DHCP ACK message on its first attempt with each, MUST initiate the Time of Day Synchronization Retry process defined in Section 7.5.4.2. A PS operating in SNMP Provisioning Mode that is not successful in synchronizing with any Time of Day server MUST NOT continue with the Provisioning Process defined in Section 13.

7.5.4.2 Time of Day Synchronization Retry Requirements

If a PS operating in DHCP Provisioning Mode is not successful in synchronizing with any Time of Day server listed in Option 4 of the DHCP ACK message AND cabhPsDevTodSyncStatus = false(2), the PS MUST continue to attempt to synchronize with the Time of Day servers listed in Option 4 of the DHCP ACK message until it is successful.

While the value of cabhPsDevTodSyncStatus = false(2), a PS operating in SNMP Provisioning Mode MUST continue to attempt to synchronize with each of the Time of Day servers listed in Option 4 of the DHCP ACK message, for a total of six attempts (initial attempt plus five retries).

The PS Time of Day client MUST NOT exceed more than 3 ToD requests per Time of Day Server in any 5 minute period. At a minimum, a PS attempting to synchronize with a ToD server MUST issue at least 1 ToD request per 5 minute period.

A PS operating in SNMP Provisioning Mode that is not successful in synchronizing with any Time of Day server after attempting six times with each ToD server listed in Option 4 of the DHCP ACK message, MUST do the following:

- set cabhPsDevTodSyncStatus = false(2)
- log Event ID 68000403 (refer to Appendix II, Table II-1) according to the configured Priority for the event and following the procedure defined in Section 6.3.3.2 CMP Event Reporting Function
- restart the provisioning process beginning with issuing DHCP DISCOVER

EXHIBIT A

7.6 BP Function - DHCP Client

7.6.1 BP DHCP Client Function Goals

The goal of the BP DHCP client function is to acquire an IP address lease and configuration parameters for the BP from the system DHCP server.

7.6.2 BP DHCP Client Function System Design Guidelines

The guideline listed in Table 7-16 guided specification of the BP DHCP Client function.:

Table 7-16 — BP DHCP Client Function System Design Guidelines

Number	BP DHCP Client Function System Design Guidelines
BP DHC 1	CableHome will provide a means by which the BP can acquire a network address lease and configuration information.

7.6.3 BP DHCP Client Function System Description

The DHCP Client function of the BP is responsible for acquiring an IP address lease from a system DHCP server. The server could be the CDS Function of the CDP sub-element of the PS or it could be a DHCP server in the cable operator's data network, depending upon how the PS packet handling mode is configured. The BP DHCP Client function also acquires configuration information passed in DHCP Option fields from the system DHCP server.

7.6.4 BP DHCP Client Function Requirements

The BP MUST implement a DHCP client function in accordance with the Client requirements of [RFC 2131].

Upon reset the BP MUST issue a DHCP DISCOVER broadcast message to acquire an IP address lease.

The BP MUST support the DHCP Options and sub-options indicated as mandatory (M) in Table 7-17.

The BP MUST include the following DHCP option codes, in each DHCP DISCOVER and DHCP REQUEST message it sends:

- DHCP Option code 55 Parameter Request List
- DHCP Option code 60 Vendor Class Identifier, with the string "CableHome1.1BP" (with no spaces and without quotation marks)[76]
- DHCP Option code 255 End

[76] Revised this bullet statement per ECN CH1.1-N-03069 by GO on 10/28/03.

EXHIBIT A

Table 7-17 — BP DHCP Client Required DHCP Options

Option Number	Option Function	Support (M)andatory or (O)ptional	Factory Default Value
0	Pad	-	N/A
255	End	M	N/A
1	Subnet Mask	M	N/A
2	Time Offset	O	0
3	Router Option	M	N/A
6	Domain Name Server	M	N/A
7	Log Server	M	N/A
12	Host Name	O	N/A
15	Domain Name	M	Null String
23	Default Time-to-live	M	N/A
26	Interface MTU	M	N/A
43	Vendor Specific Information	M	Vendor Selected
50	Requested IP Address	M	null value or vendor selected
51	IP Address Lease Time	M	N/A
54	Server Identifier	M	N/A
55	Parameter Request List	M	N/A
60	Vendor Class Identifier	M	"CableHome1.1BP"
61	Client-identifier	O	N/A

EXHIBIT A

8 PACKET HANDLING & ADDRESS TRANSLATION

8.1 Introduction/Overview

8.1.1 Goals

The key goals which drive the CableHome packet handling capabilities include:

- Provide cable friendly address translation functionality, enabling cable operator visibility and manageability of home devices while preserving cable based sourced based routing architectures.
- Prevent unnecessary traffic on the cable and home network.
- Conservation of globally routable public IP addresses as well as cable network private management addresses.
- Facilitate in-home IP traffic routing by assigning network addresses to LAN IP Devices such that they reside on the same logical subnetwork.

8.1.2 Assumptions

- It is assumed that when cable operator provisioning servers provide multiple globally routable IP addresses to customer devices in a home, these addresses will not necessarily reside on the same subnet.
- Changing Internet service providers is assumed to occur relatively infrequently, occurring at a rate similar to a household changing its primary long distance carrier.

8.2 Architecture

This section describes the key concepts behind the CableHome packet handling and address translation functionality.

8.3 PS Logical Element - CableHome Address Portal (CAP)

The CableHome Address Portal (CAP) is a logical sub-element of the Portal Services logical element. Its functions are to route traffic between the LAN and the WAN, route LAN-to-LAN traffic, and to perform address and port translation functions.

8.3.1 CAP Goals

The goals of the CAP are listed below and in Section 8.1.1:

- Route IP packets between LAN IP Devices, and between LAN IP Devices and the Portal Services' default gateway on the WAN
- Provide Network and Port Address Translation (NAPT) capability for mapping between a single global IP address on the PS WAN Interface and one or more private IP addresses in the LAN
- Provide Network Address Translation (NAT) capability for 1-to-1 mapping between global IP addresses on the PS WAN Interface and private IP addresses on the LAN
- Keep traffic between LAN IP Devices on the LAN and do not permit it to traverse the WAN

8.3.2 CAP System Design Guidelines

The system design guidelines listed in Table 8-1 guided specification of the CableHome Address Portal functionality.

EXHIBIT A

Table 8-1 – CAP System Design Guidelines

Number	CAP System Design Guideline
CAP 1	CableHome addressing mechanisms will be MSO controlled, and will provide MSO knowledge of and accessibility to CableHome devices.
CAP 2	CableHome addressing will do nothing that will compromise current cable network routing architectures (for example source based routing, MPLS).
CAP 3	CableHome traffic management mechanisms will insulate the cable network from traffic generated by in house peer-to-peer communications.
CAP 4	IP Addresses will be conserved when possible (both globally routable addresses and private cable network management addresses)

8.3.3 CAP System Description

CableHome address translation and packet handling functionality is provided by the functional entity known as the CableHome Addressing Portal (CAP). The CAP encompasses the following address translation and packet forwarding elements:

- CableHome Address Translation (CAT)
- CableHome Passthrough Function
- Upstream Selective Forwarding Switch (USFS)

As shown in Figure 8-1, the CAT function provides a mechanism to interconnect the WAN-Data address realm and LAN-Trans address realm (via address translation), while Passthrough provides a mechanism to interconnect the WAN-Data address realm and the LAN-Pass address realm (via bridging). The CAT function is compliant with Traditional Network Address Translation (NAT) [RFC 3022] section 2. As with Traditional NAT, there are two variations of CAT, referred to as CableHome Network Address Translation (C-NAT) Transparent Routing and CableHome Network Address and Port Translation (C-NAPT) Transparent Routing. C-NAT Transparent Routing is the CableHome compliant version of Basic NAT [RFC 3022] section 2.1 and C-NAPT Transparent Routing is the CableHome compliant version of NAPT [RFC 3022] section 2.2.

Per [RFC 3022], C-NAT transparent routing is "a method by which IP addresses are mapped from one group to another, transparent to end users," and C-NAPT transparent routing "is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports." Also, per [RFC 3022], the purpose of C-NAT and C-NAPT functionality is to "provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses."

The CableHome Passthrough function is a CableHome specified bridging process that interconnects the WAN-Data Address Realm and the LAN-Pass Address Realm without address translation.

The Upstream Selective Forwarding Switch (USFS) defines a function within the CAP with the capability of confining home networking traffic to the home network, even when home networking devices generating this traffic reside on different logical IP subnets. Specifically, this function forwards traffic sourced from an IP address in one of the LAN Address realms, destined to IP addresses in one of the LAN Address realms, directly to its destination. This direct forwarding functionality prevents the traffic from traversing the HFC network, and interconnects the LAN-Trans and LAN-Pass Address Realms.

EXHIBIT A

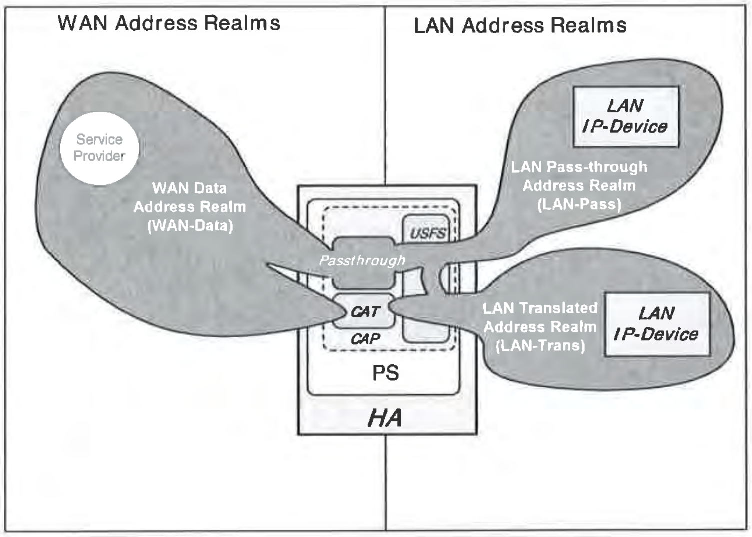

WAN Address Realms
LAN Address Realms
Service Provider
WAN Data Address Realm (WAN-Data)
LAN IP-Device
LAN Pass-through Address Realm (LAN-Pass)
USFS
Passthrough
CAT
CAP
LAN Translated Address Realm (LAN-Trans)
LAN IP-Device
PS
HA

Figure 8-1 – CableHome Address Portal (CAP) Functions

Throughout this document, the terms Address Binding, Address Unbinding, Address Translation, and Session are used as defined in [RFC 2663]. In addition, CableHome defines the term Mapping as the information required to perform C-NAT Transparent Routing and C-NAPT Transparent Routing.

In particular, a C-NAT Mapping is defined as a tuple of the form (WAN-Data IP address, LAN-Trans IP address) providing a one-to-one mapping between WAN-Data addresses and LAN-Trans addresses. Similarly, a C-NAPT Mapping is defined as a tuple of the form (WAN-Data IP address and TCP/UDP port, LAN-Trans IP address and TCP/UDP port) providing a one-to-many mapping between a single WAN-Data address and multiple LAN-Trans addresses. For ICMP traffic (such as ping), ICMP Identifier is used in place of the TCP/UDP port number.[77]

LAN-to-WAN traffic is defined as packets sourced by LAN IP Devices destined to devices on the WAN side of the PS. WAN-to-LAN traffic is defined packets sourced by WAN hosts destined to LAN IP devices. LAN-to-LAN traffic is defined as packets sourced by LAN IP Devices destined to LAN IP Devices on the same or different subnet.

8.3.3.1 Packet Handling Modes

The Portal Services element is configurable, via the cabhCapPrimaryMode MIB object, to operate in one of three Primary Packet-handling Modes when handling LAN-to-WAN and WAN-to-LAN traffic: Passthrough Mode, C-NAT Transparent Routing Mode, and C-NAPT Transparent Routing Mode. Further, the C-NAT or C-NAPT primary modes may also operate in a Mixed Mode described below.

[77] Revised this paragraph per ECN CH1.1-N-03061 by GO on 10/28/03.

EXHIBIT A

In Passthrough mode, the CAP acts as a transparent bridge [ISO/IEC10038] between the WAN-Data realm and LAN-Pass realm. In Passthrough mode, forwarding decisions are made primarily at OSI Layer 2 (data link layer). In this mode, the CAP does not perform any C-NAT or C-NAPT Transparent Routing functions. The PS bridging traffic for LAN-Pass IP devices is required to pass all OSI Layer 2 frames that a DOCSIS compliant cable modem is required to pass, including SNAP [ISO/IEC8802-2] and DIX Ethernet Version 2.0 [DIX] frames.[78]

The CAP supports OSI Layer 3 (network layer) forwarding in both the C-NAT Transparent Routing Mode and the C-NAPT Transparent Routing Mode, described below.

In C-NAT Mode, the PS element (CDC) acquires one or more IP addresses used for WAN-Data traffic during the PS boot process. After acquisition, via DHCP, these IP addresses are used as the WAN-Data IP address portion of Dynamically created C-NAT Mapping tuples. These WAN IP addresses make up a pool of addresses available for Dynamically created C- NAT Mappings. If an available IP address exists in the WAN-Data IP address pool, the CAP creates a Dynamic C-NAT Mapping when it first sees LAN-to-WAN IP traffic that does not have an existing Mapping. If no available IP address exists in the WAN-Data IP address pool, the Dynamic C-NAT Mapping can not be created, and this traffic is dropped, and an event is generated (see Appendix II).

The LAN-Trans IP address portion of the Dynamically created C-NAT Mapping tuples is provided by the pool of IP addresses defined by the cable operator in the CableHome CDP MIB. The CAP enters the tuple of the unique WAN-Data IP address and a unique LAN-Trans IP address in the CAP Mapping Table, along with other parameters including WAN and LAN Port numbers, the Mapping Method, and the transport protocol used for the Mapping. The port number will not be translated by the CAP for C-NAT Mappings: the source and destination port numbers in the UDP or TCP header will be unchanged. When the PS is operating in NAT primary packet handing mode (cabhCapPrimaryMode = nat(2)), the CAP will enter the value 0 into the WAN and LAN port number entries of the CAP Mapping Table. The CAP will also enter the value 0 into the WAN and LAN port number entries of the CAP Mapping Table for provisioned static port forwarding entries of the CAP Mapping Table when the PS is operating in NAPT primary packet handling mode (cabhCapPrimaryMode = napt(1)). For the case of a static port forwarding entry provisioned in the CAP Mapping Table for a PS operating in NAPT primary packet handling mode, the 0-value port number entry will serve two purposes: (1) indicate to the CAP that the port numbers are not to be translated, i.e., that the ports are "wild carded", and (2) indicate to anyone reading the CAP Mapping Table that this static port mapping is effectively a C-NAT mapping, thereby providing a distinction between static port forwarding entries (C-NAT mappings) (port number 0) and C-NAPT Mappings (nonzero port number). Refer to Section 8.3.3.2 Static Port Forwarding Wild Cards for more information about static port forwarding operation of the CAP.

Dynamic C-NAT Mappings for UDP traffic are destroyed when an inactivity timeout period, cabhCapUdpTimeWait, expires. Dynamic C-NAT Mappings for TCP traffic are destroyed when an inactivity timeout period, cabhCapTcpTimeWait, expires or a TCP session terminates. Dynamic C-NAT Mappings for ICMP traffic are destroyed when an inactivity timeout period, cabhCapIcmpTimeWait, expires. In addition, Static C-NAT Mappings may be created or destroyed when the NMS system writes to or deletes from the cabhCapMappingTable MIB table.

In C-NAPT Mode (the factory default mode for the system) the PS element (CDC) acquires one IP address, used for WAN-Data traffic. After acquisition, via DHCP, this IP address is used as the WAN-Data IP address portion of Dynamically created C-NAPT Mapping tuples. If the WAN-Data IP address has been acquired, Dynamic C-NAPT Mappings are created when the CAP first sees LAN-to-WAN IP traffic that does not have an existing Mapping. If the WAN-Data IP address has not been acquired (i.e. does not have an active DHCP lease), the Dynamic C-NAPT Mapping can not be created, and this traffic is dropped, and a standard event is generated (see Appendix II).

[78] Added a sentence to the end of this paragraph per ECN CH1.1-N-03070 by GO on 11/13/03.

EXHIBIT A

Dynamic C-NAPT Mappings for UDP traffic are destroyed when an inactivity timeout period, cabhCapUdpTimeWait, expires. Dynamic C-NAPT Mappings for TCP traffic are destroyed when an inactivity timeout period, cabhCapTcpTimeWait, expires or a TCP session terminates. Dynamic C-NAPT Mappings for ICMP traffic are destroyed when an inactivity timeout period, cabhCapIcmpTimeWait, expires. In addition, Static C-NAPT Mappings may be created or destroyed when the NMS system writes to or deletes from the cabhCapMappingTable MIB table.

Figure 8-2 shows a typical Dynamic C-NAPT Mapping process with a TCP packet. In this example, the PS is configured to operate in NAPT mode and already has obtained a WAN IP address, and the LAN IP Device has already obtained an IP in the LAN-Trans realm.

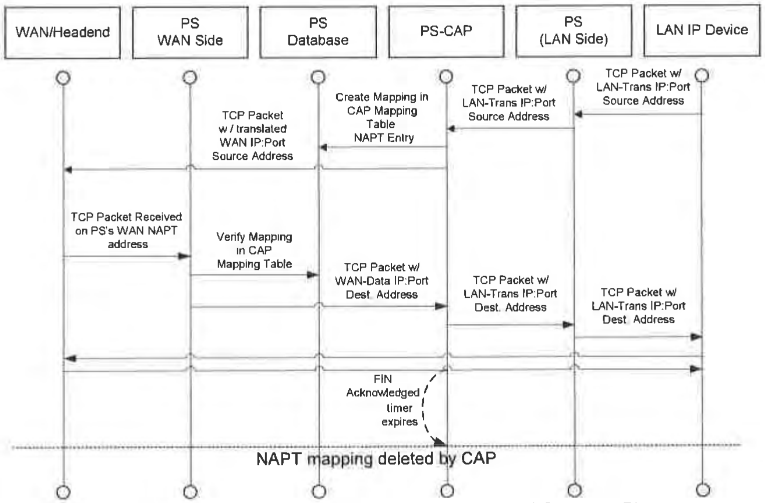

WAN/Headend
PS WAN Side
PS Database
PS-CAP
PS (LAN Side)
LAN IP Device
TCP Packet w/ LAN-Trans IP:Port Source Address
TCP Packet w/ LAN-Trans IP:Port Source Address
Create Mapping in CAP Mapping Table NAPT Entry
TCP Packet w / translated WAN IP:Port Source Address
TCP Packet Received on PS's WAN NAPT address
Verify Mapping in CAP Mapping Table
TCP Packet w/ WAN-Data IP:Port Dest. Address
TCP Packet w/ LAN-Trans IP:Port Dest. Address
TCP Packet w/ LAN-Trans IP:Port Dest. Address
FIN Acknowledged timer expires
NAPT mapping deleted by CAP

Figure 8-2 — PS Configuration (CAP Mapping Table - NAPT) Sequence Diagram

It is also possible for the PS to operate in a Mixed Bridging/Routing Mode. In this case, the NMS sets the primary mode to C-NAT or C-NAPT Transparent Routing, and the NMS writes one or more MAC addresses belonging to LAN IP Devices, whose traffic is to be bridged, into the Passthrough Table (cabhCapPassthroughTable). In this Mixed Mode, the PS examines MAC addresses of received frames to determine whether to transparently bridge the frame or to perform any C-NAT or C-NAPT Transparent Routing functions at the IP layer. In the case of LAN- to-WAN traffic, the PS examines the source MAC address, and if that MAC address exists in the cabhCapPassthroughTable, the frame is transparently bridged to the WAN-Data interface. In the case of WAN- to-LAN traffic, the PS examines the destination MAC address, and if that MAC address exists in the cabhCapPassthroughTable, the frame is transparently bridged to the appropriate LAN interface. If the MAC address does not exist in the cabhCapPassthroughTable, the packet is processed by higher layer functions, including the C-NAT/C-NAPT Transparent Routing function.

It is assumed that when the PS is in Routing mode (C-NAT/C-NAPT), that it will process broadcast traffic in accordance with [RFC 919], [RFC 922], [RFC 1812], and [RFC 2644]. It is also assumed that when the PS is in Passthrough Mode, that broadcast traffic will be bridged to all interfaces.

EXHIBIT A

When the PS is in Mixed Bridging/Routing Mode, and receives broadcast traffic sourced from a device in Passthrough Table, the PS is expected to bridge the broadcast to all interfaces. When the PS is in Mixed Bridging/Routing Mode, and receives broadcast traffic on any WAN interface, the PS is expected to bridge the broadcast to all LAN interfaces.

It should be noted that the USFS functionality (Section 8.3.3.4) is applied in each of the three primary packet- handling modes, and regardless of whether or not Mixed mode is in use. USFS forwarding decisions will take precedence over other forwarding decisions that could potentially forward traffic from the LAN to the WAN.

8.3.3.2 CAP DMZ Functionality (Static Port Forwarding with Port Wild Cards)[79]

When the PS is provisioned to operate in C-NAPT primary packet handling mode and a C-NAPT mapping is statically created with both WAN and LAN port numbers set to zero (i.e. when a DMZ entry has been created), then the CAP will handle inbound traffic in a special way. The CAP will forward all WAN-to-LAN traffic not associated with an existing C-NAPT session or an existing C-NAPT static mapping to the LAN IP address (DMZ IP address) specified in this special type of C-NAPT mapping (DMZ entry).

The CAP will process packets as follows:

1. Check all incoming WAN-to-LAN packets to see if they are associated with an existing session specified by a C-NAPT dynamic mapping. If this is the case, then the packet is translated as specified and is forwarded.

2. If not, then the CAP checks to see if there is a static C-NAPT mapping associated with the packet. If this is the case, then the packet is translated as specified and is forwarded.

3. If not, then the CAP checks to see if there is a static C-NAPT mapping for this WAN IP address with the port number set to 0. If this is the case, then the CAP translates the IP address to the LAN IP Address specified in this special C-NAPT static mapping. Note that C-NAPT does not translate the port in this case. After the address translation, the packet is forwarded.

Note: If none of the above is true, the packet is dropped.

When a DMZ entry is created in the CAP for a LAN IP address that is dynamically assigned by the PS (CDS), the PS is required to create an IP address lease reservation for that address. This ensures that the IP address of the LAN device that is set-up for the DMZ functionality does not change upon lease renewal. The PS can look up the DMZ IP address in the cabhCdpLanAddrTable. If a corresponding entry exists in this table with the value of cabhCdpLanAddrMethod equal to either dynamicActive(4) or dynamicInactive(3), then the PS is required to replace that row entry with one that represents an IP address lease reservation, that is, one with the value of cabhCdpLanAddrMethod equal to either reservationActive(2) or reservationInactive(1), respectively. If there is no entry corresponding to the DMZ IP address in the cabhCdpLanAddrTable, then the PS is not required to create an IP address lease reservation for that IP address. In this case, it is possible that the DMZ IP address is statically assigned to the LAN IP Device.

8.3.3.3 Virtual Private Network (VPN) Support in the CAP

CableHome 1.1 requires the PS to implement a *VPN Passthrough* feature that allows IPSec [RFC 2401]-based VPN clients to exchange keys using Internet Key Exchange protocol [RFC 2409]. CableHome 1.1 will support a single VPN client in the home at a time, and that client is assumed to satisfy the following conditions:

[79] Revised title and contents of this section per ECN CH1.1-N-03.0092-4 by GO on 12/5/03.

EXHIBIT A

- the LAN IP Device is in the LAN-Trans realm, i.e., it has a LAN-Trans IP address
- the LAN IP Device uses IPSec as the VPN protocol
- the LAN IP Device uses Internet Key Exchange to dynamically exchange encryption keys with the VPN server

CableHome 1.1 does not limit the number of VPN clients in the LAN-Pass realm (i.e., LAN IP Devices whose MAC address is in the PS Passthrough Table) that can simultaneously access VPN servers outside the home.

For the VPN client to operate properly a firewall policy file must be active in the PS that opens the proper ports for incoming (WAN-to-LAN) traffic, most notably port 500, for IKE traffic.

When keys are dynamically exchanged using IKE [RFC 2406] prior to initiation of an IPSec session the CAP will translate network addresses as usual and will additionally associate port 500 as an inbound port for the private (LAN-Trans) IP address of the device that initiated the VPN connection. This will ensure that incoming IKE messages will be properly forwarded to the VPN client. IPsec sessions are defined in the CAP by the port used for inbound and outbound traffic, the port used for key exchange, the VPN server address and the VPN client address.

Even though the firewall has opened port 500, incoming traffic on port 500 will only be forwarded by the CAP after an IPSec session has been initiated by a client in the LAN-Trans address realm.

If a second VPN client in the home attempts to initiate an IPsec session with a different VPN server the CAP will shift the ports used on the WAN-Data IP address for traffic and key exchange and translate these ports to the standard ports on the VPN Client IP address in the LAN-Trans realm. Additional VPN clients can be supported as well. However, the CAP does not support more than one VPN client in the home connecting to the same VPN server.

IPsec has three modes that can be used for VPNs. The PS is required to support Encapsulating Security Payload Tunneling mode [RFC 2406]. Support for Encapsulating Security Payload Transport mode [RFC 2406] and IP Authentication Header mode [RFC 2402] are not required.

8.3.3.4 Upstream Selective Forwarding Switch Overview

In some cases, a LAN IP Device in the LAN-Pass address realm will reside on a different logical IP subnet than other LAN IP Devices connected to the same PS element. It is important to prevent the traffic between these LAN IP Devices from traversing the HFC network. Preventing this unwanted HFC traffic is the function that is provided by the Upstream Selective Forwarding Switch (USFS).

Specifically, the USFS routes traffic - that is sourced from within the home network and is destined to the home network - directly to its destination. LAN IP Device sourced traffic whose destination IP address is outside the LAN address realm is passed unaltered to the CAP bridging/routing functionality.

The USFS functionality makes use of the IP Address Translation Table (as defined in [RFC 2011]) within the PS element. This table, the [RFC 2011] ipNetToMediaTable, contains a list of MAC Addresses, their corresponding IP Addresses, and PS Interface Index numbers of the physical interfaces that these addresses are associated with. The USFS will refer to this table in order to make decisions about directing the flow of LAN-to-WAN traffic. In order to populate the ipNetToMediaTable the PS learns IP and MAC addresses and their associations. For every associated physical interface, the PS learns all of the LAN-Trans and LAN-Pass IP addresses along with their associated MAC bindings, and this learning can occur via a variety of methods. Vendor specific IP/MAC address learning methods may include: ARP snooping, traffic monitoring, and consulting CDP entries. Entries are purged from the ipNetToMediaTable after a reasonable inactivity timeout period has expired.

EXHIBIT A

The USFS inspects all IP traffic received on PS LAN interfaces. If the destination IP address is found (via the ipNetToMediaTable) to reside on a PS LAN interface, the original frame's data-link destination address is changed from that of the default gateway address to that of the destination LAN IP Device, and the traffic is forwarded to the QoS Forwarding and Media Access (QFM) functionality (ref.: Section 10.2 PS Logical Element CQP) in the PS to be forwarded out on the proper PS LAN interface according to the packet priority. If a match to the destination IP address is not found in the ipNetToMediaTable, the packet is passed, in its original form, to the C-NAT/C-NAPT transparent routing function or the Passthrough bridging function (depending on the active packet handling mode).

8.3.3.5 Multicast

The CAP supports WAN-to-LAN Multicast traffic by transparently bridging downstream IGMP messaging [RFC 2236] and downstream IP Multicast packets. In addition, when in C-NAT/C-NAPT Transparent Routing Mode, the CAP performs address translation on upstream IGMP messages sourced by LAN IP Devices residing in the LAN-Trans domain. The CAP forwards WAN-originated IGMP traffic to the LAN to allow the advertisements to reach LAN IP Devices. A LAN IP Device will determine which multicast it wishes to join and will send a multicast "join" message. The multicast source will then be able to pass data to the LAN IP Device. When the multicast service is no longer desired, the LAN IP Device can either ignore the service and the stream will time out, or the LAN IP Device can send an IGMP "leave" message to the chain to tear down the streaming traffic. Figure 8-3 provides a detailed example of IGMP and Multicast processes passing through a PS.

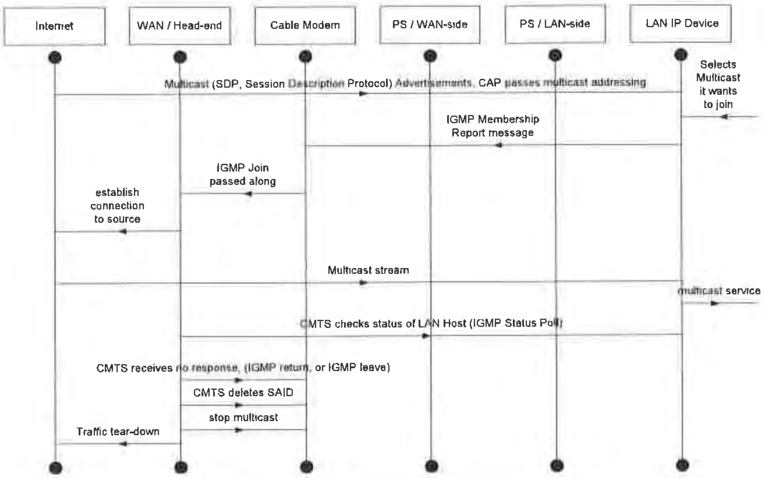

Internet
WAN / Head-end
Cable Modem
PS / WAN-side
PS / LAN-side
LAN IP Device
Selects Multicast it wants to join
Multicast (SDP, Session Description Protocol) Advertisements, CAP passes multicast addressing
IGMP Membership Report message
IGMP Join passed along
establish connection to source
Multicast stream
multicast service
CMTS checks status of LAN Host (IGMP Status Poll)
CMTS receives no response, (IGMP return, or IGMP leave)
CMTS deletes SAID
stop multicast
Traffic tear-down

Figure 8-3 – Multicast via IGMP Sequence

8.3.3.6 CableHome Packet Handling Examples

This section provides an informative look at processing involved for CableHome packet handling. Figure 8-4 shows an example of possible packet processing steps for LAN-to-WAN uni-cast traffic, and Figure 8-5 shows an example of possible packet processing steps for WAN-to-LAN uni-cast traffic.

Note: These examples are informative only and do not imply any requirements on implementation.

EXHIBIT A

LAN to WAN Frame Processing Flow

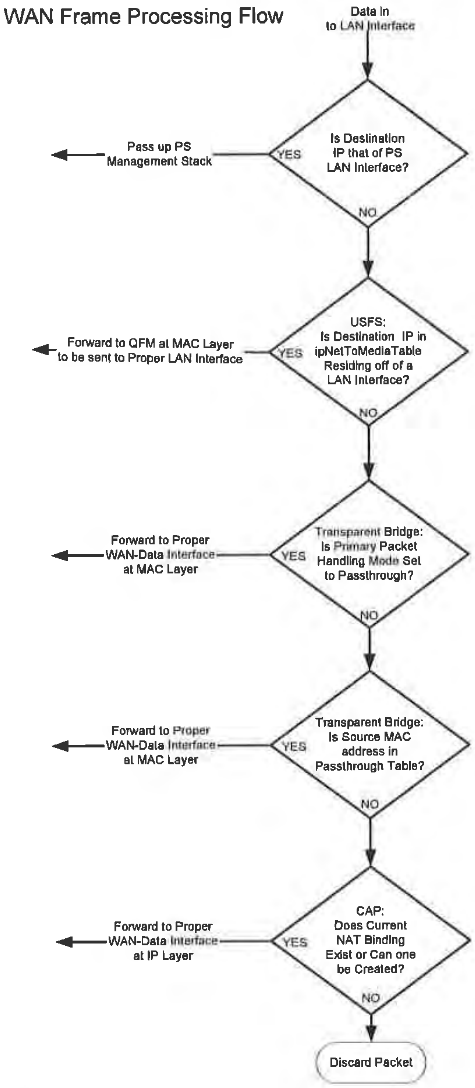


Figure 8-4 – LAN-to-WAN Packet Processing Example

EXHIBIT A

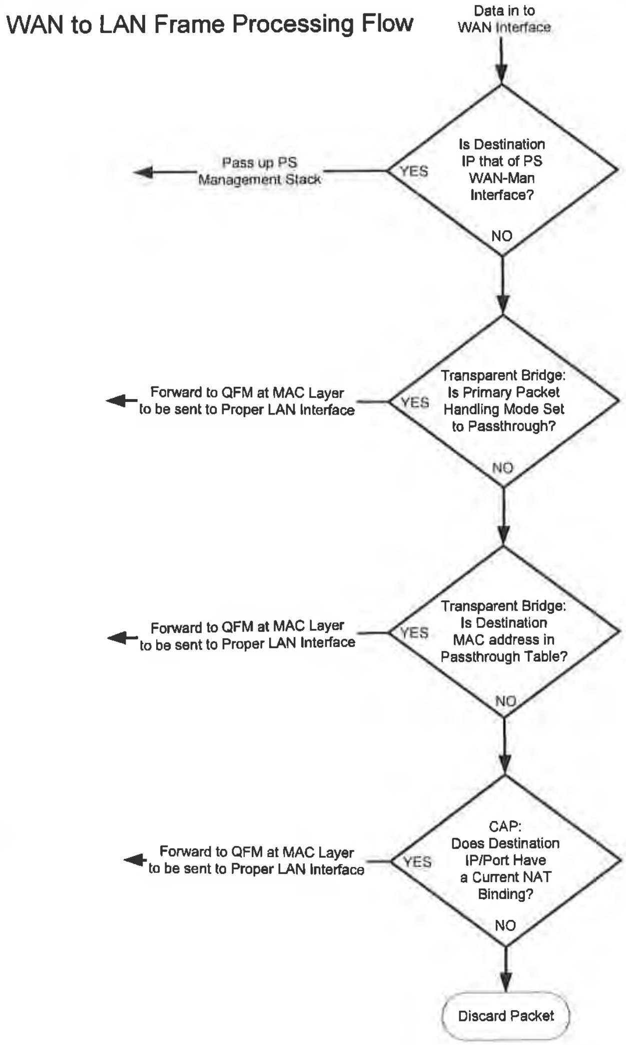

WAN to LAN Frame Processing Flow
Data in to WAN Interface
Is Destination IP that of PS WAN-Man Interface?
YES
Pass up PS Management Stack
NO
Transparent Bridge: Is Primary Packet Handling Mode Set to Passthrough?
YES
Forward to QFM at MAC Layer to be sent to Proper LAN Interface
NO
Transparent Bridge: Is Destination MAC address in Passthrough Table?
YES
Forward to QFM at MAC Layer to be sent to Proper LAN Interface
NO
CAP: Does Destination IP/Port Have a Current NAT Binding?
YES
Forward to QFM at MAC Layer to be sent to Proper LAN Interface
NO
Discard Packet

Figure 8-5 – WAN-to-LAN Packet Processing Example

EXHIBIT A

8.3.4 CAP Requirements[80]

8.3.4.1 General Requirements

All logical IP interfaces on the Portal Services element MUST be compliant with [RFC 1122] and [RFC 1123], Sections 3 and 4, to enable standard communication with Internet Hosts.

The PS MUST support WAN-to-LAN Multicast traffic by transparently bridging WAN-to-LAN IGMP messaging and WAN-to-LAN IP Multicast packets as defined in [RFC 2236].

If the Primary Packet-handling Mode, cabhCapPrimaryMode, is set to Passthrough, all LAN-to-WAN IGMP messaging MUST be transparently bridged.

If the Primary Packet-handling Mode, cabhCapPrimaryMode, is set to C-NAPT, the source IP address for all LAN-to-WAN IGMP messages, sourced from LAN IP Devices residing in the LAN-Trans Domain, MUST be translated to the WAN-Data IP address being used for C-NAPT mappings, and then forwarded out to the WAN.

If the Primary Packet-handling Mode, cabhCapPrimaryMode, is set to C-NAT, the source IP address for all LAN-to-WAN IGMP messages - sourced from LAN IP Devices residing in the LAN-Trans Domain that have an IP address that is part of an existing C-NAT mapping - MUST be translated to the WAN-Data IP address being used in that C-NAT mapping, and then forwarded out to the WAN.

8.3.4.2 Packet Handling Requirements

The PS MUST support Passthrough Mode, C-NAT Transparent Routing Mode, and C-NAPT Transparent Routing Mode, and the PS MUST support the selection of this Primary Packet-handling Mode, via the cabhCapPrimaryMode MIB object.

If the Primary Packet-handling Mode, cabhCapPrimaryMode, is set to C-NAT, the PS MUST make certain there exists an available Headend supplied IP address in the WAN-Data IP Address Pool (with a current DHCP lease) before attempting to use this IP address as part of a C-NAT Mapping. If the CAP is unable to create a C-NAT Mapping, due to WAN-Data IP Address Pool depletion, it MUST generate a standard event (as defined in Appendix II).

The PS MUST set the WAN and LAN port numbers (cabhCapMappingWanPort and cabhCapMappingLanPort, respectively) of the CAP Mapping Table equal to zero for each Dynamic C-NAT Mapping it creates.

If the cable operator creates or changes a row in the CAP Mapping Table, i.e., if a row is created via the static mapping method (cabhCapMappingMethod = static(1)), and the port number objects of the row (cabhCapMappingLanPort and cabhCapMappingWanPort) are not specified, the PS MUST enter zero for cabhCapMappingLanPort and cabhCapMappingWanPort for that row.

The PS MUST NOT translate the port number for any packet whose IP address appears in the CAP Mapping Table with a port number of zero.

If the Primary Packet-handling Mode, cabhCapPrimaryMode, is set to C-NAPT, the PS MUST make certain there exists a current WAN IP address (with a current DHCP lease from Headend provisioning) before attempting to use this IP address as part of a C-NAPT Mapping. If the CAP is unable to create a C-NAPT Mapping, due to not having a current WAN IP Address or due to port number depletion, it MUST generate a standard event (as defined in Appendix II).

[80] Removed subsection referring to USFS Requirements per ECN CH1.1-N-03.0077-4 by GO on 12/2/03.

EXHIBIT A

LAN-to-LAN uni-cast traffic MUST never be routed or bridged out a WAN interface.

When the DHCP lease of a WAN-Data IP address - that is part of C-NAT or C-NAPT mapping - expires, all mappings associated with that IP address MUST be deleted from cabhCapMappingTable.

8.3.4.3 Passthrough Requirements[81]

When the CAP's Primary Packet-handling Mode, cabhCapPrimaryMode, is set to Passthrough mode, the PS MUST act as a transparent bridge, as defined in [ISO DIS 10038 MAC Bridges], between the WAN-Data realm and LAN-Pass realm, and MUST NOT perform any C-NAT or C-NAPT Transparent Routing functions. A PS acting as a transparent bridge for LAN-Pass devices (cabhCapPrimaryMode = passthrough(3) or cabhCapPrimaryMode = napt(1) with entries in the cabhCapPassthroughTable) MUST transparently bridge all frame types that the DOCSIS specifications [[DOCSIS1]], [DOCSIS9] require a cable modem to pass. Even when the Primary Packet-handling Mode is set to Passthrough, USFS processing MUST take precedence over LAN-to-WAN bridging decisions.

8.3.4.4 C-NAT and C-NAPT Transparent Routing Requirements

When the Primary Packet-handling Mode (cabhCapPrimaryMode) is set to C-NAT the PS MUST support C-NAT address translation processes in accordance with the basic NAT requirements defined in [RFC 3022].

When the Primary Packet-handling Mode (cabhCapPrimaryMode) is set to C-NAPT the PS MUST support C-NAPT address translation processes in accordance with the basic NAPT requirements defined in [RFC 3022].

Regardless of the Primary Packet-handling Mode, the PS MUST support the creation and deletion of Static C-NAT and C-NAPT Mappings, by enabling the NMS system to read, create, and delete (via the CMP) Static CAP Mapping (cabhCapMappingTable) entries.

NMS created Static C-NAT and C-NAPT Mappings MUST persist across PS reboots.

The PS MUST support the creation of Dynamic C-NAT and C-NAPT Mappings, initiated by LAN-to-WAN TCP, UDP, or ICMP traffic. The PS MUST enable the NMS system to read (via the CMP) Dynamic CAP Mapping (cabhCapMappingTable) entries.

The PS MUST support the deletion of Dynamic C-NAT and C-NAPT Mappings if a given Mapping is associated with a TCP session and that TCP session terminates or the TCP inactivity timeout, cabhCapTcpTimeWait, for that Mapping elapses.

The PS MUST support the deletion of Dynamic C-NAT and C-NAPT Mappings if a given Mapping is associated with a UDP session and the UDP inactivity timeout, cabhCapUdpTimeWait, for that Mapping elapses.

The PS MUST support the deletion of Dynamic C-NAT and C-NAPT Mappings if a given Mapping is associated with an ICMP session and the ICMP inactivity timeout, cabhCapIcmpTimeWait, for that Mapping elapses.

Dynamic C-NAT and C-NAPT Mappings MUST NOT persist across PS reboots.

[81] Revised this paragraph per ECN CH1.1-N-03070 by GO on 11/13/03.

EXHIBIT A

8.3.4.5 Virtual Private Network Support Requirements

When the CAP is operating in C-NAT or C-NAPT Primary Packet-handling mode (as indicated by the value of cabhCapPrimaryMode), the PS MUST recognize IPSec sessions initiated by VPN clients in the LAN-Trans realm, create appropriate mappings in the CAP Mapping Table, and map port 500 for inbound (WAN-to-LAN) traffic to the LAN-Trans IP address bound to the LAN IP Device that initiated the session.

When the CAP is operating in C-NAT or C-NAPT Primary Packet-handling mode (as indicated by the value of cabhCapPrimaryMode) and it recognizes an IPSec session when another one has already been mapped in the CAP Mapping Table to a different VPN server, the PS MAY create mappings for the new session, e.g., by port shifting.

If inbound traffic on port 500 is received by the CAP and there is no active IPSec VPN session then the packets received through port 500 MUST be discarded.

The PS MUST support IPsec sessions using Encapsulating Security Payload Tunneling mode, [RFC 2406].

8.3.4.6 CAP DMZ Functionality Requirements[82]

When the Primary Packet-handling Mode (cabhCapPrimaryMode) is set to C-NAPT and there is a C-NAPT static mapping with the WAN port number and the LAN port number set to 0 (i.e. when a DMZ entry has been created in the CAP), then the PS MUST translate the IP addresses specified in the mapping (DMZ entry) for packets that are not associated with an existing dynamic or static C-NAPT mapping.

When a DMZ entry is created in the CAP Mapping Table for a LAN IP address that is dynamically assigned by the PS (CDS), the PS MUST create an IP address lease reservation for that address. The PS MUST determine if the DMZ IP address is dynamically assigned by the CDS, e.g., by looking it up in the cabhCdpLanAddrTable. If a corresponding entry exists in this table with the value of cabhCdpLanAddrMethod equal to either dynamicActive(4) or dynamicInactive(3), then the PS MUST replace that entry with one that represents a lease reservation for that IP address in the table, that is, one whose value of cabhCdpLanAddrMethod is set to either reservationActive(2) or reservationInactive(1), respectively. If there is no entry in the CAP Mapping Table corresponding to the DMZ IP address in the cabhCdpLanAddrTable, then the PS MUST NOT create a lease reservation for that IP address.

8.3.4.7 Mixed Bridging/Routing Mode Requirements

The PS MUST support Mixed Bridging/Routing Mode as described in Section 8.3, where the CAP Primary Packet-handling Mode, cabhCapPrimaryMode, is set to C-NAT or C-NAPT Transparent Routing and where the CAP will also transparently bridge traffic for particular MAC addresses. If the CAP Primary Packet-handling Mode, cabhCapPrimaryMode, is set to C-NAT or C-NAPT Transparent Routing and the NMS has written a MAC address, belonging to a LAN IP Device, into the cabhCapPassthroughTable, the PS MUST transparently bridge LAN-to-WAN traffic sourced by this MAC address and WAN-to-LAN traffic destined for this MAC address.

When in Mixed Bridging/Routing Mode, as described in Section 8.3, the USFS function MUST be applied to all LAN originated traffic received.

8.3.4.8 USFS Requirements[83]

Upstream Selective Forwarding Switch (USFS) functionality MUST be applied to packet processing, regardless of the CAP's packet-handling mode (Passthrough, C-NAT, C-NAPT, or mixed Bridging/Routing).

[82] Revised the title and contents of this section per ECN CH1.1-N-03.0092-4 by GO on 12/5/03.
[83] Section revised per CH1.1-N-03.0077-4, 27-jan-2004, ab

EXHIBIT A

The USFS function MUST inspect all IP traffic originating on PS LAN interfaces, to determine if the destination IP address of a packet is that of a device residing on a PS LAN interface. If the destination IP address in a packet inspected by the USFS is that of a LAN IP Device residing off of a PS LAN interface, the USFS function MUST replace the MAC Layer Destination address, within the packet's Layer 2 header, with the MAC address of that destination LAN IP Device and forward the frame to the QoS Forwarding and Media Access (QMA) entity (see Section 10.3.1) in the PS to be forwarded out on the proper physical LAN interface according to the packet priority.

The USFS MUST NOT forward any packet destined for a LAN IP Device out any WAN interface.

EXHIBIT A

9 NAME RESOLUTION

9.1 Introduction/Overview

9.1.1 Goals

The goals of the CableHome name resolution include:

- Provide Domain Name Service (DNS) from a server in the PS to DNS clients within LAN IP Devices, even during cable connection outages.
- Enable subscribers to refer to local devices via intuitive device names rather than by IP address.
- Via recursive queries to remote DNS servers, provide answers to LAN DNS clients when queried for resolution of non-local hostnames.
- Provide easy DNS service recovery upon re-establishment of cable connectivity after an outage.

9.1.2 Assumptions

The operating assumptions for CableHome naming services include:

- The DNS server in the PS element is the only DNS server authoritative for LAN IP Devices in the LAN-Trans realm.
- The PS element will not provide DNS service to LAN IP Devices in the LAN-Pass realm.
- If the PS element makes use of multiple WAN-Data addresses, the WAN DNS Server information obtained during the most recent WAN-Data address acquisition process (DHCP) will be used.

9.2 Architecture

9.2.1 System Design Guidelines

Table 9-1 – Name Resolution System Design Guidelines

Reference	System Design Guideline
Name Rsln 1	Provide Domain Name Service (DNS) from a server in the PS to DNS clients within LAN IP Devices, for name resolution of LAN IP Devices (independent of the state of the WAN connection).
Name Rsln 2	Provide DNS answers, via recursive queries beginning with a cable network DNS server, for DNS clients within LAN IP Devices, for resolution of non-local hostnames

9.2.2 System Description

This section provides an overview of the CableHome name resolution services within the PS element.

9.2.2.1 Name Resolution Functional Overview

The CableHome Naming Portal (CNP) is a service running in the PS that provides a simple DNS server for LAN IP Devices in the LAN-Trans address realm. However, CNP functionality for LAN-Trans address realm is bypassed if the cabhCdpServerDnsAddress MIB is set to the value other than

EXHIBIT A

cabhCdpServerRouter. The CNP is not used by LAN IP Devices in the LAN-Pass address realm, because they will be directly served by DNS servers external to the home.[84]

Typically, LAN IP Devices in the LAN-Trans realm are configured by the CDP to use the CNP as their Domain Name Server. The CNP service in the LAN-Trans realm does not depend on the state of the WAN connection. The CNP performs the following tasks:

- Resolves hostnames for LAN IP Devices, returning their corresponding IP addresses.
- Provide DNS answers, via recursive queries beginning with a DNS server in the cable network, for queries that cannot be resolved via local PS information. This action occurs only when WAN DNS server information is available in the PS. Otherwise, the CNP returns an error indicating that the name cannot be resolved.

Making the CNP the primary DNS server on the LAN avoids the need to reconfigure LAN IP Devices when the state of the WAN connection changes. It also permits changing external DNS server assignment without LAN IP Device reconfiguration.

9.2.2.2 Name Resolution Operation

When queried to resolve a hostname, the CNP function of the PS performs the lookup process shown in Figure 9-1. The CNP responds to initial standard DNS queries [RFC 1035], directed to cabhCdpServerDnsAddress, for all name lookups. It is the responsibility of the CNP to make recursive queries to external DNS servers - beginning with the first cabhCdpWanDnsServerIp entry in the CDP's cabhCdpWanDnsServerTable - when queried by a LAN IP Device and to respond to that LAN IP Device with either an answer or an error message.

The CNP relies on the CDP's cabhCdpLanAddrTable, to learn the hostnames associated with the current IP addresses of active LAN IP Devices. As long as a LAN IP Device maintains an active DHCP lease with the CDP and has provided a hostname to the CDP (as part of its IP address acquisition process) its name can be resolved by the CNP. If the hostname requested for resolution cannot be found in the cabhCdpLanAddrTable, the CNP performs recursive queries to external DNS servers (of which the initial one is learned by the CDC via DHCP options).

[84] Revised this paragraph per ECN CH1.1-N-03.0104-2 by GO on 12/5/03.

EXHIBIT A

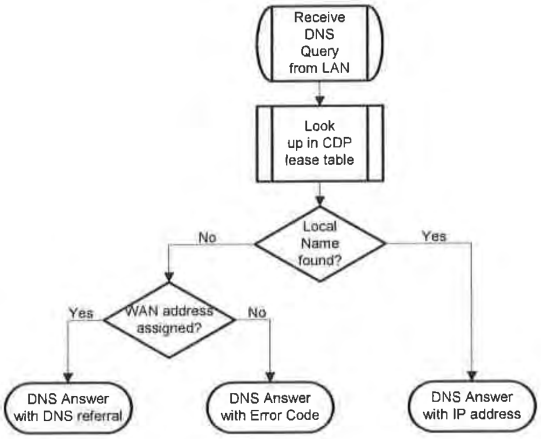

Receive DNS Query from LAN
Look up in CDP lease table
Local Name found?
No
Yes
WAN address assigned?
Yes
No
DNS Answer with DNS referral
DNS Answer with Error Code
DNS Answer with IP address

Figure 9-1 – CNP Packet Processing

A standard DNS query specifies a target domain name (QNAME), query type (QTYPE), and query class (QCLASS), and asks for Resource Records that match. The CNP will respond to the DNS queries with QCLASS = IN, and QTYPE = A, NS, SOA or PTR as defined in [RFC 1035]. Support for zone transfers and DNS over TCP is not required.

Since the CNP is an authoritative DNS server inside the LAN-Trans realm, it will provide Start of Authority (SOA) and Authoritative Nameserver (NS) records on request. An example of the SOA record fields (see Section 3.3.13 of [RFC 1035]) follows:

Table 9-2 – SOA Record Fields

[RFC 1035] RDATA field	CableHome CDP MIB Object
MNAME	cabhCdpServerDomainName
RNAME	Not specified
SERIAL	Not specified
REFRESH	Not specified
RETRY	Not specified
EXPIRE	Not specified
MINIMUM	Not specified

The MNAME field is the domain name of the LAN-trans address realm. The CNP uses the value stored in cabhCdpServerDomainName as the LAN-trans address realm domain name.

The RNAME field is the mailbox of the responsible person for the domain. If the PS maintains an E-mail address for an administrator, this information could be specified in this field.

The SERIAL field is an unsigned 32-bit number, used to identify the version of the zone information. But since CableHome does not specify zone transfers, value of this field is not specified.

EXHIBIT A

9.3 Name Resolution Requirements

The CNP MUST comply with the standard DNS message format and support standard DNS queries, as described in [RFC 1034], [RFC 1035].

The CNP is a stateless server that MUST be able to receive queries and send replies in UDP packets [RFC 768].

The CNP MUST support recursive mode, as defined in [RFC 1034].

The CNP answers name queries, beginning with local information within the PS, and its response messages MUST contain an answer or an error.

The CNP MUST only respond to DNS queries addressed to the IP address represented by the value of the cabCdpServerRouter MIB object (i.e. the PS's LAN side IP address).[85]

The CNP MUST NOT respond to any DNS queries addressed to the PS WAN-Man or WAN-Data IP addresses.

Upon receiving an initial hostname resolution query from a LAN IP Device, the CNP MUST access the CDP's cabhCdpLanAddrTable to look up hostnames associated with IP addresses that are leased to LAN IP Devices.

Regardless of the existence of any cabhCdpWanDnsServerIp entries in the CDP MIB cabhCdpWanDnsServerTable, if the hostname can be resolved by the CNP from local data, the CNP MUST respond to the hostname resolution query with the IP address of the named LAN IP Device.

If the queried host name can not be resolved by the CNP from local data, and the CDP's cabhCdpWanDnsServerTable is populated with at least one cabhCdpWanDnsServerIp entry, the CNP function of the PS MUST attempt to resolve the hostname query via recursive queries to external DNS servers, starting with queries to the DNS server, represented by the first cabhCdpWanDnsServerIp entry in the cabhCdpWanDnsServerTable.

If the host name can not be resolved by the CNP from local data and no cabhCdpWanDnsServerIp entries exist in the cabhCdpWanDnsServerTable, the CNP function of the PS MUST respond to the host name resolution query with the appropriate error specified by [RFC 1035].

The CNP MUST respond to DNS queries of type QCLASS = IN, and QTYPE = A, NS, SOA or PTR.

The CNP responses to DNS queries MUST comply with Section 3.3 of [RFC 1035], with Authoritative Answer bit set to '1' in the Header Section (see Section 4.1.1 of [RFC 1035]).

Since the CNP is an authoritative DNS server inside the LAN-Trans realm, it MUST provide Start of Authority (SOA) and Authoritative Nameserver (NS) records on request. The SOA record fields (see Section 3.3.13 of [RFC 1035]) MUST contain an entry for the MNAME field that is equal to the value of the CDP's cabhCdpServerDomainName MIB object.

If cabhCdpServerDomainName is not set, the CNP MUST still provide DNS service to LAN IP Devices.[86]

[85] Revised this paragraph per ECN CH1.1-N-03.0104-2 by GO on 12/5/03.

[86] Revised this sentence per ECN CH1.1-N-03.0104-2 by GO on 12/5/03.

EXHIBIT A

10 QUALITY OF SERVICE

10.1 Introduction

This section describes the CableHome environment for enabling home networking applications to utilize QoS resources. These resources provide a management mechanism that prioritizes data flows to support ieal-time application traffic, such as VoIP, A/V streaming, and video gaming, by using prioritized media access and queuing. CableHome 1.1 QoS is complementary to the PacketCable & DOCSIS QoS mechanisms, which allow QoS traffic management over the HFC network.

CableHome 1.1 QoS defines the necessary PS and BP element and sub-element QoS requirements that enable applications to establish different levels of QoS within the home network and for operators to communicate the desired priority treatment to the CableHome-enabled applications on the home network.

10.1.1 Goals

The goals for CableHome QoS include:

- Enable home networking applications to establish prioritized data transmission among CableHome Hosts as well as between the CableHome Hosts and the CableHome Residential Gateway using CableHome compliant messaging.
- Enable home networking applications to establish prioritized data sessions between the CMTS and CableHome Residential Gateway device using PacketCable compliant messaging. (From CH 1.0.)

10.1.2 Assumptions

The following assumptions were made for CableHome 1.1 QoS:

- To avoid problems with NAT functions in the CAP element, PacketCable 1.0 compliant applications will use CableHome LAN-Pass addressing as defined in Section 7 & Section 9.
- Applications that could benefit from QoS could be embedded in CableHome Host devices connected via a home networking technology.
- CableHome Host applications could include PacketCable services.

Note: Any device that would like to receive QoS for MSO services will have to comply with the CableHome 1.1 specification and the device's operating system and network stack will need to have appropriate QoS capabilities.

10.2 QoS Architecture

The CableHome 1.1 quality-of-service (CQoS) architecture is composed of CableHome functional elements (PS and BP) and sub-elements in the PS and BPs. Developers of CableHome networking equipment (e.g., hardware and software) implement one or more of these elements depending on the desired feature set of these products. Specified minimum sets of capabilities are required to participate in the Q-Domain. The basic CQoS elements are presented in Section 10.2.2.

10.2.1 System Design Guidelines

The overall CableHome 1.1 QoS system design guidelines are listed in Table 10-1 below.

EXHIBIT A

Table 10-1 – CableHome QoS System Design Guidelines

Number	QoS System Design Guidelines
QoS 1	QoS Media Access: CableHome 1.1 will define a mechanism that controls transmission access using priorities on shared media for the PS and BP logical elements. It will provide prioritized media access to various devices and applications on the home network.
QoS 2	QoS Forwarding: The PS will support a queuing mechanism that prioritizes packets that are received from multiple interfaces and are to be retransmitted /forwarded through LAN interfaces.
QoS 3	QoS Characteristics Management: CableHome 1.1 will specify a signalling and management mechanism for communication of QoS characteristics between the PS and BPs desiring QoS within a home network. This mechanism will be aggregated and managed in the PS.

10.2.2 CableHome QoS System Description

The CQoS Architecture is composed of the following entities:

- Q-Domain
- Portal Services element (PS)
- Boundary Point element (BP)
- CableHome Quality-of-Service Portal sub-element (CQP)
- CableHome Quality-of-Service Boundary Point sub-element (QBP)

The cable data network equipment manages the CableHome 1.1 QoS functions but is not within the Q-Domain.

10.2.2.1 CQP Sub-Element

The PS element includes a CableHome Quality of Service Portal (CQP) sub-element. The CQP acts as a CQoS portal for CableHome compliant applications. Its primary function is to enable priorities based QoS for the devices within the home network. It performs priorities based queuing/forwarding and media access for the traffic originating from the PS as well as for the traffic transiting through the PS. It is also responsible for communication of QoS characteristics to various devices within the home.

The CQP also supports the delivery of QoS messaging across the HFC network for PacketCable applications. PacketCable 1.0 compliant messaging includes QoS messaging and other messages related to the aspects of a specific service such as policy decisions and application of two phase reservation models. (From CH 1.0.)

10.2 2.2 QBP Sub-Element

The BP element includes a CableHome Quality of Service Boundary Point (QBP) sub-element. It performs priorities based media access for the traffic originating from the BP. It is also responsible for the reception of QoS characteristics from the PS.

10.2.2.3 QoS Functionality in CQP and QBP

CQP and QBP sub-elements consists of one or more of the following functionalities:

- QoS prioritized Forwarding and Media Access (QFM): Specifies prioritized queuing and packet forwarding and prioritized shared media access in the PS. This functionality is part of the PS only.

EXHIBIT A

- QoS Characteristics Server (QCS): This functionality is responsible for maintaining a repository of QoS characteristics for various devices and applications within the home network and also for communication of these characteristics to these devices and applications. This functionality is a part of the PS only.
- QoS Characteristics Client (QCC): This functionality, with the aid of QCS, determines QoS characteristics that a particular application/device needs to use. It resides within the BP only.

10.2.2.4 Q-Domain

The Q-Domain defines the sphere of direct influence of CQoS functionality. The Q-Domain exists on a per-home basis. Individual homes are separate and have independent Q-Domains. The CQP and QBP elements bound the Q-Domain within a given home.

10.2.2.5 Physical Device Classes & CQoS Functional Elements

An example of the relationship between the CableHome Devices and the CQoS functional elements is presented in Figure 10-1.

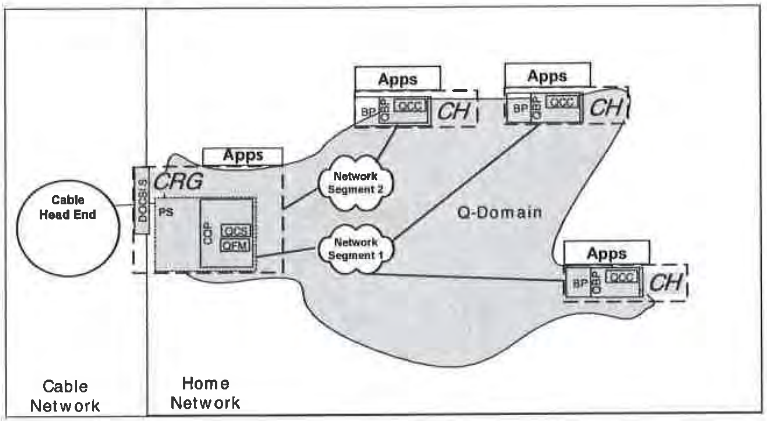


Figure 10-1 — Example of CQoS Functional Elements

10.2.2.6 CableHome Priorities and their Mappings

10.2.2.6.1 CableHome Priorities

CableHome 1.1 defines three different CableHome QoS priorities. They are:

- CableHome Generic Priorities
- CableHome Queuing Priorities
- CableHome Media Access Priorities

10.2.2.6.1.1 CableHome Generic Priorities

CableHome 1.1 defines eight CableHome Generic Priority levels, 0 through 7, 7 being the highest and 0 being the lowest. Cable operators can assign one of these eight priorities to an application. Out of the three types of priorities defined by CableHome, only the CableHome Generic Priority value for an application

EXHIBIT A

can be set by a cable operator. The other two priorities, CableHome Queuing Priorities and CableHome Media Access Priorities, are derived from this CableHome Generic Priority, depending on the capabilities of the hardware and software in the device. The higher the CableHome Generic Priority assigned to an application, the higher preference is given to that application's packets for packet forwarding and media access functionalities.

10.2.2.6.1.2 CableHome Queuing Priorities

In the PS, packets may arrive from multiple interfaces and be destined for a single interface. Hence, each interface needs to implement a queueing function. In order to provide prioritized QoS for traffic within the home passing through the PS, CableHome specifies prioritized queueing functionality per interface in the PS. For this purpose, an individual queue within an interface is designated with a certain queuing priority. This is defined as CableHome Queuing Priority. This CableHome queuing priority needs to be identified for each packet to be transmitted on each PS interface so that the packet can be placed in an appropriate queue. This CableHome Queuing priority is derived from the CableHome Generic Priority assigned to the application that sent the packet, using the number of queues supported by an interface on the PS. This mapping is specified in Section 10.2.2.6.2.

10.2.2.6.1.3 CableHome Media Access Priorities

CableHome 1.1 defines a prioritized QoS media access system in which traffic over a shared media is prioritized based on the assigned packet priority. Thus, a shared media technology needs to support prioritized QoS such that a packet with higher priority is given preferential access to the shared media, versus a packet with lower priority. Various shared media technologies support varying number of media access priorities. (e.g. HomePNA support eight media access priorities, HomePlug support four). CableHome Media Access Priority for the packet is derived from its CableHome Generic Priority based on the number of media access priorities supported by the interface's layer-2 shared media technology. This mapping is defined in Section 10.2.2.6.3. CableHome Media Access Priority values are logical levels that represent a level of preference that an application-packet should get for media access. CableHome Media Access Priority mapping is separate and distinct from native media access priority mappings defined by layer-2 shared media technologies, to keep CableHome Media Access Priority mapping independent of layer-2 technologies.

10.2.2.6.2 Mapping of CableHome Generic Priorities to CableHome Queuing Priorities

As explained in Section 10.2.2.6.1.2, the PS performs prioritized queuing for each of its interfaces. There are 8 CableHome Generic Priorities defined, hence an ideal scenario would be that an interface has 8 queues and each is assigned with a queuing priority from 0 to 7. However, the number of queues implemented for an interface in the PS varies on the implementation. The number of queues supported by an interface will be stored in the PS database and readable via a MIB object cabhPriorityQosPsIfAttribIfNumQueues. If an interface implements N (1<=N<=8) queues, the various queues in an interface will be designated with CableHome Queuing Priorities from 0 (lowest) to N-1 (highest). When a packet enters the PS, the packet's CableHome Queuing Priority needs to be determined based on its CableHome Generic Priority so a packet can be placed in an appropriate queue. This mapping between the two priorities is specified in Table 10-2.

In Table 10-2, eight CableHome Generic Priorities are expressed in the fist column. In the adjacent columns of the table, the number of queues supported for the interface is presented as a range from 8 to 1. Table entries represent CableHome Queuing Priorities for packets ranging from 0 to N-1.

Once a packet's CableHome Queuing Priority is determined from CableHome Generic Priority using Table 10-2, a packet is placed in a queue that is designated for that specific CableHome Queuing Priority.

EXHIBIT A

Table 10-2 – CableHome Queuing Priority Mappings

Generic CableHome Priority	Number of Queues Supported by the Interface (N)							
	8	7	6	5	4	3	2	1
7	7	6	5	4	3	2	1	0
6	6	5	4	3	3	2	1	0
5	5	4	3	2	2	1	1	0
4	4	3	2	2	2	1	1	0
3	3	2	1	1	1	1	0	0
2	2	1	1	1	1	0	0	0
1	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Note: The following paragraph illustrates how CableHome Queuing Priorities Mapping should be used:

If an incoming data packet has a CableHome Generic Priority of 7, and is destined for an outgoing interface that supports only three queues (N=3); then the CableHome Queuing Priority for that packet would be 2. Three queues for that particular interface would be designated with priorities of '0' (lowest), '1' and '2' (highest). This particular packet would be placed in the queue with the priority designation of two for that interface.

10.2.2.6.3 Mapping of CableHome Generic Priorities to CableHome Media Access Priorities

As discussed in Section 10.2.2.6.1.3, various layer-2 technologies support varying number of media access priorities. Hence, eight CableHome Generic Priorities defined for applications need to be mapped to the appropriate number of CableHome Media Access priorities, based on number of media access priorities (1<=M<=8) supported by a layer-2 technology interface. The number of native media access priorities (M) supported by the particular layer-2 shared media technology of each interface on the PS and BP is stored in the PS and BP respectively. The number of media access priorities supported by PS interfaces is available through the MIB object cabhPriorityQosPsIfAttribIfNumPriorities in the PS. The number of media access priorities supported by the BP interface is available in the PS though the MIB object cabhPsDevBpNumberInterfacesPriorties. The mapping between these two priorities is defined in Table 10-3.

Table 10-3 is very similar to Table 10-2, except the mapping of CableHome Generic Priority values is performed using the number of media access priorities (M) supported by a particular layer-2 shared media technology. The entries in the table represent CableHome Media Access Priorities. Thus, if a layer-2 technology supports M media access priorities, then the CableHome Media Access Priorities for that technology would range from 0 (lowest) to M-1 (highest). These CableHome Media Access Priority values represent relative logical levels. The higher the CableHome Media Access priority value for the packet, the higher preference it should be granted for accessing the shared media. Implementers of CableHome 1.1 specifications should make sure that packets are given required relative preferential access to the shared media, as described by the CableHome Media Access Priority mapping.

Note: The following paragraph illustrates how CableHome Media Access Priorities Mapping should be used:

If a CableHome Generic Priority value for an application packet is 7 (highest), and the layer-2 technology on which the packet is being transmitted supports 4 media access priorities, then referring to Table 10-3, the packet's CableHome Media Access Priority value would be 3 (highest). However, if a CableHome

EXHIBIT A

Generic Priority value for a packet is 2, the CableHome Media Access Priority value for the aforementioned technology would be 1 (second lowest). Previously, the required CableHome mapping may be different from native mappings used by the shared media technologies.

See Appendix V for examples of differences between the CableHome Media Access Priority mapping and native layer-2 technology mappings.

Table 10-3 – CableHome Media Access Priority Mappings

CableHome Generic Priority	# Media Access Priorities Supported (N) in the LAN							
	8	7	6	5	4	3	2	1
7	7	6	5	4	3	2	1	0
6	6	5	4	3	3	2	1	0
5	5	4	3	2	2	1	1	0
4	4	3	2	2	2	1	1	0
3	3	2	1	1	1	1	0	0
2	2	1	1	1	1	0	0	0
1	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

10.3 PS Logical Sub-Element CQP

The CQP contains the QFM and QCS functionalities as shown in Figure 10-1. The QFM functionality is described in Section 10.3.1. The QCS functionality is described in Section 10.3.2.

10.3.1 QoS Forwarding and Media Access (QFM)

The Quality of Service Forwarding and Media access functionality (QFM) in the PS is responsible for prioritized forwarding and media access for the packets going through the PS onto the home LAN. This section provides description of the QFM functionality in the PS and specifies associated PS requirements.

10.3.1.1 QoS Forwarding and Media Access Goals

The goals for the QoS Forwarding and Media Access functionality include:

- To order the packets arriving from multiple LAN interfaces to the PS and forward them to a destination LAN interface according to their priorities and LAN interfaces' queuing capabilities.
- Provide prioritized access to the shared media during the packet transmission based on the packet priority and capabilities of shared media for prioritized access.

10.3.1.2 QoS Forwarding and Media Access Design Guidelines

Table 10-4 – QFM System Design Guidelines

Number	QFM System Design Guidelines
QFM.1	The QFM should operate on packets to and from the LAN-Trans and LAN-Pass address realms.
QFM.2	The QFM will determine the packet priority using the information available in the PS MIB maintained by QCS.

EXHIBIT A

Number	QFM System Design Guidelines
QFM.3	The QFM will order incoming packets to exit through LAN interfaces according to their priorities.
QFM.4	The QFM should be able to work with different number of queues per interface.
QFM.5	The QFM will provide prioritized access to the shared media on each interface according to the packet priority.
QFM.6	The QFM should map CableHome Generic Priority of the packet to CableHome Media Access priority according to the defined mapping.
QFM.7	The QFM should be able to operate with interfaces that support different numbers of priorities for media access.

10.3.1.3 QoS Forwarding and Media Access Design Assumptions

- Each PS LAN interface may support less than eight queues.
- Maximum number of queues supported a PS LAN interface is eight.
- Each PS LAN networking technology may support less than eight media access priorities.
- Maximum number of media access priorities supported by a PS LAN networking technology is eight.

10.3.1.4 QoS Forwarding and Media Access System Description

The QFM provides the PS a mechanism to order and transmit packets out of the PS to a LAN host according to assigned priorities. It is through the assignment of priorities to packets and the action of the QFM that packets passing through the PS over the home LAN are provided prioritized access to the host transmission interfaces and to the shared LAN media. Any packet going out of the PS on a LAN interface should be processed by the QFM regardless of its source.

Once the QFM receives a packet destined for a particular LAN interface, it performs the following three actions before the packet is transmitted onto the destination LAN interface:

1. Classification process to identify the CableHome Generic Priority of the packet

2. Prioritized queuing

3. Prioritized media access

10.3.1.4.1 Classification of the Packet to identify CableHome Generic Priority

When the PS needs to transmit a packet over the LAN interface, it examines the packet to identify a CableHome Generic Priority for the packet. The PS reads the destination IP and destination port of the packet. The PS database stores a classifier table (cabhPriorityQosDestPriorityListTable) that uses destination IP and destination port values to determine the CableHome Generic Priority of the packet. Wild carding (0) is allowed for destination port field but not for destination IP. Hence the PS first tries to find a specific entry that matches packet's destination IP and destination port to determine the priority. If a specific entry is not found, the PS tries to determine priority using destination IP only. If no entry is found in the classifier table for packet's destination IP and destination port, then the PS assigns a CableHome Generic Priority value of 0 to the packet. The PS uses the assigned CableHome Generic Priority value to determine the packet's CableHome Queuing Priority and CableHome Media Access Priority.

10.3.1.4.2 Prioritized Queuing

The number of queues supported by an interface on the PS, to which the packet is destined, may not be the same as the eight CableHome Generic Priority values defined by this specification. Hence the PS maps

EXHIBIT A

CableHome Generic Priority value of the packet to a CableHome Queuing Priority value as defined in Section 10.2.2.6.1.2. Then the PS places the packet in an appropriate queue of the destination interface that corresponds to this mapped CableHome Queuing Priority value.

For each outgoing interface, the QFM polls all of the queues on that interface according to their priorities to extract packets out to be transmitted on the shared media. Every time the QFM is to extract a packet from the queues for a particular PS interface, it always starts its polling with the highest priority queue first. If the highest priority queue has no packets to be sent, the QFM polls the next highest priority queue of the remaining queues in the hierarchy until it finds a packet to be sent in one of the queues. Packets are extracted from each queue in the order they arrive. Thus, the queuing scheme used by the QFM may be described as First in, First Out with Priorities, and Highest Priority Queue First.

10.3.1.4.3 Prioritized Media Access

Once the QFM extracts a packet from the set of queues of an interface, the packet needs to be transmitted on the shared LAN media with an appropriate priority. Hence, the QFM maps the CableHome Generic Priority value of the packet to the CableHome Media Access Priority value as explained in Section 10.2.2.6.3, using Table 10-3. This value determines the level of preference the packet should use for accessing the shared media. Therefore, vendors need to insure that relative media access preferences, as required by CableHome Media Access Priority values, are maintained when transmitting packets over the shared LAN media.

10.3.1.4.4 PacketCable Applications Support

Since the goal of CableHome 1.1 QoS is to provide QoS over home network only, CableHome 1.1 QoS does not give special consideration for access network QoS. However, CableHome 1.1 retains the support for home networking applications to establish prioritized data sessions between the CMTS and CableHome Residential Gateway device, using PacketCable compliant messaging, as specified by the CableHome 1.0 specifications [CH1]. Hence, the necessary requirements to support this functionality in the PS are included in CableHome 1.1 QoS specifications, as it is from CableHome 1.0 specification.

The PS acts as a transparent bridge and forwards PacketCable 1.0 [PKT-CODEC], [PKT-DQOS] QoS messaging between the CMTS and PacketCable applications. Application data is associated to a DOCSIS service flow according to a classifier that is created in the CM interface, based on the information included in the PacketCable 1.0 messages (such as RSVP PATH).

Since the PS requirement for CableHome 1.1 is to forward PacketCable QoS messaging, there is no dependency on the NMS to support this function. Therefore, this CQP function remains the same for both DHCP Provisioning Mode and SNMP Provisioning Mode (see Section 5.5).

CableHome 1.1 QoS messaging over the HFC or access network is defined by PacketCable 1.0 specifications [PKT-CODEC], [PKT-DQOS]. As such, the CableHome 1.1 QoS policy management and admission control functions for access network QoS are also defined by PacketCable1.0 specifications [PKT-CODEC], [PKT-DQOS].

10.3.1.5 QoS Forwarding and Media Access Requirements

10.3.1.5.1 Packet Classification Requirements

When PS needs to transmit a packet over a LAN interface, the PS MUST determine CableHome Generic Priority for the packet from its destination IP and destination port values using PS classifier table, (cabhPriorityQosBpDestTable) stored in the PS database [CH7]. The PS MUST always try to find a specific entry in the PS database that matches both the destination IP and destination port of the packet to determine the priority. If a specific entry is not found then the PS MUST try to find an entry that matches

EXHIBIT A

only the destination IP of the packet. If there is no entry in the PS database that matches the destination IP of the packet, then the PS MUST assign CableHome Generic Priority value 0 to the packet.

10.3.1.5.2 Prioritized Queuing Requirements

The PS MUST store the number of queues implemented by each of its interface in the PS database that can be accessed via a cabhPriorityQosPsIfAttribIfNumQueues MIB [CH7].

The PS MUST map the CableHome Generic Priority value of the packet identified during the classification process to CableHome Queuing Priority value as defined in Section 10.2.2.6.1.2 using the number of queues (cabhPriorityQosPsIfAttribIfNumQueues) implemented by an interface on which the packet is to be transmitted. The PS MUST queue the packet appropriately on the destination interface according to this mapped CableHome Queuing Priority value.

For each LAN interface, the PS MUST poll various queues on that interface according to their priorities to extract packets out to be transmitted on the shared media. Every time the PS is to extract a packet from the various queues for a particular interface, the PS MUST always start its polling with the highest priority queue first. If the highest priority queue has no packets to be sent, the PS MUST poll the next highest priority queue of the remaining queues in the hierarchy, until it finds the next available highest priority packet to be sent. PS MUST always extract packets from each queue in the order they arrive.

10.3.1.5.3 Prioritized Media Access Requirements

The PS MUST store the number of native layer-2 media access priorities supported by each of its interface in the PS database that can be accessible via a MIB cabhPriorityQosPsIfAttribIfNumPriorities [CH7].

After the packet is extracted from the queues of a particular interface the PS MUST map CableHome Generic Priority of the packet to CableHome Media Access Priority, as defined in Section 10.2.2.6.1.3, using the number of media access priorities supported (cabhPriorityQosPsIfAttribIfNumPriorities) by that interface. The PS MUST transmit the packet through the shared media technology such that its relative preferential access to the media, as required by CableHome Media Access Priority value, is maintained.

10.3.1.5.4 PacketCable Applications Support Requirements

The PS MUST act as a transparent bridge and forward PacketCable 1.0 [PKT-CODEC], [PKT-DQOS] QoS messaging between the CMTS and PacketCable applications. Application data is associated to a DOCSIS service flow according to a classifier that is created in the CM interface, based on the information included in the PacketCable 1.0 messages (such as RSVP PATH).

Since the PS requirement for CableHome 1.0 is to just forward PacketCable QoS messaging, there is no dependency on the NMS to support this function. Therefore, this CQP function remains the same for both DHCP Provisioning Mode and SNMP Provisioning Mode (see Section 5.5).

10.3.2 PS QoS Characteristics Server (QCS)

The QoS Characteristics Server (QCS) functionality in the PS is responsible for management of application priorities in the home network on behalf of a cable operator. This section provides the description of the QCS functionality and associated PS requirements.

10.3.2.1 QoS Characteristics Server Goals

- To establish a set of criteria by which applications and network stacks can assign and use QoS characteristics for traffic within the home network.
- To provide a mechanism for the head-end to communicate the desired QoS Characteristics to the PS and then to CableHome Hosts (BPs). Specifically, the assignment of QoS characteristics is related to the priority information per application type.

EXHIBIT A

10.3.2.2 QoS Characteristics Server Design Guidelines

Table 10-5 – QCS Design Guidelines

Number	System Design Guidelines
QCS.1	QCS will be provided priorities information for each application from Network Management Server (NMS) in the Headend
QCS.2	Priorities information supplied to the QCS will be controlled by cable operators (individual PS or mass PS update control)
QCS.3	Priorities information supplied to the QCS may be updated by the headend and BPs (QCCs) will acquire this updated information from the QCS
QCS.4	QCS will use a defined message content protocol (XML) and message transport protocol (SOAP) for distribution of priority information to BPs
QCS.5	QCS will use a defined messaging content interface (MIB) for providing priorities information of various applications in the home LAN to Network Management Server (NMS) in the headend
QCS.6	QCS aids QoS Forwarding and Media Access (QFM) functionality to determine a priority of the application packet

10.3.2.3 QoS Characteristics Server Assumptions

- CableHome 1.1 defines a format for exchanging messages between PS and BP.
- CableHome 1.1 defines a protocol for exchanging information between PS and BP.
- CableHome Hosts can have more than one service/application.

10.3.2.4 QoS Characteristics Server System Description

The QCS maintains a "database" of information in the PS Database as described in Section 5.4. The QCS receives application priority information from the headend, via initial configuration of the PS, or through a MIB interface in the CMP. The QCS also gathers application information from various BPs in the home LAN and assigns priorities to them. The QCS communicates this application priority information to the BPs (QCCs) to be used for prioritized media access by BPs. The information maintained by the QCS is used by the QFM functionality in the PS for prioritized forwarding and prioritized media access of packets going through it.

The rest of Section 10.3.2.4 is devoted to describing the exchange of information that occurs between the headend and the PS over the WAN and between the PS and BPs over the LAN.

10.3.2.4.1 WAN Information exchange

From the WAN side, the cable operator headend provides to the PS mapping of different applications and the priorities that they should use in a configuration file, or using SNMP SETs. NMS, at the headend, can read and update (change/modify/delete) these application priorities in the PS database using SNMP via a MIB interface.

10.3.2.4.1.1 Application ID to CableHome Generic Priority Mappings from headend to the PS

The headend provides the PS with a list of Application IDs and their CableHome Generic Priorities that a cable operator wishes these applications to use. This information is supplied to the PS through a configuration file at the time of PS initialization, or via SNMP SET commands from the headend. The PS stores this information in the PS database that is accessible via a MIB table, cabhPriorityQosMasterTable [CH7]. The PS makes use of this table as a priority master table to identify the priorities for various applications on the BPs over the home LAN.

EXHIBIT A

PS can also receive requests from the NMS to update (add/modify/delete) these CableHome Generic Priorities for applications in its master table using SNMP. In response to these requests, the PS updates (add/modify/delete) priority master table (cabhPriorityQosMasterTable). Such updates to the application priorities gets communicated to the BPs during subsequent LAN Information exchanges, which is described in Section 10.3.2.4.2.

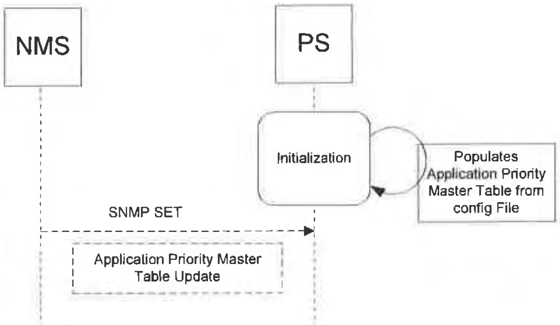

NMS
PS
Initialization
Populates Application Priority Master Table from config File
SNMP SET
Application Priority Master Table Update

Figure 10-2 — WAN Information Exchange and Processing at the PS

10.3.2.4.2 LAN Information Exchange

On the LAN side, a BP communicates its applications and sessions (destination IP and port) information to the PS in order to obtain their priorities. Once the PS receives this information, it determines appropriate priorities by looking them up in the priority master table and conveys them back to the BP. This information is exchanged between the PS and BP using QoSProfile XML schema (described below in Section 10.3.2.4.2.1) and BP Initiated SOAP Messaging (BP_Init Operation) as described in Section 6.3.3.4.4.2.

10.3.2.4.2.1 QoSProfile XML Schema

The QoSProfile XML schema contains two XML complex sequences: QoSApplicationList and the DesPriorityList. The QoSApplicationList contains four elements: BpIpAddress, ApplicationId, DefaultCHpriority, and a sequence of DestPriorityList. The DestPriorityList complex type, which is considered a secondary sequence in QoSApplicationList, contains three elements: DestIp, DestPort, and IpPortPriority. Each element has a defined type as mentioned in Table 10-6. The defined types are references from the W3C XML schema definitions [XML1].

The ApplicationId element is the application server port number for each BP application. This port number can be a well-known port assigned by IANA [IANA1]. Although applications are identified by the server port number (ApplicationId), communication may also occur on other port numbers. BP communicates a list of ApplicationIds for all the applications installed on it to the PS in the BP_Init Message (described in Section 10.4.1.4.1.1).[87]

The DefaultCHpriority element is the default CableHome Priority for an application. The BP may provide a value for this element in the QoSProfile. That value will be overwritten by the value supplied by the PS, via the BP_Init_Response Message (described later in Section 10.3.2.4.2.3), after consulting the application priority master table in the PS database (cabhPriorityQosMasterTable).

[87] Revised per ECN CH1.1-N-03.0109-1 by KB on 4/4/04.

EXHIBIT A

The BP includes DestPriorityListEntry sequence(s) in the QoSProfile for an application-session with another device. The DestPriorityListEntry sequence(s) are associated to the ApplicationId element in the QoSProfile XML schema. DestIP and DestPort elements respectively, correspond to the destination IP and destination port number of the application-session (socket connection) that is established by the BP. These entries are used to determine the priority (IpPortPriority) of the traffic, passing through the PS, based on specific destination IP address and port number as specified in the entry. Wild carding (0) is allowed only for DestPort, but not for DestIP. The BP may provide a value for IpPortPriority element in the QoSProfile. The PS overwrites that value with the DefaultCHpriority, supplied in the BP_Init_Response Message, after consulting the application priority master table in the PS database (cabhPriorityQosMasterTable).

A BP is always required to transmit the entire QoSProfile XML schema to the PS whenever it sends the BP_Init message.[88]

Table 10-6 – QoS Profile XML Schema

```
<xs:element  name="ch:QoSProfile"  type="ch:QoSProfileEntry"/>


<xs:complexType name= "ch:QoSProfileEntry">
      <xs:element name ="ch:QoSApplicationListEntry"  type="ch:QoSApplicationListEntryDescription"
minOccurs="1" maxOccurs="4"/>
</xs:complexType>


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


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

10.3.2.4.2.2 BP information to the PS using BP_Init Message

A BP is required to send its applications and sessions information to the PS in the QoSProfile XML schema format using BP_Init Message, as described in Section 6.3.3.4.4.2.1, on the following three different occasions:

- DHCP lease acquisition or renewal
- Application update (addition or deletion) in a BP

[88] Revised Table 10-6 per ECN CH1.1-N-03068 by GO on 10/31/03.

EXHIBIT A

- Establishment and termination of application-session with another device by a BP

Refer to Section 10.4.1.4.1.1.1 for detailed description of BP information exchange under each of the above three occasions.

10.3.2.4.2.3 Priority information from the PS to BP using BP_Init_Response

The processing of the QoSProfile XML schema by the PS is exactly the same in all the three different occasions (mentioned above in Section 10.3.2.4.2.2), when it receives the BP_Init Message. The processing of QoSProfile XML schema is described below:

> Upon the receipt of the QoSProfile XML schema from the BP in the BP_Init message, the PS determines values for DefaultCHPriority (part of QoSApplicationListEntry) and IpPortPriority (part of DestPriorityListEntry) elements for all the applications in the QoSProfile by looking up the priority master table in the PS database (cabhPriorityQosMasterTable). If there is no entry in the priority master table that corresponds to an application in the QoS Profile, the PS assigns priority 0 (lowest) to the values for DefaultCHPriority and IpPortPriority elements for the application. The PS updates the BP QoSProfile with these priorities by overwriting the values that BP may have provided in its original QoSProfile.[89]
>
> The PS then stores this BP application priority information, represented by the updated QoSProfile, in the PS database that is accessible via the MIB tables, cabhPriorityQosBpTable and cabhPriorityQosBpDestTable [CH7]. The PS completely replaces the old BP application priority information that may have been stored in its database with the new information represented by the updated QoSProfile. Such a complete replacement of the old BP application priority information addresses the processing of both the addition as well as the deletion of a new application or a session in the BP and keeps the processing complexity in the PS to a minimum level.
>
> The cabhPriorityQosBpTable represents information about various applications and their priorities on a particular BP in the home LAN. The cabhPriorityQosBpDestTable represents destination IP and port specific priorities for different BP application-sessions. The QFM functionality in the PS utilizes the information represented by the cabhPriorityQosBpDestTable for its prioritized queuing and prioritized media access in the PS.
>
> After updating the database with BP application priority information, the PS sends BP QoSProfile, updated with priority information, to the BP using BP_Init_Response Message as described in Section 6.3.3.4.4.2.2. This updated QoSProfile conveys to the BP appropriate priority information that it is required to use for its applications.

10.3.2.5 QoS Characteristics Server Requirements

10.3.2.5.1 WAN Information Exchange Requirements

The PS MUST store a list of Application IDs and their CableHome Generic Priorities, provided by a cable operator, in the PS databas,e that is accessible via a Application Priority Master MIB table, cabhPriorityQosMasterTable [CH7]. The PS MUST support updates (add/modify/delete) to this priority master table (cabhPriorityQosMasterTable) through a configuration file at the time of PS initialization, or via SNMP SET commands from the headend.

10.3.2.5.2 LAN Information Exchange Requirements:

The processing of the QoSProfile XML schema by the PS is identical in all three different occasions (mentioned above in Section 10.3.2.4.2.2), when it receives the BP_Init Message.

[89] Revised this paragraph per ECN CH1.1-N-03.0100-1 by GO on 12/5/03.

EXHIBIT A

The PS MUST be able to process BP QoSProfile XML schema (as described in Section 10.3.2.4.2.1) containing its applications and sessions (destination IP and port) information received in the BP_Init Message (as described in Section 6.3.3.4.4.2.). When PS receives QoSProfile XML schema from the BP (on any of the three occasions as explained in Section 10.3.2.4.2.2) in the BP_Init message, the PS MUST determine values for DefaultCHPriority (part of QoSApplicationListEntry) and IpPortPriority (part of DestPriorityListEntry) elements for all the applications in the QoSProfile by looking up the priority master table in the PS database (cabhPriorityQosMasterTable). If there is no entry in the priority master table that corresponds to an application in the QoS Profile, the PS MUST assign priority 0 (lowest) to the values for DefaultCHPriority and IpPortPriority elements for the application. The PS MUST update the BP QoSProfile with these priority values by overwriting the values that BP may have provided in its original QoSProfile.[90]

The PS then MUST store this BP application priority information, represented by the updated QoSProfile, in the PS database that is accessible via MIB tables, cabhPriorityQosBpTable and cabhPriorityQosBpDestTable [CH7]. The PS MUST completely replace the old BP application priority information that may have been stored in its database with the new information represented by the updated QoSProfile.

After updating the PS database with BP application priority information, the PS MUST send the entire BP QoSProfile, updated with priority information, to the BP using BP_Init_Response Message, as described in Section 6.3.3.4.4.2.2.

10.4 BP Logical Sub-Element QBP

10.4.1 QoS Characteristics Client (QCC)

10.4.1.1 QoS Characteristics Client Goals

- To provide a mechanism for a CableHome Host to receive desired QoS Characteristics from the PS. These QoS characteristics are communicated to the PS from the headend.
- To establish a set of criteria in a CableHome Host by which its applications and network stacks can assign and use QoS characteristics for its application traffic.

10.4.1.2 QoS Characteristics Client System Assumption

CableHome Compliant Host (BP) can have more than one service/application on it.

10.4.1.3 QoS Characteristics Client System Guidelines

Table 10-7 – QCC Design Guidelines

Number	System Design Guidelines
QCC.1	QCC will be provided application priorities information from QCS.
QCC.2	Priorities controlled by QCS will be updated dynamically and QCC will request updated priority information from QCS.
QCC.3	QCC will use a defined message content protocol (XML) and message transport protocol (SOAP) for communicating priority information to the PS.
QCC.4	The QCC will provide prioritized access to the shared media of its LAN interface according to the packet priority.

[90] Revised this paragraph per ECN CH1.1-N-03.0100-1 by GO on 12/5/03.

EXHIBIT A

10.4.1.4 QoS Characteristics Client System Description

This section provides an overview of the key concepts of the QoS Characteristics Client (QCC) in the BP.

The messaging of the QCC is closely related to the messaging of the QCS described in Section 10.3.2.4.2. The QCC in the BP is a counterpart to the QCS in the PS. The QCC performs all of the QoSProfile message exchanges with the PS (as described in Section 10.3.2.4.2) on behalf of the BP, using BP Initiated SOAP Messaging (Section 6.3.3.4.4.2). Thus the QCC obtains priority information for various applications and application-sessions on the BP. The QCC maintains an internal database to store the application priority information that it receives from the QCS, and uses this information to prioritize its application streams.

The QCC is also responsible for mapping the CableHome Generic Priority of the application packet to the CableHome Media Access Priority, using the number of media access priorities supported by the BP interface, as specified in Section 10.2.2.6.3.

The QCC is responsible for the following two main functions in the BP:

- LAN Information Exchange
- Prioritized Media Access for BP applications

Note: The rest of Section 10.4.1.4 is devoted to describing these two key functions of the QCC.

10.4.1.4.1 LAN Information Exchange

As described in Section 10.3.2.4.2, a BP is required to communicate its applications and sessions (destination IP and port) information to the PS in order to obtain their priorities. After the PS sends priority information to the BP, it stores this information in its database and uses it for prioritized media access. This BP is required to send its information to the PS, using QoSProfile XML schema (described below in Section 10.3.2.4.2.1) and BP Initiated SOAP Messaging (BP_Init Operation), as described in Section 6.3.3.4.4.2.

10.4.1.4.1.1 BP information to the PS using BP_Init Message

A BP is always required to convey its information to the PS in the QoSProfile XML schema format (Table 10-6), using BP_Init Message, as described in Section 6.3.3.4.4.2.1. A BP always sends its entire QoSProfile schema to the PS. As described in Section 10.3.2.4.2.2, a BP is required to send BP_Init Message with its entire QoSProfile schema to the PS on the following three different occasions:

- DHCP lease acquisition or renewal
- Application update (addition or deletion) in a BP
- Establishment or termination of application-session with another device by a BP

10.4.1.4.1.1.1 BP device and application information to the PS upon BP DHCP lease acquisition or renewal

After a BP receives DHCPACK message [RFC 2131] addressed to itself, either at the time of DHCP lease acquisition or DHCP lease renewal, it is required to send its device and application priority information to the PS, using BP_Init Message. The BP device information is sent using Device Profile XML schema (defined in Section 6.5.3.1.4), and application priority information is sent using QoSProfile XML schema.

The BP Device Profile sent to the PS contains a number of media access priorities (XML element: numberMedia AccessPriorities) supported by an interface on a BP. This information exchange and processing is described in Section 6.5.3.3, “MBP Discovery Function,” on page 94. Using this information,

EXHIBIT A

the PS populates cabhPsDevBpNumberInterfacePriorities [CH5] MIB, which is a part of the cabhPsDevBpProfileTable [CH5] MIB.

The BP QoSProfile sent to the PS after BP DHCP lease acquisition or lease renewal, contains a list of applications on the BP (QoSApplicationListEntry). It may also optionally contain destination IP address and port specific entries (DestPriorityListEntry) associated to an application. This information is formatted according to the QoSProfile XML schema, as described in Table 10-6. The BP may optionally provide values for DefaultCHPriority and IpPortPriority XML elements.

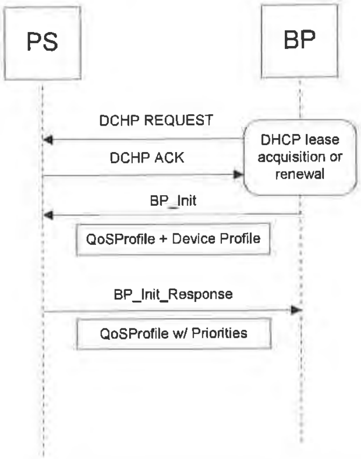


Figure 10-3 — Information Exchange upon BP Lease Acquisition or Renewal

10.4.1.4.1.1.2 BP application information to the PS upon application update in the BP

When a new application is added on the BP, the BP adds an entry for this application (QoSApplicationListEntry) in its existing QoSProfile XML schema. The BP may also optionally populate the DefaultCHPriority element associated with this ApplicationId in the QoSProfile. It may also include DestPriorityListEntry sequence for this ApplicationId. The BP is then required to send this new QoSProfile XML schema to the PS using BP_Init Message.

When an application is removed from the BP, the BP is required to delete all the entries (QoSApplicationListEntry as well as DestPriorityListEntry) related to that particular application from its QoSProfile. The BP is then required to send this modified QoSProfile to the PS using BP_Init Message.

EXHIBIT A

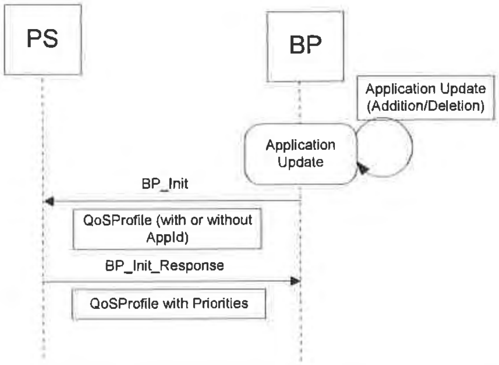

PS
BP
Application Update (Addition/Deletion)
Application Update
BP_Init
QoSProfile (with or without AppId)
BP_Init_Response
QoSProfile with Priorities

Figure 10-4 – Information Exchange upon BP Application Update

10.4.1.4.1.1.3 BP application information to the PS upon application-session establishment or termination

After an application on a BP establishes a session with another device, the BP adds session's destination IP and destination port information, (DestPriorityListEntry) associated to that application (Application ID) in its QoSProfile XML schema (Table 10-6). The BP may optionally populate the IpPortPriority element in the DestPriorityListEntry. The BP then sends this QoSProfile XML schema to the PS using BP_Init Message so that the PS can create entries in its classifier table (cabhPriorityQosBpDestTable), after identifying a priority (IpPortPriority) for the entry by using the priority master table. These classifier entries are utilized by the QFM functionality in the PS to determine the priorities of the packets by examining their destination IP and port; (if they happen to pass through the PS). Using these entries in the classifier table, the QFM performs prioritized queuing and prioritized media access as described in Section 10.3.1.4.

Once the BP terminates a session, the BP deletes the corresponding destination IP and port specific entry, DestPriorityListEntry, from its QoSProfile XML schema and sends this updated QoSProfile to the PS using BP_Init Message so that the PS can delete the entries in its classifier table.

These destination IP and port specific entries in the PS classifier table (cabhPriorityQosBpDestTable) can be used for providing prioritized packet forwarding and prioritized media access for the traffic going from the PS to a non-compliant sink-only device.

EXHIBIT A

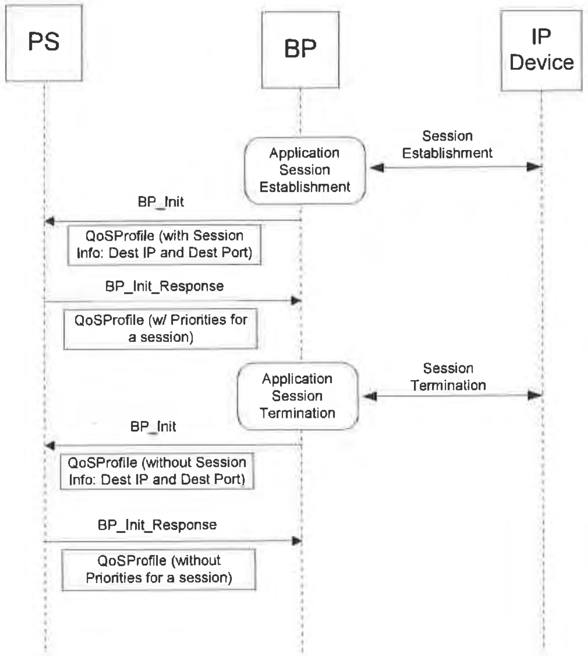

PS
BP
IP Device
Application Session Establishment
Session Establishment
BP_Init
QoSProfile (with Session Info: Dest IP and Dest Port)
BP_Init_Response
QoSProfile (w/ Priorities for a session)
Application Session Termination
Session Termination
BP_Init
QoSProfile (without Session Info: Dest IP and Dest Port)
BP_Init_Response
QoSProfile (without Priorities for a session)

Figure 10-5 – Information Exchange upon BP Session Establishment & Termination

10.4.1.4.1.2 Reception of priorities information from the PS in the BP_Init_Response

A BP receives priorities information for its applications (DefaultCHPriority) and application-sessions (IpPortPriority) in the BP_Init_ Response Message from the PS in the QoSProfile XML schema format. From the perspective of a BP, the process of receiving and processing of the QoSProfile XML schema, after it receives BP_Init_Response Message from the PS, is exactly the same for all the three occasions (as mentioned above in Section 10.4.1.4.1.1), when it sends BP_Init Message.

Upon receipt of this information, the BP completely replaces its previously stored QoSProfile XML schema with the newly received QoSProfile in its database. The BP uses the priority information supplied in this QoSProfile XML schema to determine priorities for its applications (Application Id) and application-sessions (identified by destination IP and destination Port).

10.4.1.4.2 Prioritized Media Access

The BP uses application priority information that it receives from the PS in QoSProfile XML schema (Table 10-6) to identify a CableHome Generic Priority for all packets to be transmitted on its LAN interface. If destination IP address and port number for an application-packet matches with the DestIP and DestPort of any of the DestPriorityListEntry sequences in the QoSProfile XML schema, the BP uses a priority value specified by IpPortPriority of that DestPriorityListEntry sequence as CableHome Generic Priority for that packet. Otherwise, the BP uses DefaultCHpriority corresponding to CHApplicationId as a CableHome Generic Priority for the packet. The BP maps this CableHome Generic Priority of the packet to

EXHIBIT A

a CableHome Media Access Priority as specified in Section 10.2.2.6.3, using the numberMediaAccessPriorities element of the BP Device Profile XML schema (Section 6.5.3.1). The BP then transmits the packet through its shared media technology in such way that packet's relative preferential access to the shared media as required by CableHome Media Access Priority value, is maintained.

10.4.1.5 QoS Characteristics Client Requirements

10.4.1.5.1 LAN Information Exchange Requirements

This section specifies BP requirements for the information exchange that it needs to perform in order to obtain priorities information from the PS for its applications and sessions.

10.4.1.5.1.1 BP Information to the PS using BP_Init Message

In order to receive their priorities information, a BP MUST communicate its applications and sessions (destination IP and port) information to the PS in the QoSProfile XML schema format (Table 10-6) using BP_Init Message, as described in Section 6.3.3.4.4.2.1. A BP MUST send BP_Init Message with its entire QoSProfile schema to the PS on the following three different occasions:

- DHCP lease acquisition or renewal
- Application update (addition or deletion) in a BP
- Establishment or termination of application-session with another device by a BP

10.4.1.5.1.1.1 BP device & application information to the PS upon BP DHCP lease acquisition/renewal

After a BP receives DHCPACK message [RFC 2131] addressed to itself, either at the time of DHCP lease acquisition or DHCP lease renewal, the BP is required to send its device and application priority information to the PS using BP_Init Message as specified in Section 6.5.3.3.4

The BP MUST include its list of applications (QoSApplicationListEntry) in the QoSProfile sent to the PS after its DHCP lease acquisition or renewal. The BP MAY include destination IP address and port specific entries (DestPriorityListEntry) associated to an application in this QoSProfile. The BP MAY also provide values for DefaultCHPriority and IpPortPriority XML elements in this QoSProfile.

10.4.1.5.1.1.2 BP application information to the PS upon application update in the BP

When a new application is added on the BP, the BP MUST add an entry for this application (QoSApplicationListEntry) in its existing QoSProfile XML schema. The BP MAY optionally populate the DefaultCHPriority element associated with this ApplicationId in the QoSProfile. The BP MAY also include DestPriorityListEntry sequence for this ApplicationId.

When an application is removed from the BP, the BP MUST delete all the entries (QoSApplicationListEntry as well as DestPriorityListEntry) related to that particular application from its QoSProfile.

After such update to the QoSProfile XML schema, the BP is then required to send this new QoSProfile XML schema to the PS using BP_Init Message.

EXHIBIT A

10.4.1.5.1.1.3 BP application information to the PS upon application-session establishment or termination

When an application on a BP establishes a session with another device, the BP MUST add the session's destination IP and destination port information (DestPriorityListEntry) associated to that application (Application ID) in its QoSProfile XML schema (Table 10-6). The BP MAY "wild card" (0) the DestPort element. The BP MUST NOT "wild card" the DestIP element. The BP MAY optionally populate the IpPortPriority element in the DestPriorityListEntry.

When an application on a BP terminates a session, the BP MUST delete the corresponding destination IP and port specific entry, DestPriorityListEntry, from its QoSProfile XML schema.

After such update to the QoSProfile XML schema, the BP is then required to send this new QoSProfile XML schema to the PS using BP_Init Message so that the PS can update (add/delete) the entries in its classifier table (cabhPriorityQosBpDestTable).

These destination IP and port specific entries in the PS classifier table (cabhPriorityQosBpDestTable) MAY be used for providing prioritized packet forwarding and prioritized media access for the traffic going from the PS to a non-compliant sink-only device.

10.4.1.5.1.2 Priorities information from the PS to a BP in the BP_Init_Response

A BP MUST be able to process priorities information for its applications (DefaultCHPriority) and application-sessions (IpPortPriority) that it receives from the PS in the QoSProfile XML schema format (Table 10-6) using BP_Init_ Response Message. Upon receipt of this information, the BP MUST completely replace its previously stored QoSProfile XML schema with the newly received QoSProfile XML schema.

10.4.1.5.2 Prioritized Media Access Requirements

The BP MUST use application priority (DefaultCHPriority or IpPortPriority) information that it receives from the PS in QoSProfile XML schema (Table 10-6) to identify a CableHome Generic Priority for all packets to be transmitted on its LAN interface. If destination IP address and port number for an application-packet matches with the DestIP and DestPort of any of the DestPriorityListEntry sequences in the QoSProfile XML schema, then the BP MUST use a priority value specified by IpPortPriority of that DestPriorityListEntry sequence as CableHome Generic Priority for that packet. Otherwise, the BP MUST use DefaultCHpriority corresponding to CHApplicationId as a CableHome Generic Priority for the packet. The BP MUST map this CableHome Generic Priority of the packet to a CableHome Media Access Priority as specified in Section 10.2.2.6.3, using the numberMediaAccessPriorities element of the BP Device Profile XML schema (Section 6.5.3.1). The BP then MUST transmit the packet through its shared media technology in such way that the packet's relative preferential access to the shared media, as required by CableHome Media Access Priority value, is maintained.

EXHIBIT A

11 SECURITY

11.1 Introduction/Overview

This section defines the security interfaces, protocols and functional requirements needed to secure the PS and its operations.

The delivery of reliable multi-media IP services to client devices on a home network requires a secure residential gateway along with the security mechanisms to protect these services from illegal access, monitoring, and disruption. The purpose of any security technology is to protect value, including revenue based services. Threats to a revenue stream exist when a user of the network perceives the value, expends effort and money, and invents a technique to get around making the necessary payments (See Appendix III). Some network users will go to extreme lengths to steal when value is perceived. The addition of security technology to protect value has an associated cost; the more money expended, the greater the security (security effectiveness is thus basic economics).

The CableHome security architecture focuses on securing the LAN from network attacks as well as securing communications between the PS and the Headend servers. The PS functionality can provide the foundation for other applications and services served by the cable operator to the home LAN. Security can exist for these applications independent of the CableHome security architecture. PacketCable specifies interfaces for a multi-media applications and has its own security architecture. For all references to PacketCable security, please refer to [PKT-SEC].

11.1.1 Goals

The goals for the CableHome security model include:

- Employ a cost effective security technology to force any user with the intent to steal or disrupt network services to spend an unreasonable amount of money or time.
- Secure the CableHome network used to offer high value cable-based services so that it is at least as secure as the DOCSIS and PacketCable technologies on the hybrid fiber-coax (HFC) network.
- Where possible, align CableHome security mechanisms with DOCSIS 1.0 [SCTE1], DOCSIS 1.1 [DOCSIS9], DOCSIS 2.0 [DOCSIS5] & [DOCSIS8] and PacketCable 1.x [PKT-SEC].
- From the LAN, it is the intent of CableHome security architecture to assist the operator with a secure identity to make it hard for the average subscriber to gain unauthorized access to the HFC network and cable-based services.

11.1.2 Assumptions

The assumptions for the CableHome security environment include:

- It is assumed the Embedded PS, has a DOCSIS 1.0, 1.1 or 2.0 cable modem.
- The home network includes less security for low value services.
- Back office configurations are not specified and CableHome assumes minimal configurations by the cable operator to operate in the CableHome specified modes.

11.2 Security Architecture

The CableHome security architecture is based on the CableHome architecture as defined in the CableHome Reference Architecture Section 5 of this specification. The CableHome architecture defines a Portal Services (PS) element, which includes Management, Provisioning, Security, and QoS functions.

EXHIBIT A

The CableHome architecture also includes the following set of Headend elements: Cable Modem Termination System (CMTS), Dynamic Host Configuration Protocol (DHCP) [RFC 2131] server, Network Management System, Trivial File Transfer Protocol (TFTP) server in the cable network, TFTP client in the PS, Hypertext Transfer Protocol (HTTP) server in the cable network, HTTP client in the PS, Transport Layer Security (TLS) [RFC 2246] server in the cable network, TLS client in the PS, and a Key Distribution Center (KDC) server in the cable network.

The CableHome security architecture focuses on securing the LAN from network attack, as well as securing communications between the PS and the Headend servers.

11.2.1 System Design Guidelines

The CableHome security design requirements are listed below in Table 11-1. This list provided guidance for the development of the CableHome security architecture.

Table 11-1 — CableHome Security System Design Guidelines

Reference	Security System Design Guidelines
SEC1	CableHome will include the design necessary to communicate the authentication credentials for CableHome elements.
SEC2	Authentication credentials for PS and critical back office servers will be provided. The credentials will define specific usage and ensure a source of trust.
SEC3	Network management messages between the cable Headend and PS can be authenticated and optionally encrypted to protect against unauthorized monitoring and control.
SEC4	The CableHome firewall will accept configuration files in a standard language and format.[1]
SEC5	The cable operator will have the ability to remotely manage CableHome compliant firewall products through configuration file or SNMP commands
SEC6	The CableHome compliant firewall will include a default set of rules for an expected minimum set of functionality.
SEC7	CableHome will provide the necessary support for PacketCable 1.x through the firewall.
SEC8	A minimum set of requirements will be placed on the firewall filtering capabilities for packet, port, IP addresses, and time of day
SEC9	A detailed firewall event logging interface will allow the cable operator to monitor and review firewall activity as configured.
SEC10	The CableHome firewall will support commonly used applications in specific scenarios.
SEC11	The CableHome firewall will protect the LAN and WAN from common network attacks.
SEC12	The management of the events and rulesets for the firewall will be defined in detail via the CableHome Security MIB.
SEC13	The cable operator will have the ability to securely download software images to the PS element.
Sec14	The cable operator will have the ability to authenticate and optionally encrypt the transport of configuration files for the PS or firewall.

[1] The Firewall Configuration File Requirements are defined in Section 7.4 PS Function - Bulk Portal Services Configuration (BPSC)

This section limits the scope of the specified CableHome security architecture to meet these primary system security requirements. However, it is acknowledged that in some cases additional security is desired

EXHIBIT A

and can be added by the cable operator as needed. The concerns of individual cable operators or manufacturers can result in additional security protections. This specification does not restrict the use of further protections, as long as they do not conflict with the intent and guidelines of this specification.

11.2.2 System Description

The CableHome security architecture includes the following security elements:

- Security-Domain
- Portal Services function (PS)
- CableHome Security Portal function (CSP)
- CableHome Firewall (FW)
- Key Distribution Center (KDC)
- HTTPS Server with TLS

The CableHome architecture defines the PS Element within the residential gateway. Security exists only in a few of the specified interfaces, as the System Design Guidelines require. Figure 11-1 illustrates the relationship between the various CableHome elements which contain security.

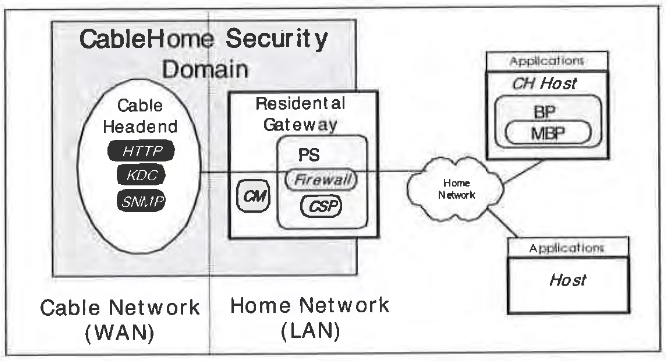


Figure 11-1 – CableHome Security Elements

11.2.2.1 Security Domain

The Security Domain is defined in Figure 11-1, and encompasses the PS element in the residential gateway and the illustrated Headend servers, with specified security. The Security Domain defines the boundary of the sphere of direct influence where security functionality is extended to the residential gateway from the cable network's Headend. The PS element is wholly within the Security Domain, with the exception of the LAN side USFS functionality. The CSP and Firewall act as the boundary elements between the Security-Domain and the non-secure domain.

11.2.2.2 PS Related Security Sub-Elements

The PS includes the following security elements:

- CableHome Security Portal (CSP)
- Firewall (FW)

EXHIBIT A

The CSP acts as a security portal for other PS sub-elements such as negotiating the SNMPv3 keys either through Diffie-Helman or Kerbero, as required. The CSP ensures there is security for SNMPv3 between the NMS and the PS, when turned on by the cable operator. The CSP provides the ability to validate and verify digital certificates for the purposes of authentication and encryption. The CSP initiates, manages, and closes a TLS session for secure downloading of the PS configuration file and firewall configuration file, if instructed by the cable operator during the DHCP exchange.

The PS firewall functionality provides protection to the user, as well as the HFC network, from unwanted traffic coming from the WAN, LAN, or PS address realms. Such traffic can include deliberate attacks on the in-home network, as well as traffic limiting for parental control applications. The CableHome security requirements include specific rules for remote management by the cable operator.

11.2.2.3 Key Distribution Center (KDC) Server

The Key Distribution Center (KDC) server is required if the cable operator deploys CableHome with SNMP provisioning mode. If a KDC server is available in the Headend, it will be used to provide mutual authentication and key distribution services with the use of the Kerberos protocol. If available, the KDC will communicate with the CSP function to establish these services.

11.3 PS Device Authentication Infrastructure

This section describes authentication for the PS device and its communication to the KDC and the HTTPS server.

11.3.1 Device Authentication Infrastructure Goals

It is important to establish the secure identity of the PS element to assist with the following goals:

- Reduce the possibility of device and software cloning, as well as theft of service. The gateways are in a widely distributed environment where the consumer has in-home physical access to the gateway. Providing a secure identity reduces risk of tampering with the gateway hardware device.
- Establish the source of trust. The PKI provides an established source of trust which is rooted within the CableLabs Manufacturer base.

11.3.2 Authentication Infrastructure System Design Guidelines

Table 11-2 – Authentication Infrastructure System Design Guidelines

Reference	Security System Design Guidelines
SEC1	CableHome will include the design necessary to communicate the authentication credentials for CableHome elements.
SEC2	Authentication credentials for CPE and critical back office servers will be provided. The credentials will define specific usage and ensure a source of trust.

11.3.3 Authentication Infrastructure System Description

For security purposes, it is important to know with whom you are communicating prior to exchanging any meaningful information. Authentication provides a secure identity. There are three parts to authentication: the identity credential, the checking of the identity credential for validity, and the common means to securely communicate the identity information. CableHome specifies an industry standard identification credential, X.509 certificates, in conjunction with [RFC 3280] for certificate use, and Kerberos, which is a common communications protocol for mutual authentication. X.509 certificates are exchanged between the PS Element and the KDC during the Kerberos PKINIT exchange, which is wrapped in the AS Request and

EXHIBIT A

AS Reply messages. The PS Element Certificate provides the identity of the associated PS Element by cryptographically binding the PS Element WAN-Man MAC address to a public key certificate. Each side validates the information in the certificate and verifies the certificate chain back to the CableLabs root for each chain. Once the trust has been established, the information for the SNMPv3 keys is sent from the KDC to the PS Element. This authentication section describes the use of Kerberos and X.509 certificates for CableHome.

11.3.4 Authentication Infrastructure Requirements

11.3.4.1 Element Authentication via Kerberos

CableHome specifies authentication when a KDC that supports CableHome, is available in the Headend. If a KDC is available, it is recommended that the cable operator provision the PS Element in SNMP Provisioning Mode (as described in Section 5.2), to take advantage of the CableHome specified mutual authentication protocol with the use of Kerberos, using the PKINIT extension. Kerberos provides a protocol to secure mutual authentication in order to provide keying material and communication establishment only between authenticated parties on the CableHome network. Because this authentication model has been specified by another CableLabs project, i.e., PacketCable, CableHome references the PacketCable model when appropriate.

Various Kerberos MIB objects are required by PacketCable. CableHome has defined some MIB objects to cover the Kerberos functionality needed by CableHome. These MIB objects are defined in the CableHome Security MIB and described in the MIB Object sections of this chapter.

Communication between the KDC and PS is initiated by the PS immediately after the DHCP options are processed during provisioning, if the DHCP options require the PS to initiate communication to the KDC. The DHCP options specified in Section 7.3.3.2.4 require option 177, sub-option 51, which contains the value for the KDC's IP Address to be included with the other DHCP options, and MUST be used by the PS to establish communication between the PS and KDC. Even though PacketCable requires a DNS name as part of the DHCP options, DNS is not required for CableHome and, therefore, the IP address of the KDC is required for the PS to be able to find the appropriate KDC.

11.3.4.1.1 Kerberos/PKINIT

When the PS Element is provisioned in SNMP Provisioning Mode, CableHome specifies the use of Kerberos with the PKINIT public key extension for authenticating CableHome elements and supporting key management requirements. CableHome elements (clients) authenticate themselves to the KDC with the PKINIT protocol. Once authenticated to the KDC, clients will receive a Kerberos ticket for authenticating themselves to a particular CableHome server.

In SNMP provisioning mode, the PS Element, the NMS (i.e. SNMP Manager) and KDC MUST follow the specification for Kerberos/PKINIT, as defined in [PKT-SEC] sections 6.4 and 6.5, unless otherwise noted in this specification. The CableHome KDC is equivalent to or the same as the PacketCable MSO KDC (PacketCable specifies the use of several KDCs). The CableHome specification uses the term Network Management Systems (NMS) to provide SNMP functionality. In referencing the PacketCable suite of specifications, it is noted that PacketCable uses the term provisioning server to denote SNMP functionality. This SNMP functionality in general is be compatible within both specifications. However, they are not identical as PacketCable and CableHome specific information is specified. The PS element MUST act as the client to the KDC. In the PacketCable Security Specification, the MTA is the client and is expected that CableHome implementations will use the client functionality specified for the MTA, for the PS element. The PS element makes use of Kerberos for SNMP key management, as well as for device authentication. The certificates used in PKINIT for CableHome are specified in the PKI Section of this document. Where PacketCable specifies an MTA device certificate, CableHome provides a certificate for the PS Element (PS Element Certificate), and implementations of PS Elements MUST include the PS Element Certificate.

EXHIBIT A

The following sections for Kerberos functionality from [PKT-SEC] do not apply to CableHome:

- section 6.4.2.1.3 Pre-Authenticator for Provisioning Sever Location
- section 6.4.6 MTA Principal Names
- section 6.4.7 Mapping of MTA MAC Address to MTA FQDN
- section 6.4.9 Service Key Versioning
- section 6.4.10 Kerberos Cross-Realm Operation
- section 6.5.2.1 Rekey Messages
- section 6.5.3 Kerberized IPSec
- section 6.4.5 Kerberos Server Locations and Naming Conventions

11.3.4.1.2 CableHome Specific Authentication Variables

The model PacketCable specifies includes some specific variable names for Kerberos in the PacketCable Network Architecture. In order for CableHome to use the PacketCable model, the following variable names MUST to be changed:

- Replace pktcKdcToMtaMaxClockSkew as defined in the PacketCable Security Spec, with KdcToClientMaxClockSkew.
- Replace pktcSrvrToMtaMaxClockSkew as defined in the PacketCable Security Spec, with SrvrToClientMaxClockSkew.
- Replace mtaprovsrvr as defined in the PacketCable Security Specification, with provsrvr.

CableHome Kerberos implementations MUST ignore the Object Identifier (OID) field portion, which reads clabProjPacketCable (2), within the AppSpecificTypedData, within the KRB-ERROR messages.

11.3.4.1.3 CableHome profile for Kerberos Server Locations and Naming Conventions

Kerberos Realm names MAY use the same syntax as a domain name. However, Kerberos Realms MUST be in all capitals. Kerberos Realm details MUST be followed according to [PKT-SEC], Appendix B.

The KDC conventions listed in [PKT-SEC], Section 6.4.5.2 are considered informative for CableHome with the expectation that the KDC will perform the necessary functions in the back office to exchange the appropriate information with the NMS (provisioning server or SNMP manager). The PS element has provided the KDC with the provisioning server IP address in the AS Request, as the necessary information to make appropriate contact between the KDC and provisioning server.

A PS Element principal name MUST be of type NT-SRV-INST with exactly two components, where the first component MUST be the string "PS" (not including the quotes), and the second component MUST be the WAN-Man-MAC address:[91]

PSElement/<WAN-Man-MAC>

where <WAN-Man-MAC> is the WAN Management MAC address of the PS Element. The format the <WAN-Man-MAC> MUST be "XX:XX:XX:XX:XX:XX" (not including the quotes), where X is a hexadecimal character of the MAC address. Hexadecimal characters a-f MUST be in lower case.

A NMS Element principal name MUST be of type NT-SRV-HST with exactly two components, where the first component MUST be the string "provsrvr" (not including the quotes), and the second component MUST be the service provider's SNMP entity address:

provsrvr/<SNMP entity address>

[91] Revised this paragraph per ECN CH1.1-N-03056 by GO on 10/28/03.

EXHIBIT A

The <SNMP entity address> MUST be the service provider's SNMP entity IP address (CDC DHCP Option 177, sub-option 3) in dotted notation enclosed in square brackets (e.g. [12.34.56.78]).

11.3.4.2 CableHome Public Key Infrastructure (PKI)

CableHome uses public key certificates, which comply with the [ITU-T X.509] specification and the IETF [RFC 3280].

11.3.4.2.1 Generic Certificate Requirements

This section describes what is commonly referred to as the generic structure, since all certificates share these requirements. All certificates specified in this section MUST include the following information:

- Certificate Version- The Version of the certificates MUST be [ITU-T X.509], v3, and noted as v2 in the actual certificate. All certificates MUST comply with [RFC 3280], except where the non-compliance with the RFC is explicitly stated in this chapter of this document. Any non-compliance request by this document for content does not imply non-compliance for format. Any specific non-compliance request for format will be explicitly described.
- Public Key Type - RSA Public Keys are used throughout the CableHome certificate hierarchies described in Section 11.3.4.2.2. The subjectPublicKeyInfo.algorithm OID used MUST be 1.2.840.113549.1.1.1 (rsaEncryption). The public exponent for all RSA CableHome keys MUST be F_4 - 65537.
- Extensions- The extensions (subjectKeyIdentifier, authorityKeyIdentifier, KeyUsage, and BasicContraints) MUST follow [RFC 3280]. All other certificate extensions, if included, MUST be marked as non-critical. The encoding tags are [c:critical, n:non-critical; m:mandatory, o:optional] and are identified in the table for each certificate.
- subjectKeyIdentifier - The subjectKeyIdentifier extension included in all CableHome certificates as required by [RFC 3280] (e.g., all certificates except the device and ancillary certificates) MUST include the keyIdentifier value composed of the 160-bit SHA1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length and number of unused bits from the ASN1 encoding) (See [RFC 3280]).
- authorityKeyIdentifier - The authorityKeyIdentifier extension included in all CableHome certificates as required by [RFC 3280], MUST include the subjectKeyIdentifier from the issuer's certificate (see [RFC 3280]), with the exception of root certificates.
- KeyUsage - The keyUsage extension MUST be used for all CableHome Certification Authority (CA) certificates and Code Verification Certificates (CVCs). For CableHome CA certificates, the keyUsage extension MUST be marked as critical with a value of keyCertSign and cRLSign. For CVC certificates, the keyUsage extension MUST be marked as critical with a value of digitalSignature and keyEncipherment. The end-entity certificates MAY use the keyUsage extension as listed in [RFC 3280].
- BasicConstraints - The basicConstraints extension MUST be used for all CableHome CA and CVC certificates and MUST be marked as critical. The values for each certificate for basicConstraints MUST be marked as specified in the certificate description Table 11-2 through Table 11-14.
- Signature Algorithm - The signature mechanism used MUST be SHA-1 [FIPS 186] with RSA Encryption. The specific OID is 1.2.840.113549.1.1.5.
- SubjectName and IssuerName - If a string cannot be encoded as a PrintableString, it MUST be encoded as a UTF8String (tag [UNIVERSAL 12]).

EXHIBIT A

When encoding an X.500 Name:

- Each RelativeDistinguishedName (RDN) MUST contain only a single element in the set of X.500 attributes.
- The order of the RDNs in an X.500 name MUST be the same as the order in which they are presented in this specification.

- serialNumber - The serial number MUST be a unique, positive integer assigned by the CA to each certificate (i.e., the issuer name and serial number identify a unique certificate). CAs MUST force the serialNumber to be a non-negative integer. The Manufacturer SHOULD NOT impose or assume a relationship between the serial number of the certificate and the serial number of the modem to which the certificate is issued.

Given the uniqueness requirements above, serial numbers can be expected to contain long integers. Certificate users MUST be able to handle serialNumber values up to 20 octets. Conformant CAs MUST NOT use serialNumber values longer than 20 octets.

11.3.4.2.2 CableHome Certificate Hierarchies

There are three distinct certificate hierarchies used in CableHome:

1. CableLabs Manufacturer Chain is used to identify CableLabs authorized manufacturers;

2. CableLabs Code Verification Chain is used to identify CableLabs compliant software images;

3. CableLabs Service Provider Chain is used to identify devices on the Service Provider's network for mutual authentication to the subscriber's devices.

The certificate hierarchies described in this document can apply to all CableLabs projects needing certificates. Each project can adopt this hierarchy as there is an opportunity to move to a more generic, shared certificate structure. Also, each project can make specific adjustments in the requirements for that particular project. It is a goal of the CableLabs security team to create a PKI which can be re-used for every CableLabs project. There can be differences in the end-entity certificates required for each project. However, in the cases where end-entity certificates overlap, one end-entity certificate could be used for several services within the cable infrastructure. For example, PacketCable requires a KDC for the service provider and CableHome also requires a KDC for the service provider. If the service provider is running both network architectures on their systems, they can use the same KDC and the same KDC certificate for communication on both systems, i.e., PacketCable and CableHome. In this case, the CableHome KDC is equivalent to the PacketCable MSO KDC (PacketCable specifies the use of several KDCs).

In Figure 11-2, the term Certificate Authority is abbreviated as CA and Code Verification Certificate is abbreviated as CVC.

EXHIBIT A

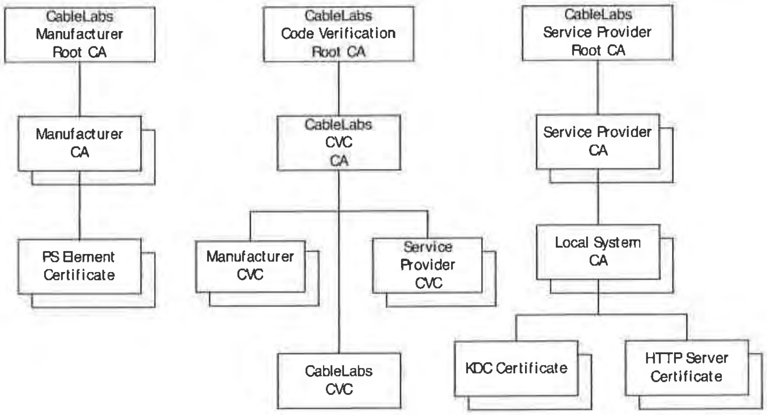


Figure 11-2 — CableHome Certificate Hierarchy

11.3.4.2.2.1 CableLabs Manufacturer Certificate Hierarchy

The CableLabs Manufacturer certificate hierarchy, or Manufacturer chain, is rooted at a CableLabs Manufacturer Root CA, which is used to issue Manufacturer Certification Authority (CA) certificates for a set of authorized CableLabs manufacturers. Manufacturers request PS Element Certificates from a first-tier CA (e.g., a Manufacturer CA or the CableLabs Hosted Manufacturer CA). This chain is used for authentication of devices in the home.[92]

The information contained in the following tables are the CableHome specific values for the required fields according to [RFC 3280]. These CableHome specific values for the CableLabs Manufacturer Certificate hierarchy MUST be followed according to Table 11-3, Table 11-4, Table 11-5 and Table 11-6. If a required field is not specifically listed in the tables, then the guidelines in [RFC 3280] MUST be followed. The generic extensions for CableHome MUST also be included as specified in CableHome PKI Section 11.3.4.2.

CableLabs Manufacturer Root CA Certificate

The CableLabs Manufacturer Root CA Certificate (see Table 11-3) MUST be verified as part of the certificate chain containing the CableLabs Manufacturer Root CA Certificate, Manufacturer CA Certificate and the PS Element Certificate.

Table 11-3 — CableLabs Manufacturer Root CA Certificate

CableLabs Manufacturer Root CA Certificate	

Subject Name Form	C=US
	O=CableLabs
	CN=CableLabs Manufacturer Root CA

Intended Usage	This certificate is used to issue Manufacturer CA Certificates.
Signed By	Self-Signed
Validity Period	20+ years

[92] Revised this paragraph per ECN CH1.1-N-04.0120-2 by KB on 4/5/04.

EXHIBIT A

CableLabs Manufacturer Root CA Certificate	
Modulus Length	2048
Extensions	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true)

Manufacturer CA Certificate

If the manufacturer is issued a CA Certificate and it is used to issue the PS Element Certificate, it MUST be verified as part of a certificate chain containing the CableLabs Manufacturer Root CA Certificate, the Manufacturer CA Certificate, and the PS Element Certificate.[93]

The state/province, city, and manufacturer's facility are optional attributes. A manufacturer MAY have more than one manufacturer's CA certificate. If a manufacturer is using more than one manufacturer CA certificate, the PS element MUST have access to the appropriate certificate as verified by matching the issuer name in the PS Element Certificate with the subject name in the Manufacturer CA Certificate. The authorityKeyIdentifier of the PS Element Certificate MUST be matched to the subjectKeyIdentifier of the manufacturer certificate as described in [RFC 3280].

Table 11-4 – Manufacturer CA Certificate

Manufacturer CA Certificate	

Subject Name Form	C=<country>
	O=<CompanyName>
	[ST=<state/province>]
	[L=<city>]
	OU=CableLabs
	[OU=<Manufacturer's Facility>]
	CN=<CompanyName> Mfg CA

Intended Usage	This certificate is issued to each Manufacturer by the CableLabs Manufacturer Root CA and can be provided to each PS Element either at manufacture time, or during a field code update. This certificate appears as a read-only parameter in the PS element. This certificate issues PS Element Certificates. This certificate, along with the CableLabs Manufacturer Root CA Certificate and the PS Element Certificate, is used to authenticate the PS element identity. The optional listing for manufacturer's facility can be the facility name and/or facility location.
Signed by	CableLabs Manufacturer Root CA
Validity Period	20 Years
Modulus Length	2048
Extensions	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=0)

[93] Revised this paragraph per ECN CH1.1-N-04.0120-2 by KB on 4/5/04.

EXHIBIT A

The Company Name in the Organization (O) field MAY be different than the Company Name in the Common Name (CN) field.

CableLabs Hosted Manufacturer CA Certificate[94]

When the CableLabs Hosted Manufacturer CA Certificate is used to issue the PS Element Certificate it MUST be verified as part of a certificate chain containing the CableLabs Manufacturer Root CA Certificate, the CableLabs Hosted Manufacturer CA Certificate, and the PS Element Certificate.

The state/province, city, and manufacturer's facility are optional attributes. The authorityKeyIdentifier of the PS Element Certificate MUST be matched to the subjectKeyIdentifier of the CableLabs Hosted Manufacturer CA Certificate as described in [RFC 3280].

Table 11-5 — CableLabs Hosted Manufacturer CA Certificate

Manufacturer CA Certificate	

Subject Name Form	C=<country>
	O=<CompanyName>
	[ST=<state/province>]
	[L=<city>]
	OU=CableLabs
	[OU=<CA Identifier>]
	CN=<CompanyName> Mfg CA

Intended Usage	This certificate is issued by the CableLabs Manufacturer Root CA and can be provided to each PS Element either at manufacture time, or during a field code update. This certificate appears as a read-only parameter in the PS element. This certificate issues PS Element Certificates. This certificate, along with the CableLabs Manufacturer Root CA Certificate and the PS Element Certificate, is used to authenticate the PS element identity.
Signed by	CableLabs Manufacturer Root CA
Validity Period	20 Years
Modulus Length	2048
Extensions	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=0)

The Company Name in the Organization (O) field MAY be different than the Company Name in the Common Name (CN) field.

PS Element Certificate[95]

The PS Element Certificate MUST be verified as part of a certificate chain containing the CableLabs Manufacturer Root CA Certificate, Manufacturer CA Certificate or CableLabs Hosted Manufacturer CA Certificate and the PS Element Certificate.[96]

[94] Added this item including table per ECN CH1.1-N-04.0120-2 by KB on 4/5/04.

[95] Revised Table 11-6 per ECN CH1.1-N-03.0074-3 by GO on 12/5/03.

[96] Revised this paragraph per ECN CH1.1-N-04.0120-2 by KB on 4/5/04.

EXHIBIT A

The state/province, city, product name and manufacturer's facility are optional attributes.

The PS Element WAN-Man MAC address MUST be expressed as six pairs of hexadecimal digits separated by colons, e.g., "00:60:21:A5:0A:23". The Alpha HEX characters (A-F) MUST be expressed as uppercase letters.

A PS Element Certificate is permanently installed and not renewable or replaceable. Therefore, the PS Element Certificate has a validity period greater than the expected operational lifetime of the specific device.

Table 11-6 – PS Element Certificate

PS Element Certificate	

Subject Name Form	C=<country>
	O=<Company Name>
	[ST=<state/province>]
	[L=<city>]
	OU=CableHome
	[OU=<Product Name>]
	[OU=<Manufacturer's Facility>]
	CN=<WAN-Man MAC Address>

Intended Usage	This certificate is issued by the Manufacturer CA and installed in the factory. The NMS server cannot update this certificate. This certificate appears as a read-only parameter in the PS Element. This certificate is used to authenticate the PS element identity
Signed By	Manufacturer CA
Validity Period	20+ years
Modulus Length	1024, 1536, 2048
Extensions	keyUsage [c,m] (digitalSignature, keyEncipherment), authorityKeyIdentifier [n,m]

11.3.4.2.2.2 CableLabs Code Verification Certificate Hierarchy

The Code Verification Certificate (CVC) hierarchy, or code verification chain, is rooted at a CableLabs Code Verification Root CA, which issues the CableLabs Code Verification CA certificate. The CableLabs Code Verification CA is used to issue CVCs to a set of authorized manufacturers and service providers. The CableLabs Code Verification CA also issues the CableLabs CVC. This chain is specifically used to authenticate software downloads. The CableHome PKI allows for Manufacturer CVCs, a CableLabs CVC and Service Provider CVCs.

The information contained in the following tables are the CableHome specific values for the required fields according to [RFC 3280]. These CableHome specific values for the CableLabs Code Verification Certificate hierarchy MUST be followed according to Table 11-7, Table 11-8, Table 11-9, Table 11-10, and Table 11-11 below. If a required field is not specifically listed in the tables, the guidelines in [RFC 3280] MUST be followed. The generic extensions for CableHome MUST also be included as specified in CableHome PKI Section 11.3.4.2.

CableLabs Code Verification Root CA Certificate

This certificate MUST be verified as part of the certificate chain containing the CableLabs Code Verification Root CA Certificate, the CableLabs Code Verification CA, and the Code Verification Certificates.

EXHIBIT A

Table 11-7 – CableLabs Code Verification Root CA Certificate

CableLabs Code Verification Root CA Certificate	

Subject Name Form	C=US
	O=CableLabs
	CN=CableLabs CVC Root CA

Intended Usage	This certificate is used to sign Code Verification CA Certificates
Signed By	Self-signed
Validity Period	20+ years
Modulus Length	2048
Extensions	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true)

CableLabs Code Verification CA Certificate

The CableLabs Code Verification CA Certificate MUST be verified as part of a certificate chain containing the CableLabs Code Verification Root CA Certificate, CableLabs Code Verification CA Certificate, and the Code Verification Certificate. A Stand-Alone PS MUST only support one CableLabs CVC CA at a time.

Table 11-8 – CableLabs Code Verification CA Certificate

CableLabs Code Verification CA Certificate	

Subject Name Form	C=US
	O=CableLabs
	CN=CableLabs CVC CA

Intended Usage	This certificate is issued to CableLabs by the CableLabs Code Verification Root CA. This certificate issues Code Verification Certificates.
Signed By	CableLabs Code Verification Root CA
Validity Period	20 years
Modulus Length	2048
Extensions	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints [c,m](cA=true, pathLenConstraint=0)

Manufacturer Code Verification Certificate

This certificate MUST be verified as part of the certificate chain containing the CableLabs Code Verification Root CA Certificate, CableLabs Code Verification CA Certificate, and Code Verification Certificates.

EXHIBIT A

Table 11-9 – Manufacturer Code Verification Certificate

Manufacturer Code Verification Certificate	

Subject Name Form	C=<country>
	O=<CompanyName>
	[ST=<state/province>]
	[L=<city>]
	CN=<CompanyName> Mfg CVC

Intended Usage	The CableLabs Code Verification CA issues this certificate to each authorized Manufacturer. It is used in the policy set by the cable operator for secure software download. The CompanyName in the O and CN fields may be different.
Signed By	CableLabs Code Verification CA
Validity Period	up to 10 years
Modulus Length	1024, 1536, 2048
Extensions	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m]

CableLabs Code Verification Certificate

The CableLabs Code Verification Certificate MUST be verified as part of a certificate chain containing the CableLabs Code Verification Root CA Certificate, CableLabs Code Verification CA Certificate, and CableLabs Code Verification Certificate.

Table 11-10 – CableLabs Code Verification Certificate

CableLabs Code Verification Certificate	

Subject Name Form	C=US
	O=CableLabs
	CN=CableLabs CVC

Intended Usage	The CableLabs Code Verification CA issues this certificate. It is used to authenticate CableLabs certified code. It is used in the policy set by the cable operator for secure software download
Signed By	CableLabs Code Verification CA
Validity Period	up to 10 years
Modulus Length	1024, 1536, 2048
Extensions	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m]

Service Provider Code Verification Certificate

The Service Provider Code Verification Certificate MUST be verified as part of a certificate chain containing the CableLabs Code Verification Root CA Certificate, CableLabs Code Verification CA Certificate, and Service Provider Code Verification Certificate.

EXHIBIT A

Table 11-11 – Service Provider Code Verification Certificate

Service Provider Code Verification Certificate	

Subject Name Form	C=<country>
	O=<CompanyName>
	[ST=<state/province>]
	[L=<city>]
	CN=<CompanyName> Service Provider CVC

Intended Usage	The CableLabs Code Verification CA issues this certificate to each authorized Service Provider. It is used in the policy set by the cable operator for secure software download. The CompanyName in the O and CN fields may be different.
Signed By	CableLabs Code Verification CA
Validity Period	up to 10 years
Modulus Length	1024, 1536, 2048
Extensions	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m]

11.3.4.2.2.3 CableLabs Service Provider Certificate Hierarchy

The CableLabs Service Provider certificate hierarchy, or Service Provider chain, is rooted at a CableLabs Service Provider Root CA, which is used to issue certificates for a set of authorized CableLabs Service Providers. The Service Provider CA can be used to issue optional Local System CA Certificates or ancillary certificates. If the Service Provider CA does not issue the ancillary certificates, the Local System CA will. The ancillary certificates are the end entity certificates on the cable operator's network. CableLabs will host a Service Provider CA for those MSOs who do not want to manage their own Service Provider CA.[97]

The information contained in the following tables are the CableHome specific values for the required fields according to [RFC 3280]. These CableHome specific values for the CableLabs Service Provider Certificate hierarchy MUST be followed according to Table 11-12 through Table 11-15 below. If a required field is not specifically listed in the tables, the guidelines in [RFC 3280] MUST be followed. The generic extensions for CableHome MUST also be included as specified in CableHome PKI Section 11.3.4.2.

CableLabs Service Provider Root CA Certificate

This certificate MUST be verified as part of the certificate chain containing the CableLabs Service Provider Root CA Certificate, Service Provider CA Certificate, optional Local System CA Certificate, and Ancillary Certificates.

[97] Revised this paragraph per ECN CH1.1-N-04.0120-2 by KB on 4/5/04.

EXHIBIT A

Table 11-12 – CableLabs Service Provider Root CA Certificate

CableLabs Service Provider Root CA Certificate	

Subject Name Form	C=US
	O=CableLabs
	CN=CableLabs Service Provider Root CA

Intended Usage	This certificate is used to issue Service Provider CA Certificates
Signed By	Self-signed
Validity Period	20+ years
Modulus Length	2048
Extensions	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true)

Service Provider CA Certificate

The Service Provider CA certificate MUST be verified as part of the certificate chain containing the CableLabs Service Provider Root CA Certificate, Service Provider CA Certificate, optional Local System CA Certificate, and Ancillary Certificates.

Table 11-13 – Service Provider CA Certificate

Service Provider CA Certificate	

Subject Name Form	C=<country>
	O=<CompanyName>
	CN=<CompanyName> CableLabs Service Provider CA

Intended Usage	The CableLabs Service Provider Root CA issues this certificate to each Service Provider. In order to make it easy to update this certificate, each network element is configured with the OrganizationName attribute of the Service Provider CA Certificate SubjectName. This is the only attribute in the certificate that must remain constant. This certificate appears as a read-write parameter in the MIB object that identifies the OrganizationName attribute for the CableHome Kerberos realm. The CableHome element does not accept Service Provider certificates that do not match this value of the OrganizationName attribute in the SubjectName. If the Headend contains a KDC that supports CableHome, then the PS element needs to perform the first PKINIT exchange with the KDC right after a reboot, at which time its MIB tables are not yet configured. At that time, the CableHome Kerberos client MUST accept any Service Provider OrganizationalName attribute, but it MUST later check that the value added into the MIB object for this realm is the same as the one in the initial PKINIT reply. This CA issues Local System CA certificates or ancillary certificates.
Signed By	CableLabs Service Provider Root CA
Validity Period	20 years
Modulus Length	2048
Extensions	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=1)

EXHIBIT A

The Company Name in the Organization (O) field MAY be different than the Company Name in the Common Name (CN) field.

Local System CA Certificate

This certificate is optional for the service provider. If this certificate exists, it MUST be verified as part of the certificate chain containing the CableLabs Service Provider Root CA Certificate, Service Provider CA Certificate, optional Local System CA Certificate, and Ancillary Certificates.

Table 11-14 – Local System CA Certificate

Local System CA Certificate	

Subject Name Form	C=<country>
	O=<CompanyName>
	OU=<Local System Name>
	CN=<CompanyName> CableLabs Local System CA

Intended Usage	This certificate is optional, and if it exists, is issued by the Service Provider CA. This CA issues ancillary certificates. Network servers are allowed to move freely between regional CAs of the same service provider.
Signed By	Service Provider CA
Validity Period	20 years
Modulus Length	1024, 1536, 2048
Extensions	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=0)

The Company Name in the Organization (O) field MAY be different than the Company Name in the Common Name (CN) field.

KDC Certificate

This certificate MUST be verified as part of the certificate chain containing the CableLabs Service Provider Root CA Certificate, Service Provider CA Certificate, optional Local System CA Certificate, and Ancillary Certificates (e.g., the KDC Certificates).

The KDC Certificate MUST include the Kerberos PKINIT subjectAltName as specified in [PKT-SEC] subsection "Key Distribution Center Certificate."

Table 11-15 – KDC Certificate

KDC Certificate	

Subject Name Form	C=<country>
	O=<Company Name>
	[OU=<Local System Name>]
	OU= CableLabs Key Distribution Center
	CN=<DNS Name>

EXHIBIT A

KDC Certificate	
Intended Usage	This certificate is issued either by the Service Provider CA or the Local System CA. It is used to authenticate the identity of the KDC to the Kerberos clients during PKINIT exchanges. This certificate is passed to the PS element inside the PKINIT reply.
Signed By	Service Provider CA or the Local System CA
Validity Period	20 years
Modulus Length	1024, 1536, 2048
Extensions	keyUsage[c,o](digitalSignature) authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>) subjectAltName[n,m] (see [PKT-SEC], Appendix C)

HTTPS server Server Certificate[98]

This certificate MUST be verified as part of the certificate chain containing the CableLabs Service Provider Root CA Certificate, Service Provider CA Certificate, optional Local System CA Certificate, and Ancillary Certificates (e.g., the KDC Certificates).

Table 11-16 — HTTPS Server Certificate

HTTPS Server Certificate	

Subject Name Form	C=<country>
	O=<Company Name>
	[OU=<Local System Name>]
	OU= CableLabs HTTPS Server
	CN=<DNS Name>

Intended Usage	This certificate is issued either by the Service Provider CA or the Local System CA. It is used to authenticate the identity of the HTTPS server to the HTTP clients for the TLS session during provisioning. This certificate is passed to the PS element inside the TLS Server Certificate message.
Signed By	Service Provider CA or the Local System CA
Validity Period	20 years
Modulus Length	1024, 1536, 2048
Extensions	keyUsage[c,m](digitalSignature, keyEncipherment, dataEncipherment), extendedKeyUsage[n,m] (id-kp-serverAuth), authorityKeyIdentifier [n,m]

11.3.4.2.3 Certificate Validation

CableHome certificate validation involves validation of a linked chain of certificates from the end entity certificates up to the valid Root. For example, the signature on the PS Element Certificate is verified with the CableLabs Manufacturer CA Certificate, and then the signature on the CableLabs Manufacturer CA Certificate is verified with the CableLabs Manufacturer Root CA Certificate. The CableLabs Manufacturer Root CA Certificate is self- signed, and is received from a trusted source in a secure way. The public key present in the CableLabs Manufacturer Root CA Certificate is used to validate the signature on the same certificate.

[98] Revised Table 11-16 per ECN CH1.1-N-03.0074-3 by GO on 12/5/03.

EXHIBIT A

The exact rules for certificate chain validation MUST fully comply with [RFC 3280], where they are referred to as "Certificate Path Validation." In general, [ITU-T X.509] certificates support a liberal set of rules for determining if the issuer name of a certificate matches the subject name of another. The rules are such that two name fields MAY be declared to match, even though a binary comparison of the two name fields does not indicate a match. [RFC 3280] recommends that certificate authorities restrict the encoding of name fields, so that an implementation can declare a match or mismatch, using simple binary comparison. CableHome security follows this recommendation. Accordingly, the DER-encoded tbsCertificate.issuer field of a CableHome certificate MUST be an exact match to the DER-encoded tbsCertificate.subject field of its issuer certificate. An implementation MAY compare an issuer name to a subject name by performing a binary comparison of the DER-encoded tbsCertificate.issuer and tbsCertificate.subject fields.

The CableHome validation of validity periods for nesting is not checked and intentionally not enforced, which is compliant with current standards. At the time of issuance, the validity start date for any end-entity certificate MUST be the same as or later than the start date of the issuing CA certificate validity period. After a CA certificate is renewed, the start dates of end-entity certificates MAY be earlier than the start date of the issuing CA certificate. The validity end date for end entity certificates MAY be before, the same as, or after the validity end date for the issuing CA, as specified in the CableHome Certificate tables.

11.3.4.2.3.1 Validation for the Manufacturer Chain and Root Verification

The KDC will validate the linked chain of manufacturer certificates. Usually the first certificate in the chain is not explicitly included in the certificate chain that is sent over the wire. In the cases where the CableLabs Manufacturer Root CA Certificate is explicitly included over the wire, it MUST already be known to the verifying party ahead of time to verify this certificate. The CableLabs Manufacturer Root CA Certificate sent over the wire MUST NOT contain any changes to the certificate, with the possible exception of the certificate serial number, validity period, and the value of the signature. If changes other than the certificate serial number, validity period, and the value of the signature, exist in the CableLabs Manufacturer Root CA certificate that was passed over the wire in comparison to the known CableLabs Manufacturer Root CA Certificate, the KDC making the comparison MUST fail the certificate verification.[99]

11.3.4.2.3.2 Validation for the Code Verification Chain and Root Verification

A back office server can check the validity of the Code Verification Chain prior to beginning the software download process. For details, see the secure software download Section 11.8 of this document.

11.3.4.2.3.3 Validation for the Service Provider Chain and Root Verification

The CableHome PS Element MUST validate the linked chain of Service Provider certificates. Usually the first certificate in the chain is not explicitly included in the certificate chain that is sent over the wire. In the cases where the CableLabs Service Provider Root CA Certificate is explicitly included over the wire, it MUST already be known to the verifying party ahead of time to verify this certificate. The CableLabs Service Provider Root CA Certificate MUST NOT contain any changes to the certificate, with the possible exception of the certificate serial number, validity period, and the value of the signature. If changes other than the certificate serial number, validity period, and the value of the signature, exist in the CableLabs Service Provider Root CA Certificate that was passed over the wire in comparison to the known CableLabs Service Provider Root CA Certificate, the PS element making the comparison MUST fail the certificate verification.

11.3.4.2.4 Certificate Revocation

Certificate revocation is out of scope for CableHome.

[99] Revised the first sentence of this paragraph per ECN CH1.1-N-03056 by GO on 10/28/03.

EXHIBIT A

11.4 Secure Management Messaging to the PS

The security algorithm used to initialize SNMP management messaging depends upon the provisioning mode of the PS element (see Section 5.5). In CableHome 1.1, there are three provisioning modes: DHCP Provisioning Mode, SNMP Provisioning mode, and Dormant mode. DHCP Provisioning Mode has additional sub-modes that identify whether it is configured for NmAccess Mode or Coexistence Mode. SNMP Provisioning Mode requires SNMPv3 for management messaging.

The following sections describe the security algorithms and requirements needed to initialize SNMP management messaging, based on the provisioning mode of the PS element. The PS element MUST support the SNMPv3 security algorithms specified in Section 11.4.4.1.2 and Section 11.4.4.2.

11.4.1 Goals of Secure Management Messaging

Securing management messages include the following goals:

- Provide options to encrypt network management messages to the PS
- Provide options to authenticate network management messages to the PS
- If possible, provide security on management messaging that will not require additional protocols to be implemented
- Provide guidelines and minimum requirements for the encryption and authentication algorithms

11.4.2 Secure Management Messaging System Design Guidelines

Reference	Security System Design Guidelines
SEC3	Network management messages between the cable Headend and PS can be authenticated and optionally encrypted to protect against unauthorized monitoring and control.

11.4.3 Secure Management Messaging System Description

CableHome specifies the use of SNMP of management to the PS from the cable operators network. SNMP has been adopted into cable industry products for several years. The cable operator back office can support SNMPv1, v2 or v3. The PS is required to support management messaging for all three versions of SNMP. There is no security, per se, built into SNMPv1 or v2. SNMPv3 provides basic authentication and encryption algorithms defined in [RFC 3410] - [RFC 2576] and CableHome specifies the use of the RFC defined security. SNMPv3 does not specify how the keys are set up to start the encryption and authentication process, and therefore, CableHome specifies some details to generate and establish key exchange. The details are listed within the next section.

11.4.4 Secure Management Messaging Requirements

11.4.4.1 Security Algorithms for SNMP in DHCP Provisioning Mode

In DHCP Provisioning Mode, the PS element can be configured for NmAccess Mode or Coexistence Mode. In Coexistence Mode the PS element can be configured for SNMPv1, SNMPv2, and/or SNMPv3 management messaging.

11.4.4.1.1 NmAccess Mode

If the PS Element is provisioned in DHCP Provisioning Mode with NmAccess Mode, the SNMP-based network management within the PS Element does not use SNMPv3 and therefore does not need to initialize SNMPv3 security functions. Initialization of the SNMPv1/v2 management link is defined in Section 6.3.3.1.

EXHIBIT A

11.4.4.1.2 CoexistenceMode

If the PS Element is provisioned in DHCP Provisioning Mode with Coexistence Mode and the management messaging protocol is determined to be SNMPv3 (see Section 6.3.3.1), then the PS Element MUST use SNMPv3 security specified by [RFC 3414]. The PS MUST support SNMPv3 authentication and SNMPv3 privacy. The cable operator is strongly encouraged to turn on SNMPv3 authentication at all times. The use of SNMPv3 privacy is recommended if the cable operator can handle the additional load for encryption.

In order to establish SNMPv3 keys in DHCP provisioning mode, all CableHome SNMP interfaces MUST utilize the SNMPv3 initialization and key changes procedure as defined in section 2.2 of the DOCSIS 1.1 Operations Support Systems Interface specification, [DOCSIS11] (replace "CM" wording with "PS element" and replace "DOCSIS 1.1 compliant" wording with "CableHome compliant").

To support SNMPv3 initialization and key changes in DHCP provisioning mode, the PS element MUST also be capable of receiving TLVs of type 34, 34.1, and 34.2, as defined in section C.1.2.8 of the DOCSIS 1.1 Radio Frequency Interface specification, [DOCSIS9] and implement the key-change mechanism specified in [RFC 2786] which includes the usmDHKickstartTable MIB object.

11.4.4.1.3 SNMPv3 Key Initialization

For each of up to 5 different security names, the Ultimate Authorization (CHAdministrator) generates a pair of numbers. First, the CHAdministrator generates a random number Rm.

Then, the CH Administrator uses the DH equation to translate Rm to a public number z. The equation is as follows:

z = g ^ Rm MOD p

where g is from the set of Diffie-Hellman parameters, and p is the prime from those parameters.

The PS configuration file is created to include the (security name, public number) pair. The PS MUST support a minimum of 5 pairs. For example:

TLV type 34.1 (SNMPv3 Kickstart Security Name) = CHAdministrator

TLV type 34.2 (SNMPv3 Kickstart Public Number) = z

The PS MUST support the VACM entries defined in Section 6.3.3.1.4.5. Only VACM entries specified by the corresponding security name in the PS configuration file MUST be active.

During the PS boot process, the above values (security name, public number) MUST be populated in the usmDHKickstartTable.

At this point:

usmDHKickstartMgrpublic.1 = "z" (octet string)

usmDHKickstartSecurityName.1 = "CHAdministrator"

When usmDHKickstartMgrpublic.n is set with a valid value during the registration, a corresponding row is created in the usmUserTable with the following values:

usmUserEngineID: localEngineID

EXHIBIT A

usmUserName: usmDHKickstartSecurityName.n value

usmuserSecurityName: usmDHKickstartSecurityName.n value

usmUserCloneFrom: ZeroDotZero

usmUserAuthProtocol: usmHMACMD5AuthProtocol [RFC 2104]

usmuserAuthKeyChange: (derived from set value)

usmUserOwnAuthKeyChange: (derived from set value)

usmUserPrivProtocol: usmDESPrivProtocol

usmUserPrivKeyChange: (derived from set value)

usmUserOwnPrivKeyChange: (derived from set value

usmUserPublic

usmUserStorageType: permanent

usmUserStatus: active

Note: For (PS) dhKickstart entries in usmUserTable, Permanent means it MUST be written to but not deleted and is not saved across reboots.

After the PS has completed initialization (indicated by a value of '1' (pass) for cabhPsDevProvState):

1. The PS generates a random number xa for each row populated in the usmDHKickstartTable which has a non-zero length usmDHKickstartSecurityName and usmDHKickstartMgrPublic.
2. The PS uses DH equation to translate xa to a public number c (for each row identified above).

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

where g is from the set of Diffie-Hellman parameters, and p is the prime from those parameters.

At this point:

usmDHKickstartMyPublic.1 = "c" (octet string)

usmDHKickstartMgrPublic.1 = "z" (octet string)

usmDHKickstartSecurityName.1 = "CHAdministrator"

3. The PS calculates shared secret sk where sk = z ^xa mod p.
4. The PS uses sk to derive the privacy key and authentication key for each row in usmDHKickstartTable and sets the values into the usmUserTable.

EXHIBIT A

As specified in [RFC 2786], the privacy key and the authentication key for the associated username, "CHAdministrator" in this case, is derived from sk by applying the key derivation function PBKDF2 defined in PKCS#5 v2.0.

privacy key <--- PBKDF2(salt = 0xd1310ba6,

iterationCount = 500,

keyLength = 16,

prf = id-hmacWithSHA1) [RFC 2104]

authentication key <---- PBKDF2(salt = 0x98dfb5ac,

iterationCount = 500,

keyLength = 16 (usmHMACMD5AuthProtocol) [RFC 2104],

prf = id-hmacWithSHA1) [RFC 2104]

At this point, the PS (CMP) has completed its SNMPv3 initialization process and MUST allow appropriate access level to a valid securityName with the correct authentication key and/or privacy key.

The PS MUST properly populate keys to appropriate tables as specified by the SNMPv3-related RFCs and [RFC 2786].

5. The following describes the process that the manager uses to derive the PS's unique authentication key and privacy key.

The SNMP manager accesses the contents of the usmDHKickstartTable using the security name of 'dhKickstart' with no authentication.

The PS MUST provide pre-installed entries in the USM table and VACM tables to correctly create user 'dhKickstart' of security level noAuthNoPriv that has read-only access to system group and usmDHkickstartTable.

If the PS is in Coexistence Mode and is configured to use SNMPv3 the Group specification for the dhKickstart View MUST be implemented as follows:

dhKickstart Group	
vacmGroupName	'dhKickstart'
vacmAccessContextPrefix	""
vacmAccessSecurityModel	3 (USM)
vacmAccessSecurityLevel	NoAuthNoPriv
vacmAccessContextMatch	exact
vacmAccessReadViewName	'dhKickstartView'
vacmAccessWriteViewName	""'
vacmAccessNotifyViewName '	""

EXHIBIT A

vacmAccessStorageType	permanent
vacmAccessStatus	active

The VACM View for the dhKickstart view MUST be implemented as follows:

dhKickstartView subtree 1.3.6.1.2.1.1 (System Group) and 1.3.6.1.3.101.1.2.1 (usmDHkickstartTable)

The SNMP manager gets the value of the PS's usmDHKickstartMypublic number associated with the securityName for which the manager wants to derive authentication and privacy keys. Using the private random number, the manager can calculate the DH shared secret. From that shared secret, the manager can derive operational authentication and confidentiality keys for the securityName that the manager is going to use to communicate with the PS.

11.4.4.1.4 Diffie-Hellman Key Changes

The PS MUST support the key-change mechanism specified in the above section as well as [RFC 2786].

11.4.4.2 Security Algorithms for SNMPv3 in SNMP Provisioning Mode

If the PS Element is provisioned in SNMP Provisioning Mode, the SNMP-based network management within the PS Element MUST run over SNMPv3 with security specified by [RFC 3414]. The PS MUST support SNMPv3 authentication and SNMPv3 privacy. The cable operator is strongly encouraged to turn on SNMPv3 authentication at all times. The use of SNMPv3 privacy is recommended if the cable operator can handle the additional load for encryption. In order to establish SNMPv3 keys in SNMP provisioning mode, the PS MUST utilize Kerberized SNMPv3 key management as specified in Section 11.4.4.2.1.

11.4.4.2.1 Kerberized SNMPv3

The Kerberized key management profile specific for SNMPv3 MUST be followed as defined in section 6.5.4 in [PKT-SEC].

11.4.4.2.2 SNMPv3 Encryption Algorithms

The encryption Transform Identifiers for Kerberized SNMPv3 key management MUST be followed as defined in section 6.3.1 in [PKT-SEC].

11.4.4.2.3 SNMPv3 Authentication Algorithms

The authentication algorithms for Kerberized SNMPv3 key management MUST be followed as defined in section 6.3.2 in [PKT-SEC].

11.4.4.2.4 SNMPv3 Engine IDs[100]

Because the SNMP Manager and Client MUST verify that the SNMPv3 Engine ID in the AP Request and AP Reply messages are based on the appropriate NMS principal name in the ticket [PKT-SEC], the following Rules are used in generating SNMPv3 Engine IDs for use in CableHome:

Rule 1: The SNMPv3 Engine ID MUST follow the format defined in [RFC 3411], i.e., the first bit is set to 1 (one) and the appropriate value is used for the first four bytes [RFC 3411];

Rule 2: The fifth byte MUST be the value 4 (four) to indicate that the following bytes, up to 27, are to be considered as text and are defined as follows:

[100] Revised this section per ECN CH1.1-N-03056 by GO on 10/28/03.

EXHIBIT A

- The characters of the NMS principal name MUST be used for the engine ID bytes starting on the 6th byte.
- The sequence of bytes, indicating the NMS principal name, MUST be followed by one byte and is considered as an 8bit Hex value. Each unique value identifies a particular SNMP engine in the device (element or NMS server). The value 0 (zero) MUST not be used.
- The text string that starts on the 6th byte MUST be terminated with a Null character.

Note: Other formats are possible by following the approach in [RFC 3411]. The above selection, though, is intended to reduce implementation complexity that would be required if all of the approaches in [RFC 3411] were allowed.

11.4.4.2.5 Populating the usmUserTable

SNMPv3 security settings for the cable operator "CHAdministrator" user are defined in Section 6.3.6.3 View-based Access Control Model (VACM) Requirements. The CHAdministrator is the ultimate authority for management of the Portal Services element. Other users can also be defined. In this section, a USM user is defined specifically for the provisioning process. In particular, it is defined to enable a notification receiver to be specified for the cabhPsDevProvEnrollTrap and cabhPsDevInitTrap, which the PS is required to send during the provisioning process (ref.: Table 13-1 Flow Descriptions for PS WAN-Man Provisioning Process for DHCP Provisioning Mode, step CHPSWMD-11; Table 13-2 Flow Descriptions for PS WAN-Man Provisioning Process for SNMP Provisioning Mode, step CHPSWMS-11 and step CHPSWMS-13; and Section 13.3.3 Provisioning Enrollment/Provisioning Complete Informs).

The msgSecurityParameters in SNMPv3 messages carry a msgUserName field that specifies the user on whose behalf the message is being exchanged and with whose security information the fields msgAuthenticationParameters and msgPrivacyParameters are produced. For the SNMP engine of a CableHome element to process these messages, the necessary information is required to be entered in the usmUserTable [RFC 3414] for the element engine.

The usmUserTable MUST be populated with the following information in the PS Element right after the AP Reply message is received:

- usmUserEngineID: the local SNMP engine ID as defined in Section 11.4.4.2.4, SNMPv3 Engine IDs[101]
- usmUserName: CHAdministratorxx:xx:xx:xx:xx:xx, where xx:xx:xx:xx:xx:xx is the device's WAN-Man hardware address
- usmUserSecurityName: CHAdministratorxx:xx:xx:xx:xx:xx, where xx:xx:xx:xx:xx:xx is the device's WAN-Man hardware address
- usmUserCloneFrom: 0.0
- usmUserAuthProtocol: indicates the authentication protocol selected for the user, from the AP Reply message
- usmUserAuthKeyChange: default value ""
- usmUserOwnAuthKeyChange: default value ""
- usmUserPrivProtocol: indicates the encryption protocol selected for the user, from the AP Reply message
- usmUserPrivKeyChange: default value ""
- usmUserOwnPrivKeyChange: default value ""
- usmUserPublic: default value ""
- usmUserStorageType: permanent

[101] Revised this bullet statement per ECN CH1.1-N-03056 by GO on 10/28/03.

EXHIBIT A

- usmUserStatus: active

New SNMPv3 users MAY be created with standard SNMPv3 cloning, as defined in [RFC 3414].

The VACM Security To Group Table [RFC 3415] MUST be populated with the following information in the PS right after the AP Reply message is received:

- vacmSecurityModel: 3(usm)
- vacmSecurityName: CHAdministratorxx:xx:xx:xx:xx:xx
- vacmGroupName: CHAdministratorSNMP
- vacmSecurityToGroupStatus: active

The VACM Access Table [RFC 3415] MUST be populated with the following information, linked to the vacmSecurityToGroupTable defined above, in the PS right after the AP Reply message is received:

- vacmAccessContentPrefix: “”
- vacmAccessSecurityModel: 3(usm)
- vacmAccessSecurityLevel: AuthNoPriv
- vacmAccessContextMatch: exact(1)
- vacmAccessReadViewName: CHAdministratorView
- vacmAccessWriteViewName: CHAdministratorView
- vacmAccessNotifyViewName: CHAdministratorNotifyView
- vacmAccessStorageType: permanent
- vacmAccessStatus: active

Seven rows of the VACM View Tree [RFC 3415] MUST be populated with the following information in the PS right after the AP Reply message is received:

- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: cabhPsDevProvEnrollTrap
- vacmViewTreeFamilyType: included
- vacmViewTreeFamilyMask: “”

- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: cabhPsDevBase
- vacmViewTreeFamilyType: included
- vacmViewTreeFamilyMask: “”

- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: docsDevSoftware
- vacmViewTreeFamilyType: included
- vacmViewTreeFamilyMask: “”

- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: cabhPsDevInitTrap
- vacmViewTreeFamilyType: included

EXHIBIT A

- vacmViewTreeFamily Mask: ""

- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: cabhPsDevBase
- vacmViewTreeFamilyType: included
- vacmViewTreeFamily Mask: ""

- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: docsDevEventTable
- vacmViewTreeFamilyType: included
- vacmViewTreeFamily Mask: ""

- vacmViewTreeFamilyName: CHAdministratorNotifyView
- vacmViewTreeFamilySubtree: cabhPsDevProv
- vacmViewTreeFamilyType: included
- vacmViewTreeFamily Mask: ""

11.5 CQoS in the PS

CQoS is a transparent bridge for PacketCable and LAN-to-LAN QoS. The PacketCable DQoS messages between the MTA and the CMTS, CMS, or CM are secured by the PacketCable Security Specification. It is not within the scope of CableHome to add security for PacketCable messages. CableHome 1.1 in-home, LAN-to-LAN QoS messaging is not secured since the threat for attacks within the home are seen as extremely low. It is not within the scope of CableHome to add security for PacketCable messages. Since there is no security requirement for the PS element to secure CQoS messages originated on the WAN, there is no dependency on the back office servers to support this function.

11.6 Firewall in the PS[102]

Security issues have been a major concern for companies relying on networks for decades, and now there is increasing awareness of security and privacy issues for home users with the always on CM. Because the average CableHome subscriber might lack some technical knowledge or even if not, lacks the time to keep their home computers in top-notch secure operation, a firewall has become a necessary first line of defense in protecting the unsecured computers and other LAN IP devices in the home.

11.6.1 Goals and Assumptions of CableHome Firewall

Goals:

- Provide the cable operator with a standard and interoperable configuration for the firewall
- Provide the cable operator with a minimum set of required functionality for the firewall
- Enable monitoring of the firewall events using the event messaging mechanism
- Protect the home network and LAN IP devices on that network from unwanted WAN-to-LAN traffic
- Protect the HFC from unwanted LAN-to-WAN traffic.

[102] Revised this section per ECN CH1.1-N-03.0097-5 by GO on 12/9/03.

EXHIBIT A

- Protect the PS from attacks and traffic deemed as unwanted by the cable operator.
- Ensure the firewall will process packets at sufficient rates so packet filtering does not introduce a performance bottleneck, regardless of the complexity or size of the ruleset.
- Ensure support of identified applications through the firewall for specified scenarios.
- Provide the cable operator the ability to monitor and change rules used by the firewall
- Ensure that the proper security configurations (e.g. filtering rules and policies) exist on the firewall system.
- Identify the types of attacks the firewall will log and specify the log so the operator can view the log as needed.
- Support PacketCable through the firewall
- Notify the administrator of defined important events in real time
- Provide a factory default ruleset to ensure consistent baseline resets of the firewall

Assumptions:

- The firewall treats all packets destined to or coming from the LAN according to the current policy regardless of address mode, CAT or Pass-through. (e.g. address mode has no affect on the firewall operations).
- The firewall begins operation immediately after the provisioning complete message, regardless of provisioning mode.
- SNMP, in particular SNMP messaging directed at the CableHome Management Portal (CMP), can be used to configure CableHome firewall rulesets. Thus, the ruleset is represented, externally as a collection of MIB objects.
- MIB objects control the logging actions taken by the firewall
- The firewall will apply filtering rules and policies in conjunction with checking the translated addresses known to the CAT in the PS.

11.6.2 Firewall System Design Guidelines

Firewall system design guidelines listed in Table 11-17 guided CableHome firewall specifications.

Table 11-17 — CableHome Security System Design Guidelines

Reference	Security System Design Guidelines
SEC4	The CableHome firewall will accept configuration files in a standard language and format.[1]
SEC5	The cable operator will have the ability to remotely manage CableHome compliant firewall products through configuration file or SNMP commands
SEC6	The CableHome compliant firewall will include a default set of rules for an expected minimum set of functionality.
SEC7	CableHome will provide the necessary support for PacketCable through the firewall.
SEC8	A minimum set of requirements will be placed on the firewall filtering capabilities for packet, port, IP addresses, TOD, etc.
SEC9	A detailed firewall event logging interface will allow the cable operator to monitor and review firewall activity as configured.
SEC10	The CableHome firewall will support commonly used applications in specific scenarios.
SEC11	The CableHome firewall will protect the LAN and WAN from common network attacks.

EXHIBIT A

Reference	Security System Design Guidelines
SEC12	The management of the events and rulesets for the firewall will be defined in detail via the CableHome Security MIB.

[1] The Firewall Configuration File Requirements are defined in Section 7.4 PS Function - Bulk Portal Services Configuration (BPSC).

11.6.3 Firewall System Description

Today, firewalls are built using a combination of the following components: Packet Filtering (PF), Stateful Packet Filtering (SPF), Application Level Gateway (ALG), and Application Server Proxy (ASP). A packet-filtering module is probably the most common firewall component because it determines which packet streams are blocked and which are allowed to cross the firewall. Each individual packet decision is based on static configuration information (the ruleset) configured into the firewall's filtering mechanisms (policy) so that the packet will be allowed or denied, based on the inspection of packet header fields: source and destination IP addresses, source and destination protocol port numbers, protocol type, etc. Depending on the desired level of security, a great number of filters might need to be configured on a firewall. The cable operator will need to balance the ruleset complexity with customer needs. CableHome attempts to specify a rich set of configuration filters, managed via MIB objects, so the various types of services (protocols and applications) can be individually configured, if needed.

A stateful packet filtering (SPF) module uses accumulated state information from packets that belong to the same connection when making packet-dropping decisions. The SPF differentiates between different protocols and handles each protocol's connection correctly. The SPF module stores and utilizes information found in the packet's network layer and transport layer headers.

An application level gateway (ALG) is a component that knows how to extract information required for connection tracking from the packet's application layer. As some protocols incorporate connection control information at the application layer, the SPF will incorporate ALGs to perform the connection tracking. The specific ALG (e.g. FTP-ALG, IPSEC-ALG) is required for handling each such protocol needed to support CableHome. For example, the FTP protocol in active mode incorporates the TCP port number that will be used later on for the data transfer. Therefore, it is required to use an FTP ALG to track the state of all FTP connections. See Appendix IV for more information on ALG requirements.

An application specific proxy (ASP) firewall filters, based on the application layer protocol unique features, or messages specifically for the client-server protocols. There are security benefits in the use of ASPs. For one, it is possible to add access control lists to protocols, requiring users or systems to provide some level of authentication before access is granted. In addition to being protocol specific, an ASP understands the protocol and can be configured to block only subsections of the protocol. The ASP allows the operation of NAT-unfriendly applications when the Portal Service is operating in either of its two transparent routing modes: C-NAT or C-NAPT. For example, an FTP ASP can be configured to block the traffic from unauthenticated users, while granting authenticated users selective access to the "put" and "get" commands, depending on which directions these commands are issued.

The particular combination of packet filer, SPF AGLs and ASPs on a given firewall product, constitutes a trade off between performance and the security level. Typically, being a network layer mechanism, packet filters tend to yield better performance than ALGs/ASPs that are application layer mechanisms. A compromise solution becoming increasingly popular consists of the use of stateful packet filtering (SPF), where state information accumulated from packets that belong to the same connection is kept and used in making packet-dropping decision.

SPFs and ASPs both include filtering against the security policy to achieve the desired level of security for a site. However, while the security policy determines the allowed services and the way in which they are used across the firewall, the security policy does not spell out the specific configuration for the firewall. The ruleset is expressed in human readable form, then interpreted by the firewall, and implemented into the

EXHIBIT A

filtering policy in the internal language of the firewall. The filters inspect each packet and determines which packets the firewall forwards and which it rejects.

The following is a high-level diagram of the CableHome firewall and the roles of the various firewall components referenced by this specification.

Note: This diagram does not indicate any specific technical architecture or implementation. It is only for logical reference.

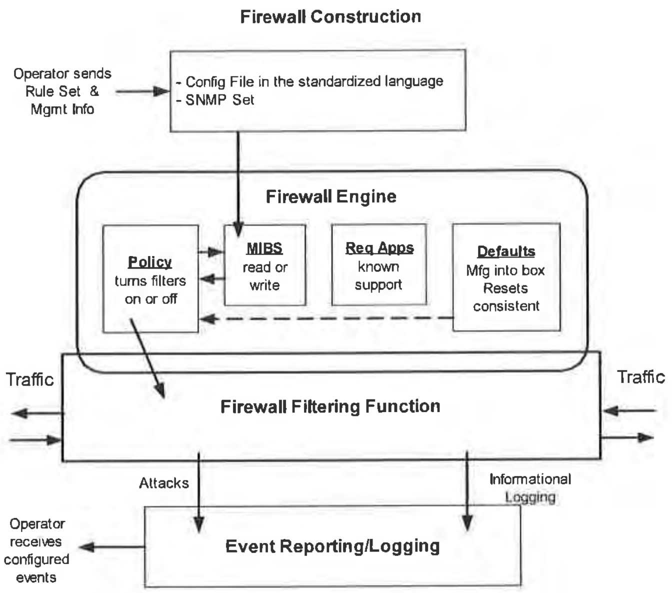


Figure 11-3 – Firewall Logical Reference

11.6.4 Firewall Requirements

11.6.4.1 Configuration File Language for the Firewall

A cable operator chosen ruleset can be configured into the CableHome firewall via a PS configuration file or firewall configuration file download. Within this section the term configuration file is used to mean either the PS configuration file or firewall configuration file. The language and format for the configuration file containing the ruleset applicable to a particular CableHome firewall product is defined.

The PS MUST be able to receive and interpret a firewall configuration file constructed, using TLVs formatted as described in Section 7.4.4.1 Configuration File Format Requirements. Inside the firewall, the compiler translates the policy language into a vender specific internal format. TLV type 28 MUST be used

EXHIBIT A

for all the CableHome firewall MIB objects. The language of the PS configuration file and the firewall configuration file is the same. The requirements for firewall configuration file processing are defined in Section 7.[103]

11.6.4.2 Firewall Configuration

The PS supports, but the operator is not required to utilize, remote management of firewall functions. The firewall in the PS MUST accept rulesets configured in bulk via the specified PS, Firewall Configuration Files, or configured individually via SNMP SET commands. The PS MUST NOT activate the firewall while the value of cabhPsDevProvState = inProgress(2). When a configuration file is used to configure rulesets, upon completion of configuration file download and processing, i.e., cabhPsDevProvState = pass(1), the firewall rules from the configuration file MUST immediately be applied and available for use in the PS without reboot of the PS. If the PS cannot process the configuration file for any reason, i.e., if cabhPsDevProvState = fail(3), the PS MUST use the existing firewall filter table rules indicated by the cabhSec2FwPolicySelection object.

11.6.4.3 Firewall Policy and Rulesets

The firewall policy instructs the firewall to filter traffic based on particular rules. The policy accepts the rulesets to be applied by the filtering function since the filtering function alone has no meaning, as it is only a set of capabilities. The firewall filtering capabilities, combined with the firewall policy, provide firewall protection for the CableHome LAN. The firewall filters actively inspect each packet or connection with the policy to apply the two allowed actions: allow or deny.

CableHome defines three components as inputs into the firewall policy depending upon the configuration:

- General Behavior Rules - the expected behavior for either allowing or denying traffic flows. These rules always apply unless there is an exception written into either the CableHome Factory Default Ruleset or Configured Ruleset
- CableHome Factory Default Ruleset - the firewall filtering factory default rules used as exceptions to the General Behavior Rules. These rules may also be used in conjunction with the Configured Ruleset.
- Configured Ruleset - the configured rules used as exceptions to the General Behavior Rules. These rules may also be used in conjunction with the CableHome Factory Default Ruleset.

The General Behavior Rules, CableHome Factory Default Ruleset, and the Configured Ruleset apply to session initiation traffic and not to response traffic

The PS may receive traffic for the PacketCable MTA. Therefore, the CableHome specification takes a brief look at the support needed for the MTA. Support for PacketCable, described in Section 11.6.4.4, consists of the CableHome Factory Default Ruleset, plus the needed protocols to enable PacketCable messaging to traverse the firewall. Appendix IV also notes which ports must be opened for the MTA. Support for PacketCable enables provisioning, management, and services through the firewall.

11.6.4.3.1 Firewall Policy and Address Realms

The concept of IP addressing realms are defined in this specification for WAN and LAN IP addresses. Although the PS is considered part of the LAN, packets originating from or destined to the PS are not referred to as LAN traffic for the purpose of firewall filtering. Instead, the specific PS IP address is called out. Packets originating from or destined to the PS are indicated by the use of the WAN-Man IP address, PS server router IP address, or to the fixed 192.168.0.1 IP address (which can be, but not necessarily, the same as the PS server router IP address). Accordingly, the firewall will distinguish traffic to and from the PS in the CableHome Factory Default Ruleset and Configured Ruleset. Firewall behavior is independent of

[103] Revised the first sentence in this paragraph per ECN CH1.1-N-03069 by GO on 10/28/03.

EXHIBIT A

Addressing Realms defined in Section 4. Firewall rules are not effected by Primary Packet Handling Mode or WAN Address Modes.

11.6.4.3.2 General Firewall Behavior for CableHome

The firewall in the PS is required to filter traffic based on the specified General Behavior Rules. These rules are specified to provide a baseline level of filtering behavior by the firewall in the PS. The General Behavior applies unless an exception is defined in the Default or Configured Ruleset. The states defined for the General Behavior Rules are either to allow or deny traffic. With the General Behavior Rules in place, the cable operator can expect the PS to always behave in a standardized way with regard to filtering traffic. The PS MUST apply the General Behavior Rules for firewall filtering as specified in <<cross reference to CableHome Firewall General Behavior Rules Table>> to a packet unless the firewall is configured to use another rule written into the Factory Default Ruleset (cabhSec2FwFactoryDefaultFilterTable [CH1]) or the Configured Ruleset (docsDevFilterIpTable).

Table 11-18 — CableHome Firewall General Behavior Rules

Source IP Address	Destination IP Address	General Behavior Rule
Any WAN IP Address	PS WAN-Man IP Address	Deny All
	PS WAN-Data IP Address	Deny All
	PS Server Router IP Address OR 192.168.0.1	Deny All
	Any LAN IP Address (passthrough mode)	Deny All
PS WAN-Man OR WAN-Data IP Address	Any WAN IP Address	Allow All
	Any LAN IP Address	Deny All
PS Server Router IP Address OR 192.168.0.1	Any WAN IP Address	Deny All
	Any LAN IP Address	Allow All
Any LAN IP Address	PS Server Router IP Address OR 192.168.0.1	Allow All
	PS WAN-Man OR WAN-Data IP Address	Deny All
	Any WAN IP Address	Allow All

11.6.4.3.3 CableHome Factory Default Ruleset

The CableHome Factory Default Ruleset defines a set of filtering rules to be applied when the Default Ruleset option of the cabhSec2FwPolicySelection object is selected. The CableHome Factory Default Ruleset MUST be hard-coded into the PS at the time of manufacture. The PS MUST use the CableHome Factory Default Ruleset when the cabhSec2FwPolicySelection object is set to factoryDefault(1), or factoryDefaultAndConfiguredRuleset (3).

Table 11-19 specifies the CableHome Factory Default Ruleset. Both LAN address realms, LAN-Trans and the LAN-Pass, are treated the same for the CableHome Factory Default Ruleset and are labeled LAN IP Address. The firewall MUST be able to look up addresses in the CAT mapping table to apply policy based on the real Host device IP Address. The table bases information on session initiation, not on allowed traffic. The CableHome Firewall Factory Default Ruleset MUST be implemented for session initiation and not for traffic returning in response to an allowed session. Traffic returning at the request of the initiator is understood as state information for a session and the firewall will check the session state after checking the policies to ensure a packet is not denied that is part of a current session.

EXHIBIT A

Table 11-19 – CableHome Firewall Factory Default Policy

Source IP Address	Destination IP Address	General Behavior	Exception Filtering Protocol List (Rule Number)
Any WAN IP Address	PS WAN-Man IP Address	Deny All	Allow ICMP (1) Allow SNMP (2,3)
	PS WAN-Data IP Address	Deny All	Allow ICMP (15)
	PS Server Router IP Address OR 192.168.0.1	Deny All	None
	Any LAN IP Address (passthrough mode)	Deny All	Allow ICMP (4)
PS WAN-Man OR WAN-Data IP Address	Any WAN IP Address	Allow All	None
	Any LAN IP Address	Deny All	Allow ICMP (5,16)
PS Server Router IP Address OR 192.168.0.1	Any WAN IP Address	Deny All	None
	Any LAN IP Address	Allow All	None
Any LAN IP Address	PS Server Router IP Address OR 192.168.0.1	Allow All	None
	PS WAN-Man OR WAN-Data IP Address	Deny All	Allow ICMP (6,17)
	Any WAN IP Address	Allow All	Deny Kerberos (7 - 12) Deny Syslog (13,14)

The CableHome Firewall Factory Default Ruleset listed in Table 11-20 MUST be implemented in the cabhSec2FwFactoryDefaultFilterTable MIB object. The column headers correspond to the defined MIB objects in the CableHome Security MIB but since the object names are rather long, only the varying part of the object name is used in the table below. The rules that include the PS WAN-Data IP address are listed starting with Table Index 15, since the cable operator can optionally provision one or more WAN-Data IP addresses in the PS. This table will be correctly populated at the time the PS completes provisioning dependent upon how the cable operator has configured the IP addresses.

EXHIBIT A

Table 11-20 – CableHome Firewall Factory Default Ruleset

Table Index	Control	IfIndex	Direction	Saddr	Smask	Daddr	Dmask	Protocol	SourcePortLow	SourcePortHigh	DestPortLow	DestPortHigh	Continue
1	Allow	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Man	(255.255.255.255)	1	0	65535	0	65535	true
2	Allow	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Man	(255.255.255.255)	6	0	65535	161	161	true
3	Allow	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Man	(255.255.255.255)	17	0	65535	161	161	true
4	Allow	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	LAN IP (0.0.0.0) [104]	(0.0.0.0)	1	0	65535	0	65535	true
5	Allow	255	2	PS WAN-Man	(255.255.255.255)	LAN IP (0.0.0.0)	(0.0.0.0)	1	0	65535	0	65535	true
6	Allow	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Man	(255.255.255.255)	1	0	65535	0	65535	true
7	Deny	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	6	0	65535	88	88	true
8	Deny	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	17	0	65535	88	88	true
9	Deny	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	6	0	65535	749	749	true
10	Deny	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	17	0	65535	749	749	true
11	Deny	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	6	0	65535	1293	1293	true
12	Deny	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	17	0	65535	1293	1293	true
13	Deny	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	6	0	65535	514	514	true
14	Deny	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	17	0	65535	514	514	true
15	Allow	2[105]	1	WAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Data	(255.255.255.255)	1	0	65535	0	65535	true
16	Allow	255	2	PS WAN-Data	(255.255.255.255)	LAN IP (0.0.0.0)	(0.0.0.0)	1	0	65535	0	65535	true
17	Allow	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Data	(255.255.255.255)	1	0	65535	0	65535	true

The cable operator can configure the PS with any firewall ruleset via configuration file or SNMP Set. When a cable operator sends rules to the PS, these rules are known as the Configured Ruleset. The PS MUST store the Configured Rules in the docsDevFilterIpTable [RFC 2669] and any scheduling information for particular rules in the MIB objects defined by CableHome in the cabhSec2FwFilterScheduleTable [CH1]. The Configured Ruleset is only active for firewall filtering if the

[104] Revised this cell per ECN CH1.1-N-04.0123-2 by KB on 4/5/04.

[105] Revised this cell per ECN CH1.1-N-04.0123-2 by KB on 4/5/04.

EXHIBIT A

firewall is enabled, and the policy selection is set to configuredRuleset(2) or factoryDefaultAndConfiguredRuleset(3). The Configured Ruleset can be cleared from the docsDevFilterIpTable by setting the value of cabhSec2FwClearPreviousRuleset to true(1).

11.6.4.4 PacketCable Support

If the cable operator deploys PacketCable, the CableHome firewall may need to pass traffic to and from the MTA, depending upon network and device configuration. The CableHome firewall will not break protocols defined in the PacketCable specifications if the cable operator correctly configures the CableHome firewall. The cable operator may need to configure the firewall for any additional rules to ensure that PacketCable will be enabled through the firewall. The following Table 11-21, is a list of specifications which have unique port requirements for communication with the MTA. However, it is not a comprehensive list of all the PacketCable specifications.

Table 11-21 – Relevant PacketCable 1.x Specifications for CableHome Firewall

Description	Specification
Audio/Video Codecs Specification	[PKT-CODEC]
Dynamic Quality of Service Specification	[PKT-DQOS]
Network-Based Call Signaling Protocol Specification	[PKT-MGCP]
MTA Device Provisioning Specification	[PKT-PROV]
Security Specification	[PKT-SEC]
Management Event Mechanism Specification	[PKT-MEM]
Audio Server Protocol Specification	[PKT-ASP]
Call Management Server Signaling Specification	[PKT-CMSS]

The list of the required PacketCable protocols to the MTA have been taken from the indicated specifications. The IANA assigned port numbers to open the ports needed by the PacketCable specified protocols through the firewall are listed in Appendix IV, Applications Through CAT and the Firewall. The PacketCable 1.x defined protocols include the following:

- Provisioning SNMPv3, DHCP, DNS, TFTP, SYSLOG
- Media Stream RTP, RTCP
- QoS RSVP
- Security Kerberos, IPSec
- Network Call Signaling MGCP, SDP (Note: SDP does not require any specific port.)

11.6.4.5 Firewall Filtering

This section specifies requirements for the CableHome firewall's packet filtering component. The specified packet filter examines individual packets and determines whether to allow or deny their passage across the firewall. More specifically, the packet filter inspects packet header fields and makes per-packet decisions based upon the contents of those fields and configured ruleset.

11.6.4.5.1 Minimum Set of Filtering Capability

For the purpose of CableHome, a simple NAT or packet filter is not sufficient. In order to provide a flexible and secure solution the firewall MUST implement an Application Specific Proxy (ASP) or a Stateful Packet Filtering (SPF) firewall. Additionally, specific requirements for these filtering techniques are needed in order to provide a sufficient level of testable, reliable, and interoperable products for the cable industry. The CableHome firewall's ASP/SPF component controls traffic flows associated with application-layer protocols that cannot be effectively and transparently controlled through static filtering.

EXHIBIT A

The filtering mechanisms will examine applications that are dynamically established over IP, TCP, UDP, or ICMP sessions. Port, IP address, and scheduling activity is managed as related to a "session" within the firewall. Also, the application specific proxy allows the operation of NAT-unfriendly applications when the Portal Service is operating in either of its two transparent routing modes: C-NAT or C-NAPT.

Regardless of the type of firewall that is implemented, the PS firewall MUST be session aware and able to track information on an IP address pair (source and destination) in conjunction with the current policy for the specified IP address. A session consists of a pairing of IP addresses on a per request basis. This request includes matching the request with the allowed policy for that session which consists of IP address, application port and curfew.

The firewall's packet filter architecture specifies separate inbound (WAN-to-LAN) and outbound (LAN-to-WAN) packet filters and PS. The inbound packet filter examines packets coming into the PS WAN interface. The outbound packet filter examines packets coming into the PS LAN interface. Separate rules can be applied to inbound and outbound packet filters. Packets destined to the PS from the WAN or LAN are filtered at the firewall prior to forwarding to any of the PS non-firewall components (CAP, CDP, CNP, CSP, CQP, and CPM).

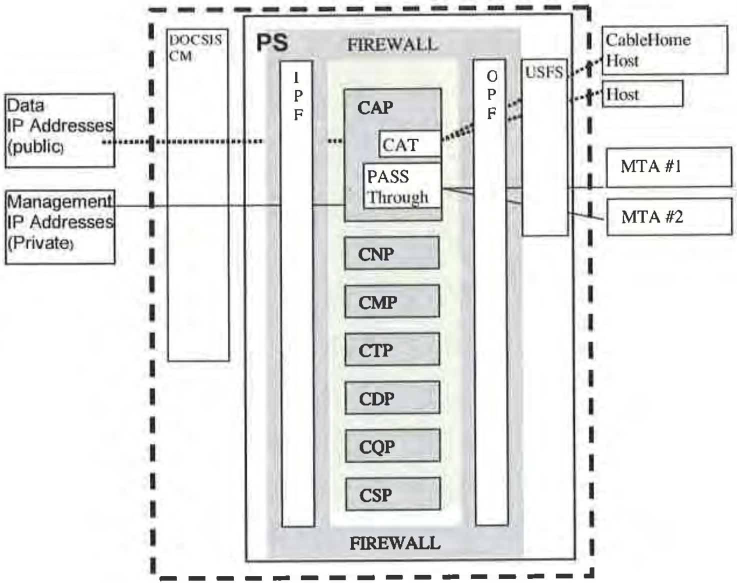


Figure 11-4 – Firewall Functionality inside the PS

CableHome uses the following filtering definitions:

- ALLOW means "let the packet through".
- DENY means to "drop the packet".
- NAT/NAPT (CH CAT) packets will be translated from the LAN, while packets returning from the WAN to the LAN will be recognized as such and will undergo reverse NAT/NAPT. The firewall filters will be applied in conjunction with the correct source or destination address on the LAN.

EXHIBIT A

The CableHome firewall's inbound and outbound packet filters MUST exhibit the following behavior:

- The firewall MUST filter traffic based on the CableHome defined policy as listed in Section 11.6.4.3 Firewall Policy, in cases where there is not an explicit rule to follow when checking a packet.
- The firewall MUST deny replayed packets from either the LAN or the WAN.
- The firewall MUST create a "state" for all allowed packets initiating a session. A packet will either be accepted because there is a static rule to allow packets of that criteria, or there is a state that implies that the packet will be allowed through as a result of an ongoing allowed session.
- The firewall SHOULD NOT allow TCP outbound traffic prior to establishing a TCP session (i.e., prior to completing a 3-way TCP handshake).[106]
- Packets with one of the following IP Options: LSRR (Loose-Source-Route), SSRR (Strict-Source-Route), RR (Record-Route) MUST be denied.

There are many types of network attacks that the firewall can filter. Many methods and tools are used to attack various devices on a network. The list is very long and changes faster then any current published document can claim. The CableHome specification calls out some the well known attacks for general security consideration. The firewall SHOULD protect against port or network scanning launched from LAN or WAN. The firewall SHOULD protect against floods of packets and malformed packets. The firewall SHOULD protect against the following list of denial of service attacks: "Ping of Death", "Teardrop", "Bonk", "Nestea", "SYN Flood", "LAND Attack", "IP Spoofing", "Smurf Attack", "WinNuke", and any high-frequency messaging originated by LAN IP Devices, such as BP_Init or DHCP DISCOVER messages.

11.6.4.5.2 Filter Criteria

The default is to deny traffic initiated from WAN IP addresses, the PS WAN-Man IP address, or the PS Server Router IP address. Therefore, the rulesets are built to allow particular traffic for these addresses. The default is to allow traffic from LAN IP addresses unless explicitly set to deny, therefore, the rulesets are built to deny particular traffic to these addresses. This section does not specify all the expected filtering capabilities, but lists a minimum set of criteria which is expanded by specified MIB objects. Inbound and outbound packet filters MUST examine traffic to see if a rule will allow the traffic based on the following filtering criteria:

- IP source address
- IP destination address
- IP ("next level") protocol; e.g., TCP, UDP, ICMP, IPsec AH, IPsec ESP
- TCP or UDP source and destination ports
- Start-of-connection information for TCP packets (i.e., absence of ACK bit) for session tracking
- Sequence number tracking for sessions

The above packet data is used as criteria for matching incoming packets to a specific rule, and hence, arriving at a specific filtering decision (allow/deny). The firewall MUST check the IP source and destination address to see if any rule applies to that address. If the ruleset currently prohibits forwarding traffic to or from an IP address, the firewall MUST deny the packet, unless it needs to be passed due to state.

Note: Filtering against the current policy include more requirements for filtering that must be applied, however, are not considered a part of the built-in filtering criteria.

[106] Revised this bullet per ECN CH1.1-N-04.0123-2 by KB on 4/5/04.

EXHIBIT A

11.6.4.5.3 Filtering Architecture

The CableHome firewall packet filter MUST be able to filter traffic as it enters the PS, with the exception of using the USFS function from the LAN, and provide distinct inbound (WAN-to-LAN), outbound (LAN-to-WAN), and PS packet filters. This firewall MUST have the following attributes:

- filter packets received from the PS WAN interface, e.g. IfIndex = 1, (this is referred to as inbound filtering)
- packets received from the PS LAN interface, e.g. IfIndex = 255, (this is referred to as outbound filtering)
- filter packets originating from within the PS going either to the LAN or WAN
- apply filters only as currently enabled
- inbound and outbound packet filtering precedes the delivery of packets to any of the PS's non-firewall components, except the USFS for packets coming from the LAN
- outbound packet filtering precedes any ASP/SPF processing

The WAN inbound packet filter MUST exhibit the following behavior:

- Default deny; meaning the default behavior of the firewall on inbound packets, that do not have explicit filter rules to allow the packet, is to drop the packet.
- Deny all packets whose source address is in the LAN-Pass or LAN-Trans address realms received from the PS WAN interface, e.g. IfIndex = 1.
- Deny all packets with broadcast or multicast source addresses.

The LAN outbound packet filter MUST exhibit the following behavior:

- Default allow; meaning the default behavior of the firewall on outbound packets, that do not have explicit filter rules to deny the packet, is to allow the packet.
- Reject all packets with broadcast or multicast source addresses.

11.6.4.6 Firewall Event Reporting

The information coming out of the firewall is critical for routine management and monitoring, as well as providing the appropriate events for specified attacks. The events generated by the firewall can be used for intrusion detection, DOS attacks, and any failures or logs related to the firewall system. The analysis of the logs can be quite cumbersome if there are large amounts of data to sort through. Also, if there are too many events sent to the cable operator, it could tie up bandwidth, since there can be many firewalls sending events to the NMS located in the cable operator back office. The cable operator will need to decide which items they wish to turn on to monitor the firewall and how often they would like to receive events. Turning-on event reporting is separate from turning-on the ruleset for the firewall filtering criteria. When the firewall event enable MIB objects have been set to enable the firewall to track defined event types, the firewall will log and send specified event messages as defined in this section and Appendix II.

Each of the specified events can be turned on or off by the cable operator through setting a SNMP MIB object through a configuration file, or a SNMP set. It is recommended that SNMPv3 be used to secure SNMP messages containing firewall information.

11.6.4.6.1 Firewall Events

Firewall events allow a cable operator to remotely assess the level of hacker activity and modifications to the firewall on specific PS elements. Event generation is based on management changes to the ruleset, events detected by the firewall as enabled by the ruleset, or TFTP/HTTP events based on downloading. The TFTP/HTTP events for firewall download MUST be sent, as defined by Appendix II.

The firewall MUST be capable of logging the following types of events:

EXHIBIT A

TYPE 1: Type 1 MUST log all attempts from both LAN and WAN clients to traverse the firewall that violate the Security Policy when this type is turned on via the cabhSec2FwEventEnable MIB object. This logs all connection attempts that are dropped due to policy violation. An attack is defined as packets (meaning each packet is counted as an attack), that attempt to traverse the firewall and violate the current policy. If enabled, and the threshold is reached, the PS MUST immediately send event 80010201.

TYPE 2: Type 2 MUST log identified Denial of Service attack attempts when this type is turned on, via the cabhSec2FwEventEnable MIB object. A type 2 attack is defined as any attempt that is considered to be disrupting any service, like the flood of duplicate packets (meaning 10 packets are counted as one attempt), or malformed packets or unpermitted connection attempts from the same host, for a multiple number of times. If enabled, and the threshold is reached, the PS MUST immediately send event 80010202.[107]

TYPE 3: Type 3 MUST log all changes made to the cabhSec2FwPolicyFileURL or cabhSec2FwPolicyFileCurrentVersion or cabhSec2FwEnable MIB objects when this type is turned on, via the cabhSec2FwEventEnable MIB object. Tracking the changes to the firewall configuration provides valuable feedback to the cable operator for debugging purposes. If enabled and the threshold is reached, the PS MUST immediately send event 80010203.[108]

TYPE 4: Type 4 MUST log all failed attempts to modify cabhSec2FwPolicyFileURL and cabhSec2FwEnable MIB objects when this type is turned on, via the cabhSec2FwEventEnable MIB. If enabled and the threshold is reached, the PS MUST immediately send event 80010204.[109]

TYPE 5: Type 5 MUST log allowed inbound packets from the WAN when this type is turned on, via the cabhSec2FwEventEnable MIB object. This enables the cable operator to monitor traffic in a scenario where there are signs of detection intrusion or DOS attacks from the WAN side. If enabled and the threshold is reached, the PS MUST immediately send event 80010205.[110]

TYPE 6: Type 6 MUST log allowed outbound packets from the LAN when this type is turned on, via the cabhSec2FwEventEnable MIB object. This enables the cable operator to monitor traffic in a scenario where there are signs of attacks coming from a home LAN across the WAN. If enabled and the threshold is reached, the PS MUST immediately send event 80010206.[111]

The event types for CableHome are defined for monitoring purposes only. It is up to the individual cable operator to evaluate and execute any necessary response to issues detected and reported by the firewall.

11.6.4.6.2 Firewall Logs

The firewall log information MUST be recorded in the PS for each enabled log type, as specified in Section 11.6.4.6.1. The PS MUST log the specified information unless the cabhSec2FwEventThreshold is set to zero, or the cabhSec2FwEventEnable is set to disable, or the cabhSec2FwEventInterval is set to zero. If the log table is full, the PS MUST remove the oldest entry and add the new one. If the cabhSec2FwEventThreshold is not set to zero, the cabhSec2FwEventEnable is enabled, the cabhSec2FwEventInterval is not set to zero and the log is not full, the PS MUST continue to log events of the enabled type. Once the cabhSec2FwEventLogReset is set to 1 to clear the log, and the cabhSec2FwEventEnable is enabled, the cabhSec2FwEventCount MUST start counting from zero.[112]

[107] Revised this paragraph per ECN CH1.1-N-04.0123-2 by KB on 4/5/04.
[108] Revised this paragraph per ECN CH1.1-N-04.0123-2 by KB on 4/5/04.
[109] Revised this paragraph per ECN CH1.1-N-04.0123-2 by KB on 4/5/04.
[110] Revised this paragraph per ECN CH1.1-N-04.0123-2 by KB on 4/5/04.
[111] Revised this paragraph per ECN CH1.1-N-04.0123-2 by KB on 4/5/04.
[112] Revised this paragraph per ECN CH1.1-N-04.0123-2 by KB on 4/5/04.

EXHIBIT A

The PS, at a minimum, MUST support the logging of 40 entries in the Firewall Log Table (cabhSec2FwLogTable). If an event type is enabled, the PS MUST log information required by the event type at a minimum rate of 1 event per every 5 seconds, even while under attack. It is expected that the PS will not consume the majority of its computing resources on logging and when attacks occur, the PS SHOULD be able to pass traffic at a normal rate and otherwise function normally.[113]

Logging can pose different problems if not properly done. Logging all events and packets can make the log complex, lengthy, and difficult to understand. It is difficult to sort through a lot of information to look for one item in particular. If logging is limited to only a few types of events, it will not provide enough information to the cable operator to debug intrusions or detect attacks. Note that logs can be sniffed if they are not encrypted. A hacker can use log information to gain insight into the various services running on the PS or LAN Host devices.

CableHome requires a particular set of information to be logged for each type of event that is enabled. The log function MUST log packets of each type according to the rules for that type of event. The requirement for Date and Time assumes that the Date and Time will be as accurate as the last update of the PS clock during the provisioning sequence.

The cabhSec2FwLogTable for the event types 1, 2, 5, & 6 MUST record the following information for each occurrence unless otherwise specified:

- Event Number - MUST be recorded as defined in Appendix II, one time, at the start of the log
- Event Priority - MUST be recorded as defined in Appendix II, one time, at the start of the log
- Date and Time - when the event occurred:
    - MUST consist of the four-digit year, month, and day
    - MUST consist of the hour, minute, and second
- Protocol – the protocol indicated in the IP header field (1 = ICMP; 2= IGMP; 6 =TCP; 17= UDP)
- Source IP Address
- Destination IP Address
- Source Port (TCP and UDP)
- Destination Port (TCP and UDP)
- Message Type (ICMP) - [RFC 2474] defines ICMP and when the firewall blocks an ICMP packet the log MUST display a number indicating what type of ICMP message it was. 0 - Echo Reply, 3 - Destination Unreachable, 4 - Source Quench, 5 - Redirect, 8 - Echo Request, 9 - Router Advertisement, 10 - Router Solicitation, 11 - Time Exceeded, 12 - Parameter Problem, 13 - Timestamp Request, 14 - Timestamp Reply, 15 - Information Request, 16 - Information Reply, 17 - Address Mask Request, 18 - Address Mask Reply
- Replay Count - If the data being recorded is a replay attack, the firewall SHOULD NOT record each occurrence of the attack. However, the firewall SHOULD record the number of occurrences up to the threshold value set for the specific type

The cabhSec2FwLogTable for the event type 3 MUST record the following information for each occurrence unless otherwise specified:

- Event Number - MUST be recorded as defined in Appendix II, one time, at the start of the log
- Event Priority - MUST be recorded as defined in Appendix II, one time, at the start of the log
- Date and Time – when the event occurred:
    - MUST consist of the four-digit year, month, and day
    - MUST consist of the hour, minute, and second

[113] Revised this paragraph per ECN CH1.1-N-04.0123-2 by KB on 4/5/04.

EXHIBIT A

- Source IP Address
- MIB object changed

The cabhSec2FwLogTable for the event type 4 MUST record the following information for each occurrence unless otherwise specified:[114]

- Event Number - MUST be recorded as defined in Appendix II, one time, at the start of the log.
- Event Priority - MUST be recorded as defined in Appendix II, one time, at the start of the log
- Date and Time – when the event occurred:
    - MUST consist of the four-digit year, month, and day
    - MUST consist of the hour, minute, and second
- Source IP Address
- MIB object attempted to be changed

11.6.4.7 Applications Through the Firewall

As part of the minimum set of capabilities, the CableHome firewall MUST be capable of allowing specified applications, as defined by Appendix IV, to traverse the PS to reach its intended destination. The firewall applies the current ruleset to the policy to ensure the correct openings are created to support specific traffic between the LAN and WAN, as well as to and from the PS itself. The PS MUST NOT limit the number of sessions or connections to be supported simultaneously, unless otherwise specified in Appendix IV, Applications through the CAT and Firewall.

The firewall policy is applied to the traffic as it attempts to traverse the firewall. The packets are first processed in the firewall prior to being sent to the PS for further processing, or to the destination on the WAN or LAN. The policy is applied to source and destination IP addresses, ports, and time of day. Appendix IV lists the requirements and provides more detail.

11.6.4.8 Firewall MIB Objects

The firewall MIB objects consist of a three general groupings: 1) a set to manage the firewall configuration, 2) a set to monitor and log events, and 3) a set to manage the rulesets themselves. The requirements for the firewall MIB objects MUST be used in conjunction with the CableHome Security MIB document [CH1].

11.6.4.8.1 Firewall Ruleset Management MIB Objects

The following firewall management objects MUST be implemented in the PS:

> cabhSec2FwPolicyFileURL - contains the name of the policy rule set file and the IP address of the TFTP or HTTPS server containing the policy rule set file, in a TFTP or HTTPS URL format. A policy rule set file download is triggered when the value used to SET this MIB is different than the value in the cabhSec2FwPolicySuccessfulFileURL MIB. Refer to Section 7.4.4.2.3 Firewall Configuration File Trigger.
>
> If the download of the Firewall Configuration File is not successful, the PS MUST NOT update the cabhSec2FwPolicySuccessfulFileURL MIB with the same value as the cabhSec2FwPolicyFileURL MIB. In any case, the cabhSec2FwPolicyFileURL MIB object MUST contain the value SET by either the PS Configuration File or by a SNMP SET command. When the PS is reset, the cabhSec2FwPolicyFileURL MIB object MUST be populated with its default

[114] Revised following bulleted list per ECN CH1.1-N-04.0115-1 by KB on 4/5/04.

EXHIBIT A

value.[115]

CabhSec2FwPolicySuccessfulFileURL - contains the name of the policy rule set file and the IP address of the TFTP server that contained the policy rule set file, in a TFTP or HTTPS URL format, which was used to trigger the last successful download. If a successful download has not yet occurred, this MIB should have a Null value.[116]

cabhSec2FwPolicyFileHash - Defines the SHA-1 digest for the corresponding ruleset file.

cabhSec2FwPolicyFileOperStatus - Contains the operational status of the firewall configuration file download and it MUST contain the following three states:

- inProgress(1) - indicates that a firewall configuration file download is underway.
- complete(2) - indicates that the firewall configuration file has downloaded successfully.
- failed(3) - indicates that the last attempted download of the firewall configuration file failed.

cabhSec2FwPolicyFileCurrentVersion - A label set by the cable operator that can be used to track various versions of configured rulesets. Once the label is set, and it, along with the configured rules are changed, may not accurately reflect the version of configured rules running on the box. This object MUST contain the string "null", if it has never been configured.

cabhSec2FwEnable - Allows for activation and deactivation of firewall. If this object is set to disabled, the firewall MUST be completely turned off. If this object is set to enable, the firewall MUST be activated immediately without re-booting the PS.

cabhSec2FwClearPreviousRuleset - Allows the Operator to clear the filter rule entries in the docsDevFilterIpTable.

cabhSec2FwPolicySelection - Allows for selection of the filtering policy as defined by the following options:

- factoryDefault (1) indicates the firewall is using the factory default settings defined in Section 11.6.4.3.2. If the cabhSec2FwPolicySelection MIB object is set to factoryDefault (1), then the firewall filters against the Factory Default Ruleset in the cabhSec2FwFactoryDefaultFilterTable.
- configuredRuleset (2) indicates the firewall is using the Configured Ruleset. If the cabhSec2FwPolicySelection MIB object is set to configuredRuleset (2), then the firewall filters against the Configured Ruleset in the docsDevFilterIpTable.
- factoryDefaultAndConfiguredRuleset (3) indicates the firewall is using the Factory Default Ruleset and the Configured Ruleset. If the cabhSec2FwPolicySelection MIB object is set to factoryDefaultAndConfiguredRuleset(3) the PS MUST filter against the CableHome specified Factory Default Ruleset in the cabhSec2FwFactoryDefaultFilterTable and the Configured Ruleset in the docsDevFilterIpTable. In the case of conflicting rules between the two tables, the rule in the Configured Ruleset (docsDevFilterIpTable) is the rule that the PS MUST apply to the packet.

cabhSec2FwEventSetToFactory - Allows the operator to clear all the events currently set in the event table. The PS MUST immediately clear the cabhSec2FwEventControlTable if this object is set to true.

[115] Revised the two preceding paragraphs per ECN CH1.1-N-03035 by GO on 07/03/03.

[116] Added this statement per ECN CH1.1-N-03035 by GO on 07/03/03.

EXHIBIT A

cabhSec2FwEventLastSetToFactory - This object reports the last time the event table was cleared.[117]

11.6.4.8.2 MIB Objects for Firewall Events

The following firewall event objects MUST be implemented in the PS, as defined in the CableHome Security MIB and are included in the cabhSec2FwEventControlTable:

cabhSec2FwEventType - Assigns the event type for the table to track. Event types are defined in Section 11.6.4.6.1.

cabhSec2FwEventEnable - Enables or disables counting and logging of firewall events by type as assigned in cabhSec2FwEventType. Logging requirements are defined in the log data section of this document. This is an on/off switch only. If the enable value changes, the PS MUST immediately send the appropriate event (8001010x). If this value is enabled, the firewall MUST log occurrences in the cabhSec2FwLog. The firewall MUST NOT count, send events, or collect log data for attacks when cabhSec2FwEventEnable is disabled. Default = false

cabhSec2FwEventThreshold - Number of attacks to count before sending the appropriate event by type as assigned in cabhSec2FwEventType. If the value is set to zero, the firewall MUST NOT count, send events, or collect log data for this type. Default = 0

cabhSec2FwEventInterval - Indicates the time interval in hours to count and log occurrences of a firewall event type as assigned in cabhSec2FwEventType. This time interval applies as long as the cabhSec2FwEventThreshold object is not exceeded. If the cabhSec2FwEventInterval MIB object has a value of zero, there is no interval assigned and the PS MUST NOT count, send, or log events. Default = 0

cabhSec2FwEventCount - Indicates the current count of attacks, up to the cabhSec2FwEventThreshold value by type as assigned by cabhSec2FwEventType. The firewall MUST start counting attacks from zero each time the cabhSec2FwEventEnable MIB object is enabled, or the cabhSec2FwEventInterval is over, or the cabhSec2FwEventCount equals the cabhSec2FwEventThreshold value. If the number of attacks counted in the cabhSec2FwEventCount equals the threshold set in the cabhSec2FwEventThreshold, prior to the end of the time interval defined by the cabhSec2FwEventInterval object, the PS MUST immediately send the appropriate event (8001020x). Default = 0

cabhSec2FwEventLogReset - Setting this object to true clears the log table for the specified event type. Reading this object always returns false. Default = false

cabhSec2FwEventLogLastReset - This object reports the last time the log was cleared.

11.6.4.8.3 Firewall Policy MIB Objects

The CableHome firewall policy MIB objects provide a way for the cable operator to configure rules that will be used by the firewall to filter traffic. The cable operator can create any configured ruleset needed to filter traffic passing through the firewall on the PS. The firewall filtering policy MIB objects are based on the minimum set of filtering requirements. The firewall's filtering capability is similar to the filters defined in the cable industry CM MIB objects, specified in [RFC 2669]. Therefore, CableHome had adopted some of the filtering objects already defined in [RFC 2669], and add some CableHome firewall specific MIB objects within the CableHome Security MIB.

[117] Revised this statement per ECN CH1.1-N-03035 by GO on 07/03/03.

EXHIBIT A

Within [RFC 2669], the docsDevFilterIpTable provides the basic filtering properties. The docsDevFilterIpTable contains a sequence, docsDevFilterIpEntry, of MIB object. Each row in the table describes rules associated with IP addresses which is then compared to IP packets traversing the firewall. The template includes source and destination IP addresses (and their associated masks), upper level protocol (e.g. TCP, UDP), as well as the source and destination port ranges. This is the heart of the policy implementation. It is in this MIB table that the policy is defined and constructed. Each packet, inbound or outbound, shall be compared to the enabled policy

CableHome defines a docsDevFilterIPTable extension, cabhSec2FwFilterScheduleTable that provides filter attributes for start time, end time and day of week to the filter settings in the docsDevFilterIPTable entries . This table allows a rule or filter to be enforced via the day of week, (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday), during a start and end time. For example, a parent may request that communications be denied between the WAN and the child's computer for Monday through Friday, 9pm to 7am and on Saturday and Sunday, 10pm to 8am. Filter rule entries in the docsDevFilterIpTable MIB object MUST always be applied if their associated cabhSec2FwFilterScheduleTable MIB objects have the following values: cabhSec2FwFilterScheduleStartTime = 0, cabhSec2FwFilterScheduleEndTime = 2359, and cabhSec2FwFilterScheduleDOW = 0xFE.

The combination of filters defined in [RFC 2669], and in the CableHome Security MIB, allow for any rules to be created based on any combination of source IP address, destination IP address, source port, destination port, time of day, and day of week.

If there is not a match when the PS is comparing each inbound or outbound packet to the rules in the docsDevFilterIpTable, then the PS MUST apply the minimum set of firewall capabilities and architecture, as defined in sections 11.6.4.4.1 and 11.6.4.4.3. The docsDevFilterIpDefault flag defined in [RFC 2669] MUST be ignored for CableHome.[118]

The following MIB objects MUST be implemented from [RFC 2669] to create the FilterIpTable for the filtering rules of the firewall. Unless otherwise noted in this section, the functionality is as specified in [RFC 2669]:

- docsDevFilterIpTable >>DocsDevFilterIpEntry
  - docsDevFilterIpIndex
    - consistent with [RFC 2669], the filter with the lowest index is always applied, meaning the filter is checked, then the PS MUST continue checking filters and apply the filter with the highest index in the case of conflicts
  - docsDevFilterIpStatus
  - docsDevFilterIpControl
    - the PS MUST ignore the setting (3) for policy; CableHome does not use the policy table
  - docsDevFilterIpIfIndex
    - This object MUST use a default value of 255 (Aggregated LAN Interfaces)[119]
    - The index number assigned to this object MUST match to the ifIndex numbering assigned in the ifTable from the Interfaces Group MIB [RFC 2863], as specified in Table 6-16 Numbering Interfaces in the ifTable
  - docsDevFilterIpDirection
    - For CableHome, this value represents direction in relationship to the assigned docsDevFilterIpIfIndex in this particular rule, meaning that the PS MUST represent traffic direction (inbound, outbound, or both), relative to the indicated ifIndex. Vendor assigned ifIndex values MUST follow the same rule for application of direction. For example, CableHome assigns

[118] Replaced this paragraph per ECN CH1.1-N-03035 by GO on 07/03/03.

[119] Revised this bullet per ECN CH1.1-N-04.0123-2 by KB on 4/5/04.

EXHIBIT A

the number 255 to the aggregated LAN interface. In this case, the PS will see inbound traffic on ifIndex 255, as all traffic coming from the LAN going to or traversing through the PS and outbound traffic on ifIndex 255, as all traffic going to the LAN coming from or traversing through the PS.

- docsDevFilterIpBroadcast
  - it is expected that this will always be the default value of false. Therefore, the rule will apply to all traffic
- docsDevFilterIpSaddr
- docsDevFilterIpSmask
- docsDevFilterIpDaddr
- docsDevFilterIpDmask
- docsDevFilterIpProtocol
- docsDevFilterIpSourcePortLow
- docsDevFilterIpSourcePortHigh
- docsDevFilterIpDestPortLow
- docsDevFilterIpDestPortHigh
- docsDevFilterIpMatches
- docsDevFilterIpTos[120]
  - this object can be ignored; its function is not required for CableHome.
- docsDevFilterIpTosMask
  - this object can be ignored; its function is not required for CableHome.
- docsDevFilterIpContinue
  - this object MUST always be set to true so the PS will continue checking filters until all the filters have been checked. Unlike RFC2669, this object MUST NOT trigger a discard until all the filters have been checked and there are no later filters which requires the packet to be accepted.
- docsDevFilterIpPolicyId
  - this object can be ignored; its function is not required for CableHome.

Additionally, the firewall MUST support the following MIB objects as specified in the CableHome Security MIB document:

- cabhSec2FwFilterScheduleStartTime
- cabhSec2FwFilterScheduleEndTime
- cabhSec2FwFilterScheduleDOW

11.6.4.8.4 Firewall Factory Default Ruleset MIB Objects

The CableHome Firewall Factory Default Ruleset MIB objects provide a way for the cable operator to view the CableHome Factory Default Rules, which are exceptions to the general rules, or General Firewall Behavior defined in Table 11-18 and Table 11-19. For more information on the Default Ruleset MIB objects used for filtering, please refer to the CableHome Security MIB [CH1] for description of the cabhSec2FwFactoryDefaultFilterTable and its entries.

11.7 Additional Security MIB Objects in the PS

The CableHome firewall MIB objects are described in the firewall section of this document. This section describes the remaining security MIB objects required for CableHome. The security MIB objects are

[120] Revised the following four bullet statements per ECN CH1.1-N-03035 by GO on 07/03/03.

EXHIBIT A

defined in more detail and MUST be supported as defined in Appendix I of this specification, [draft-ietf-ipcdn-bpiplus-mib-05], CH-SP-MIB-SEC-I03-030411 [CH1] and CL-SP-MIB-CLABDEF-I03-030411 [CableLabs2].

11.7.1 Secure Software Download MIB Objects

Secure software download follows the design as created by DOCSIS, and as such, the MIB objects can be re-used in the PS just as the CM uses them. The PKI structure for CableHome is defined separately and therefore some of the certificate MIBs MUST be used as defined by CableHome, not by the DOCSIS MIBs, as currently written in [draft-ietf-ipcdn-bpiplus-mib-05].

The Standalone PS MUST support the following MIB objects as defined in the CL-SP-MIB-CLABDEF-I03-030411 [CableLabs2]:

- clabCVCRootCACert - CableLabs Code Verification Root CA used for CVC validation
- clabCVCCACert - CableLabs Code Verification CA used for CVC validation
- clabMfgCVCCert - Manufacturer Code Verification Certificate used to store the Mfg CVC Cert

The Standalone PS MUST support the following software download MIB objects defined in [draft-ietf-ipcdn-bpiplus-mib-05]:

- docsBpi2CodeDownloadGroup - Collection of objects that provide authenticated software download support. The docsBpi2CodeDownloadGroup includes:
- docsBpi2CodeDownloadStatusCode - Indicates the result of the latest configuration file CVC verification, SNMP CVC verification, or code file verification.
- docsBpi2CodeDownloadStatusString - Additional information to the status code.
- docsBpi2CodeMfgOrgName - The device manufacturer's organizationName.
- docsBpi2CodeMfgCodeAccessStart - The device manufacturer's current codeAccessStart value referenced to Greenwich Mean Time (GMT).
- docsBpi2CodeMfgCvcAccessStart - The device manufacturer's current cvcAccessStart value referenced to Greenwich Mean Time (GMT).
- docsBpi2CodeCoSignerOrgName - The Co-Signer's organizationName.
- docsBpi2CodeCoSignerCodeAccessStart - The co-signer's current codeAccessStart value referenced to Greenwich Mean Time (GMT).
- docsBpi2CodeCoSignerCvcAccessStart - The co-signer's current cvcAccessStart value referenced to Greenwich Mean Time (GMT).
- docsBpi2CodeCvcUpdate - Triggers the device to verify the CVC and update the cvcAccessStart value.

11.7.2 Security Configuration File MIB Objects

The PS MUST support the following configuration file download MIB object as defined in the CableHome Security MIB:

> cabhPsDevProvConfigHash - SHA-1 [FIPS 186] hash of the entire content of the configuration file, taken as a byte string.

11.7.3 Security Service Provider MIB Objects

The PS MUST support the following service provider authentication MIB object as defined in the CableHome Security MIB:

EXHIBIT A

clabSrvcPrvdrRootCACert - The CableLabs Service Provider Root CA used to validate certificates of devices on the service provider's network.

11.7.4 PS Certificate MIB Objects

The PS MUST support the following PS Certificate MIB object as defined in the CableHome Security MIB:

cabhSecCertPsCert - The X.509 DER-encoded PS certificate used to provide secure identity of the PS.

11.7.5 Kerberos MIB Objects

The needs of Kerberos within CableHome is a subset of the functionality required by PacketCable. The following MIB objects are required for CableHome and the PS MUST support these MIB objects, as defined in the CableHome Security MIB:

- cabhSecKerbPKINITGracePeriod - The number of minutes prior to current ticket expiration for the PS to initiate a request with the KDC for a new ticket.
- cabhSecKerbTGSGracePeriod - The number of minutes prior to current ticket expiration for the PS to initiate a request with the KDC for a new ticket.
- cabhSecKerbUnsolicitedKeyMaxTimeout -The maximum timeout value for the AP Req/Rep exchange.
- cabhSecKerbUnsolicitedKeyMaxRetries - The maximum number of retries the PS is allowed to attempt AP Req/Rep negotiation

11.8 Secure Software Download for the PS

11.8.1 Goals of Secure Software Download

Secure Software Download goals include the following:

- The cable operator can securely load code into the PS as needed.
- The cable operator can manage secure downloads with various configuration policies.
- The security of the download will provide integrity, authentication, and if possible, encryption.
- The PS will only download images appropriate for the device.

11.8.2 Secure Software Download Design Guidelines

Table 11-22 – CableHome Security System Design Guidelines

Reference	Security System Design Guidelines
SEC13	The cable operator will have the ability to securely download software images to the PS element.

11.8.3 Secure Software Download System Description

Secure software download ensures that only a software image can be downloaded to the PS if the image is created by the same manufacturer. It also ensures that the image has not been modified since the manufacturer signed the code image. The image can also be signed by CableLabs, as a co-signer, to guarantee that the image has been certified. For additional security on the download process, the cable operator can optionally sign any image as a co-signer to ensure that only images will be loaded into the PS that the cable operator has approved. The control mechanism for secure software download is to insert the

EXHIBIT A

code verification certificates (CVCs) into the configuration file which match the CVCs on the code image to be downloaded. After the PS has received CVC(s) in the configuration file, the PS is enabled to download the new code image when triggered via configuration file, or SNMP Set.

11.8.4 Secure Software Download Requirements

A Standalone PS Element MUST be capable of remotely downloading a software image over the network. As described in Section 6.3.3.2.4.9, secure software download to an Embedded PS is controlled by the cable modem. The new software image would allow the cable operator to improve performance, accommodate new functions and features, correct design deficiencies, and to allow a migration path for CableHome devices as the CableHome evolves. The CableHome software download capability MUST allow the functionality of the PS element to be changed without requiring that cable system personnel physically visit and reconfigure each unit. The Standalone PS secure software download process addresses the following primary system requirements:

- The CableHome mechanism used for software download MUST be TFTP file transfer.
- The CableHome software download MUST be initiated in one of two ways: 1) An SNMP set request issued by the NMS to the docsDevSwAdminStatus; 2) via the PS element's configuration file. If the Software Upgrade File Name in the configuration file does not match the current software image of the device, the PS element MUST request the specified file via TFTP from the Software Server.
- The PS element MUST verify that the downloaded software image is appropriate for itself. If the downloaded software image is appropriate, the PS element MUST write the new software image to non-volatile storage. Once the file transfer is completed successfully, the device MUST restart itself with the new code image.
- If the PS element is unable to complete the file transfer for any reason, the PS element MUST remain capable of accepting new software downloads (without operator or user interaction), even if power or connectivity is interrupted between attempts.
- The PS element MUST log software download failures and can report failures asynchronously to the network manager.
- Where software has been upgraded to meet a new version of the CableHome specification, then it is critical that the software MUST work with the previous version in order to allow a gradual transition of units on the network.
- The PS element MUST authenticate the downloaded software image.
- The PS element MUST verify that the downloaded code has not been altered from the original form in which it was provided by the trusted source.
- The software download process MUST provide a cable operator with mechanisms to upgrade or downgrade the code version of the CableHome elements.
- The software download process MUST provide options for a cable operator to dictate their own download policies.
- The code file manufacturer MUST apply a Code Verification Signature (CVS) over the code image and any other authenticated attributes as defined in this specification for the PKCS#7 structure digital signature to the code file; the private key used to apply the signature MUST be bound to a public key certificate that chains up to the CableLabs CVC root. The manufacturer's signature authenticates the source and integrity of the code file.
- A Co-Signer (cable operator or CableLabs) MAY counter sign the code file in addition to the manufacturer's signature.
- The PS element MUST be able to process a PKCS#7 digital signature and a CableHome [ITU-T X.509] certificate as defined in Section 11.8.4.1.1 and Section 11.3.4.1.1, respectively.
- (Optional): The PS element SHOULD be able to update the CableLabs CVC Root CA Certificate stored in the device.

EXHIBIT A

- (Optional): The PS element SHOULD be able to replace the Manufacturer CA Certificate(s) stored in the device.
- (Optional): The PS element SHOULD be able to update the CableLabs CVC CA Certificate stored in the device.
- (Optional): The PS element SHOULD be able to update the CableLabs Service Provider Root CA Certificate stored in the device.

The optional downloading of the CableLabs Service Provider Root CA Certificate, CableLabs CVC Root CA Certificate, CableLabs CVC CA Certificate, and/or the Manufacturer CA Certificate, as a part of the Code File, are clearly separated from the code image and the other parameters in the code download file. It is possible to change the CableLabs Service Provider Root CA Certificate, CableLabs CVC Root CA Certificate, CableLabs CVC CA Certificate, and/or the Manufacturer CA Certificate, understood by the PS element, by including the new certificates in the code image. Inclusion of the Manufacturer CVC Certificate and/or a co-signer CVC and corresponding CVS, permits the PS element to verify that the code image has not been altered since the CableLabs Service Provider Root CA Certificate, CableLabs CVC Root CA Certificate, CableLabs CVC CA Certificate, and/or the Manufacturer CA Certificate, or SignedData parameters, are appended to the code image.

A CableHome Complaint Residential Gateway device MAY include a DOCSIS cable modem and the CableHome PS Element, as separate entities or embedded as defined in the architecture section of this document.

- If the PS Element is embedded with a DOCSIS cable modem, the PS/CM image MUST be a single image, and the software download MUST be performed only by the DOCSIS cable modem as described in [SCTE1] for a DOCSIS 1.0 CM, and in [DOCSIS9] for a DOCSIS 1.1 CM, and in [DOCSIS5] for a DOCSIS 2.0 CM.
- If the PS Element is composed of separate standalone entities, the software download for the CableHome elements MUST be performed by the PS Element, as described below in this specification.

11.8.4.1 Code Download File Structure for Secure Software Download

For secure software download, the code download file is a file built using a [PKCS #7] compliant structure that has been defined in a specific format for use with PS Elements. The code file MUST comply with [PKCS #7] and MUST be DER encoded. The code file MUST match the structure shown in Table 11-23.

When certificates are downloaded as a part of the Code File, the certificates MAY be contained in the fields as specified in Table 11-23, and separated from the actual code image contained in the CodeImage field.

Table 11-23 – Code File Structure

Code File	Description
PKCS#7 Digital Signature {	
ContentInfo	
ContentType	SignedData
SignedData ()	EXPLICT signed-data content value: includes CVS and [ITU-T X.509] compliant CVSs
} end [PKCS #7] Digital Signature	
SignedContent {	
Download Parameters {	Mandatory TLV format (Type 28). (Length is zero if there is no sub-TLVs).
MfgCACerts ()	Optional TLV for one or more DER-encoded certificate(s) each formatted according to the Manufacturer CA-Certificate TLV format (Type 17).

EXHIBIT A

Code File	Description
clabServProvRootCACert ()	Optional TLV for one DER-encoded certificate formatted according to the CableLabs Service Provider Root CA-Certificate TLV Format (Type 50).
clabCVCRootCACert ()	Optional TLV for one DER-encoded certificate formatted according to the CableLabs CVC Root CA Certificate TLV Format (Type 51).
clabCVCCACertificate ()	Optional TLV for one DER-encoded certificate formatted according to the CableLabs CVC CA-Certificate TLV Format (Type 52).
}	
CodeImage ()	Upgrade code image.
} end SignedContent	

11.8.4.1.1 Signed Data

The code download file will contain the information in a [PKCS #7] Signed Data content type as shown in Table 11.8.4.1.2. Though maintaining compliance to [PKCS #7], the structure used has been restricted in format to ease the processing performed by the PS to validate the signature. The [PKCS #7] Signed Data MUST be DER encoded and exactly match the structure shown below, except for any change in order required to DER encode (e.g., the ordering of SET OF attributes). The PS element SHOULD reject the [PKCS #7] signature if the [PKCS #7] Signed Data does not match the DER encoded structure.

Table 11-24 – PKCS#7 Signed Data[121]

PKCS#7 Field	Description
SignedData {	
version	1
digestAlgorithms	SHA-1
contentInfo	
contentType	data (SignedContent is concatenated at the end of the PKCS#7 structure)
certificates {	
mfgCVC	(REQUIRED for all code files) [Note 1]
co-signerCVC	(OPTIONAL; required for co-signatures) [Note 2]
} end certificates	
signerInfos {	
MfgSignerInfo {	(REQUIRED for all code files)
version	1
issuerAndSerialNumber	
issuer	
countryName	US
organizationName	CableLabs
commonName	CableLabs CVC CA
serialNumber	<Mfg CVC serial number>
digestAlgorithm	SHA-1
authenticatedAttributes	
contentType	data (contentType of signedContent)
signingTime	UTCTime (GMT), YYMMDDhhmmssZ
messageDigest	(digest on the content together with the signer's authenticated attributes as defined in [PKCS#7])
digestEncryptionAlgorithm	rsaEncryption
encryptedDigest	
} end mfg signer info	
CoSignerInfo {	(OPTIONAL; required for co-signatures)
version	1

[121] Revised Table 11-24 and notes per ECN CH1.1-N-03078 by GO on 11/7/03.

EXHIBIT A

PKCS#7 Field	Description
issuerAndSerialNumber	
issuer	
countryName	US
organizationName	CableLabs
commonName	CableLabs CVC CA
serialNumber	<Co-signer CVC serial number>
digestAlgorithm	SHA-1
authenticatedAttributes	
contentType	data (contentType of signedContent)
signingTime	UTCTime (GMT), YYMMDDhhmmssZ
messageDigest	(digest on the content together with the signer's authenticated attributes as defined in [PKCS#7])
digestEncryptionAlgorithm	rsaEncryption
encryptedDigest	
} end co-signer info	
} end signer infos	
} end signed data	

1. Manufacturer CVC MUST comply the format specified in Table 11-9;
2. Co-signer CVC MUST comply the format specified in Table 11-10 or Table 11-11 depending on the type of co-signer, which can be CableLabs or Service Provider correspondingly.

11.8.4.1.2 Signed Content

The signed content field of the code file contains the code image and the download parameters field, which possibly contains the following additional optional items:

- CableLabs Service Provider Root CA Certificate
- CableLabs (CL) CVC Root CA Certificate
- CL CVC CA Certificate
- Manufacturer CA Certificate

The final code image is in a format compatible with the destination PS element. In support of the [PKCS #7] signature requirements, the code content is typed as data; i.e., a simple octet string. The format of the final code image is not specified here and will be defined by each manufacturer according to their requirements.

Each manufacturer SHOULD build their code with additional mechanisms that verify an upgrade code image is compatible with the destination PS element.

If included in the signed content field, a certificate is intended to replace the certificate currently stored in the PS element. If the code download and installation is successful, the PS element MUST replace its currently stored certificate with the new certificate received in the signed content field. This new certificate will be used for subsequent verification.

11.8.4.1.3 Code Signing Keys

The [PKCS #7] digital signature uses the RSA Encryption Algorithm [PKCS #1] with SHA-1 [FIPS 186]. The PS element MUST be able to verify code file signatures. The public exponent is F_4 (65537 decimal).

11.8.4.1.4 Manufacturer CA Certificate

This Attribute is a string attribute containing an X.509 CA Certificate, as defined in [ITU-T X.509].

Type Length Value

EXHIBIT A

17	Variable	X.509 CA Certificate (DER-encoded ASN.1)

11.8.4.1.5 CableLabs Service Provider Root CA Certificate

This Attribute is a string attribute containing an X.509 CableLabs Service Provider Root CA Certificate, as defined in [ITU-T X.509]. This certificate must be used by the PS Element in SNMP provisioning mode for mutual authentication.

Type	Length	Value
50	Variable	X.509 CA Certificate (DER-encoded ASN.1)

11.8.4.1.6 CableLabs CVC Root CA Certificate

This Attribute is a string attribute containing an X.509 CableLabs CVC Root CA Certificate, as defined in [ITU-T X.509]. This certificate must be used by the standalone PS Element in the secure software downloading process.

Type	Length	Value
51	Variable	X.509 CA Certificate (DER-encoded ASN.1)

11.8.4.1.7 CableLabs CVC CA Certificate

This Attribute is a string attribute containing an X.509 CableLabs CVC CA Certificate, as defined in [ITU-T X.509]. This certificate must be used by the standalone PS Element in the secure software downloading process.

Type	Length	Value
52	Variable	X.509 CA Certificate (DER-encoded ASN.1)

11.8.4.2 CVC Format for Secure Software Download[122]

For secure software download, the format used for the CVC is [ITU-T X.509] compliant. However, the X.509 structure has been restricted to ease the processing a PS element does to validate the certificate and extract the public key used to verify the CVS. The CVC MUST be DER encoded comply with Table 11-9, Table 11-10 and Table 11-11 depending on type of CVC. The PS element SHOULD reject the CVC if it does not match with the corresponding Table.

11.8.4.2.1 Certificate Revocation

This specification does not require or define the use of certificate revocation lists (CRLs). The PS element is not required to support CRLs. MSOs can define and use CRLs to help manage code files provided to them by manufacturers. However, there is a method for revoking certificates based on the validity start date of the certificate. This method requires that an updated CVC be delivered to the PS element with an updated validity start time. Once the CVC is successfully validated, the X.509 validity start time will update the PS element's current value of cvcAccessStart.

11.8.4.3 Code File Access Controls

For secure software download, special control values are included in the code file for the PS element to check before it will validate a code image. The conditions placed on the values of these control parameters MUST be satisfied before the PS element will validate the CVC or the CVS, and accepts the code image.

[122] Revised this section per ECN CH1.1-N-03078 by GO on 11/7/03.

EXHIBIT A

11.8.4.3.1 Subject Organization Names

The PS element will recognize up to two names, at any one time, that it considers a trusted code-signing agent in the subject field of a code file CVC:

- The CableHome device manufacturer: The manufacturer name in the manufacturer's CVC subject field MUST exactly match the manufacturer name stored in the PS element's non-volatile memory by the manufacturer. A manufacturer CVC MUST always be included in the code file.
- A co-signing agent: It is permitted that another trusted organization co-sign code files destined to the CableHome device. In most cases, this is the cable operator controlling the current operating domain of the device. The organization name of the co-signer is communicated to the PS element via a co-signer's CVC in the configuration file when initializing the PS element's code verification process. The co-signer's organization name in the co-signer's CVC subject field MUST exactly match the co-signer's organization name previously received in the co-signer's initialization CVC and stored by the PS element.

The PS element MAY compare organization names using a binary comparison.

11.8.4.3.2 Time Varying Controls

To mitigate the possibility of a PS element receiving a previous code file via a replay attack, the code files include a signing-time value in the PKCS#7 structure that can be used to indicate the time the code image was signed. The PS element MUST keep two UTC time values associated with each code-signing agent. One set MUST always be stored and maintained for the CableHome device's manufacturer. Additionally, if the code file is co-signed, the PS element MUST also store and maintain a separate set of time values for the co-signer.

These values are used to control code file access to the PS element by individually controlling the validity of the CVS and the CVC:

- codeAccessStart: a 12-byte UTC time value referenced to Greenwich Mean Time (GMT).
- cvcAccessStart: a 12-byte UTC time value referenced to GMT.

UTCTime values in the CVC MUST be expressed as GMT and MUST include seconds. That is, they MUST be expressed in the following form: YYMMDDhhmmssZ. The year field (YY) MUST be interpreted as follows:

- Where YY is greater than or equal to 50, the year shall be interpreted as 19YY.
- Where YY is less than 50, the year shall be interpreted as 20YY.

These values will always be referenced to Greenwich Mean Time, so the final ASCII character (Z) can be removed when stored by the PS element as codeAccessStart and cvcAccessStart.

The PS element MUST maintain each of these time values in a format that contains equivalent time information and accuracy to the 12 character UTC format (i.e., YYMMDDhhmmss). The PS element MUST accurately compare these stored values with UTC time values delivered to the PS element in a CVC. These requirements are discussed later in this specification.

The values of codeAccessStart and cvcAccessStart corresponding to the PS Element's manufacturer MUST NOT decrease. The value of codeAccessStart and cvcAccessStart, corresponding to the co-signer, MUST NOT decrease as long as the co-signer does not change and the PS element maintains that co-signer's time-varying control values.

EXHIBIT A

11.8.4.4 Code Upgrade Initialization

11.8.4.4.1 Manufacturer Initialization

It is the responsibility of the manufacturer to correctly install the initial code version in the PS Element.

In support of secure software download, values for the Manufacturer's time-varying controls MUST be loaded into the PS Element's non-volatile memory:

- PS Element manufacturer's organizationName
- Manufacturer's time-varying control values:
  - codeAccessStart initialization value
  - cvcAccessStart initialization value

The organization name of the PS Element manufacturer MUST always be present in the device. The PS Element manufacturer's organizationName MAY be stored in the device's code image. The manufacturer name used for code upgrade is not necessarily the same name used in the Manufacturer CA certificate.[123]

The time-varying control values, codeAccessStart, and cvcAccessStart, MUST be initialized to a UTCTime compatible with the validity start time of the manufacturer's latest CVC. These time-varying values will be updated periodically under normal operation via manufacturer's CVCs that are received and verified by the PS element.[124]

The Manufacturer MUST initialize the following certificates into the Standalone PS Element's non-volatile memory:

- CableLabs Service Provider Root CA Certificate
- CableLabs CVC Root CA Certificate
- CableLabs CVC CA Certificate
- Manufacturer CA Certificate
- PS Element Certificate

The Manufacturer MUST initialize the following certificates into the Embedded PS Element's non-volatile memory:

- CableLabs Service Provider Root CA Certificate
- Manufacturer CA Certificate
- PS Element Certificate

11.8.4.4.2 Network Initialization

In support of code verification, the PS configuration file is used as an authenticated means in which to initialize the code verification process. In the PS element configuration file, the PS element receives configuration settings relevant to code upgrade verification.

The configuration file SHOULD always include the most up-to-date CVC applicable for the destination PS element. When the configuration file is used to initiate a code upgrade, it MUST include a Code Verification Certificate (CVC) to initialize the PS element for accepting code files according to this specification. Regardless of whether a code upgrade is required, a CVC in the configuration file MUST be processed by the PS element. A configuration file MAY contain:

- No CVC - The PS element MUST NOT accept a code file.

[123] Revised this paragraph per ECN CH1.1-N-03078 by GO on 11/7/03.
[124] Revised this paragraph per ECN CH1.1-N-03078 by GO on 11/7/03.

EXHIBIT A

- A Manufacturer's CVC only - The PS element MUST verify that the manufacturer's CVC chains up to the CableLabs CVC Root before accepting a code file. When the PS element's configuration file only contains a valid Manufacturer's CVC, the device will only require a manufacturer signature on the code files. In this case, the PS element MUST NOT accept code files that have been co-signed.
- A Co-Signer's (cable operator or CableLabs) CVC only - The PS element MUST verify the Co-Signer CV chains up to the CableLabs CVC Root before accepting a code file. When the PS element's configuration file contains a valid co-signer's CVC, it is used to initialize the device with a co- signer. Once validated, the name of the CVC's subject organizationName will become the code co-signer assigned to the PS element. In order for a PS element to subsequently accept a code image, the co-signer, in addition to the CableHome device manufacturer, MUST have signed the code file.
- Both a Manufacturer's CVC and a Co-Signer's CVC - The PS element MUST verify that both CVCs chain up to the CableLabs CVC Root before accepting a code file.

Before the PS element will enable its ability to upgrade code files on the network, it MUST receive a valid CVC in a configuration file. In addition, when the PS element's configuration file does not contain a valid CVC, which means that its ability to upgrade code files has been disabled, the PS element MUST reject any information in a CVC subsequently delivered via docsBpi2CodeCvcUpdate SNMP MIB object.[125]

The organization name of the PS Element manufacturer and the manufacturer's time-varying control values MUST always be present in the PS element. If the PS element is initialized to accept code co-signed by an additional code-signer, the name of the organization and their corresponding time-varying control values MUST be stored and maintained while operational. Space MUST be allocated in the PS element's memory for the following co-signer's control values:

- co-signing agent's organizationName
- co-signer's time-varying control values:
  - cvcAccessStart
  - codeAccessStart

The manufacturer's set of these values MUST be stored in the PS element's non-volatile memory and not lost when the CableHome device's main power source is removed or during a reboot.

When a co-signer is assigned to the PS element, the co-signer's set of CVC values MUST be stored in the PS element's memory. The PS element MAY retain these values in non-volatile memory that will not be lost when the CableHome device's main power source is removed or during a reboot. However, when assigning a PS element a co-signer, the CVC is always in the configuration file. Therefore, the PS element will always receive the co-signer's control values during the initialization phase and is not required to store the co-signer's time- varying control values when main power is lost or during a reboot process.

11.8.4.4.3 CVC Processing

To expedite the delivery of an updated CVC without requiring the PS to process a code upgrade, the CVC MAY be delivered in the configuration file or an SNMP Set message. The format of the CVC is the same whether it is in a code file, configuration file, or SNMP message.

11.8.4.4.3.1 Processing the Configuration File CVC[126]

When a CVC is included in the configuration file, the PS element MUST verify the CVC before accepting any of the code upgrade settings it contains. At receipt of the CVC in the configuration file, the PS element MUST perform the following validation and procedural steps. If any of the following verification checks fail, the PS element MUST immediately halt the CVC verification process and log the error if applicable. If the PS Configuration File does not include a CVC that validates properly, the PS element MUST NOT

[125] Revised this paragraph per ECN CH1.1-N-03078 by GO on 11/7/03.

[126] Revised this paragraph and the first numbered bullet per ECN CH1.1-N-03078 by GO on 11/7/03.

EXHIBIT A

download upgrade code files whether triggered by the PS Configuration File or via docsDevSwAdminStatus SNMP MIB object. In addition, if the PS Configuration File does not include a CVC that validates properly (manufacturer or co-signer CVC), the PS element is not required to process CVCs subsequently delivered via docsBpi2CodeCvcUpdate SNMP MIB object, and MUST NOT accept information from these CVCs (i.e. the PS element MUST ignore any SNMP Set requests made to docsBpi2CodeCvcUpdate SNMP MIB object).

At receipt of the CVC in a configuration file, the PS element MUST:

1. Verify that the CVC complies with the structure and values as required in Section 11.3.4.2.

2. Check the CVC subject organization name:

    a) If the CVC is a Manufacturer's CVC (Type 32) then:

        1. If, the organizationName is identical to the CableHome device's manufacturer name, then this is the manufacturer's CVC. In this case, the PS element MUST verify that the manufacturer's CVC validity start time is greater-than or equal-to the manufacturer's cvcAccessStart value currently held in the PS element.

        2. If, the organizationName is not identical to the CableHome device's manufacturer name, then this CVC MUST be rejected and the error logged.

    b) If the CVC is a Co-signer's CVC (Type 33) then:

        1. If, the organizationName is identical to the PS element's current code co-signer, then this is the current co-signer's CVC, and the PS element MUST verify that the validity start time is greater-than or equal-to the co-signer's cvcAccessStart value currently held in the PS element.

        2. If, the organizationName is not identical to the current code co-signer name, then after the CVC has been validated (and registration is complete), this subject organization name will become the PS element's new code co-signer. The PS element MUST NOT accept a code file unless it has been signed by the manufacturer, and co-signed by this code co-signer.

3. Validate the CVC issuer signature using the CL CVC CA Public Key held by the PS element.

4. Validate the CL CVC CA signature using the CL CVC Root CA Public Key held by the PS element. Verification of the signature will authenticate the source and validate trust in the CVC parameters.

5. Update the PS element's current value of cvcAccessStart corresponding to the CVC's subject organizationName (i.e., manufacturer or co-signer) with the validity start time value from the validated CVC. If the validity start time value is greater than the PS element's current value of codeAccessStart, update the PS element's codeAccessStart value with the validity start time value. The PS element SHOULD discard any remnants of the co-signer CVC.

11.8.4.4.3.2 Processing the SNMP CVC

The PS element MUST process SNMP delivered CVC's when enabled to upgrade code files. Otherwise, all CVC's delivered via SNMP MUST be rejected. When validating the CVC delivered via SNMP, the PS element MUST perform the following validation and procedural steps:

Note: If any of the following verification checks fail, the PS element MUST immediately halt the CVC verification process, log the error if applicable, and remove all remnants of the process to that step.

EXHIBIT A

The PS element MUST:

1. Verify that the CVC complies with the structure and values as required in Section 11.3.4.2.[127]
2. Check the CVC subject organization name:

    a) If, the organizationName is identical to the CableHome device's manufacturer name, then this is the manufacturer's CVC. In this case, the PS element MUST verify that the manufacturer's CVC validity start time is greater-than the manufacturer's cvcAccessStart value currently held in the PS element.

    b) If, the organizationName is identical to the PS element's current code co-signer, then this is a current co-signer's CVC and the validity start time MUST be greater-than the co-signer's cvcAccessStart value currently held in the PS element.

    c) If, the organizationName is not identical to CableHome device's manufacturer or current co-signer's name, then the PS element MUST immediately reject this CVC.

3. Validate the CVC issuer signature using the CL CVC CA Public Key held by the PS element.
4. Validate the CVC issuer signature using the CL CVC Root CA Public Key held by the PS element. Verification of the signature will authenticate the certificate and confirm trust in the CVC's validity start time.
5. Update the current value of the subject's cvcAccessStart values with the validated CVC's validity start time value. If the validity start time value is greater than the PS element's current value of codeAccessStart, update the PS element's codeAccessStart value with the validity start value.

11.8.4.5 Code Signing Requirements

11.8.4.5.1 Certificate Authority (CA) Requirements

Code Verification Certificates (CVCs) are signed and issued by the CableLabs (CL) CVC CA. The CVC MUST be exactly as specified in Table 11-9, Table 11-10 and Table 11-11 depending on type of CVC. The CL CVC CA MUST NOT sign any CVC unless it is identical to the format specified in Table 11-9, Table 11-10 or Table 11-11. Before signing a CVC, the CL CVC CA MUST verify that the certificate request is authentic.[128]

The CL CVC CA will be responsible for registering names of authorized CVC subscribers. CVC Subscribers include PS Element manufacturers and cable operator's that will co-sign code images. It is the responsibility of the CL CVC CA to guarantee that the organization name of every CVC Subscriber is different. The following guidelines MUST be enforced when assigning organization names for code file co-signers:

- The organization name used to identify itself as a code co-signer agent in a CVC MUST be assigned by CableLabs.
- The name MUST be a printable string of eight hexadecimal digits that uniquely distinguishes a code-signing agent from all others.
- Each hexadecimal digit in the name MUST be chosen from the character set 0-9 (0x30-0x39) or A- F (0x41-0x46).
- The string consisting of eight 0-digits is not allowed and MUST NOT be used in a CVC.

[127] Revised this sentence per ECN CH1.1-N-03078 by GO on 11/7/03.

[128] Revised this paragraph per ECN CH1.1-N-03078 by GO on 11/7/03.

EXHIBIT A

In any alternate format, all the information MUST be maintained and the original format MUST be reproduced; e.g., as a 32-bit nonzero integer, with an integer value of 0 representing the absence of a code-signer.

11.8.4.5.2 Manufacturer CVC Requirements

To sign their code files, the manufacturer MUST obtain a valid CVC from the CL CVC CA. All manufacturer code images provided to a cable operator for remote upgrade of a CableHome device MUST be signed according to the requirements defined in this specification. When signing a code file, a manufacturer MAY choose not to update the [PKCS #7] signingTime value in the manufacturer's signing information. This specification requires that the [PKCS #7] signingTime value be equal-to or greater-than the CVC's validity start time. If the manufacturer uses a signingTime equal to the CVC's validity start time when signing a series of code files, those code files can be used and re-used. This allows a cable operator to use the code file to upgrade or downgrade the code version for that manufacturer's CableHome devices. These code files will be valid until a new CVC is generated and received by the PS element.

11.8.4.5.3 Cable Operator Requirements

When a cable operator receives software upgrade code files from a manufacturer, the cable operator will validate the code image using the CL CVC CA Public Key. This will allow the cable operator to verify that the code image is as built by the trusted manufacturer. The cable operator can re-verify the code file at any time by repeating the process.

If a cable operator wants to exercise the option of co-signing the code image destined for a CableHome device on their network, the cable operator MUST obtain a valid CVC from the CL CVC CA.

When signing a code file, the cable operator MUST co-sign the file content according to the PKCS#7 signature standard, and include their cable operator CVC, as defined in Section 11.8.4.1.1. CableHome does not require a cable operator to co-sign code files. However, when the cable operator follows all the rules defined in this specification for preparing a code file, the PS element MUST accept it.

11.8.4.6 Triggering Process

Code downloads, regardless of the provisioning mode, can be initiated during the provisioning and registration process via a configuration-file-initiated download, or, during normal operation, using an SNMP-initiated download command. The PS element MUST support both methods.

Note: Prior to triggering a secure software download, appropriate CVC information MUST be included in the configuration file. If the operator decides to use the SNMP-initiated download as a method to trigger a secure software download. It is recommended that CVC information always be present in the configuration file so that a PS element will always have the CVC information initialized when needed. If the operator decides to use the configuration-file-initiated download as a method to trigger secure software download, CVC information is needed to be present in the configuration file at the time the CableHome device is rebooted to get the configuration file that will trigger the upgrade.

11.8.4.6.1 SNMP-initiated Software Download

From a network management station:

- Set docsDevSwServer to the address of the TFTP server for software upgrades
- Set docsDevSwFilename to the file pathname of the software upgrade image
- Set docsDevSwAdminStatus to Upgrade-from-mgt. docsDevSwAdminStatus MUST persist across reset/reboots until over-written from an SNMP manager, or via the PS element configuration file.

EXHIBIT A

The default state of docsDevSwAdminStatus MUST be allowProvisioningUpgrade{2} until it is overwritten by ignoreProvisioningUpgrade{3}, following a successful SNMP-initiated software upgrade, or otherwise altered by the management station. docsDevSwOperStatus MUST persist across resets to report the outcome of the last software upgrade attempt.

If a PS element suffers a loss of power or resets during SNMP-initiated upgrade, the PS element MUST resume the upgrade without requiring manual intervention, and when the PS element resumes the upgrade process:

- docsDevSwAdminStatus MUST be Upgrade-from-mgt{1}
- docsDevSwFilename MUST be the filename of the software image to be upgraded
- docsDevSwServer MUST be the address of the TFTP server containing the software upgrade image to be upgraded
- docsDevSwOperStatus MUST be inProgress{1}
- docsDevSwCurrentVers MUST be the current version of software that is operating on the CableHome device

In case the PS element reaches the maximum number of retries (max retries = 3) resulting from multiple losses of power or resets during an SNMP-initiated upgrade, the PS element's status MUST adhere to the following requirements after it is registered:

- docsDevSwAdminStatus MUST be allowProvisioningUpgrade{2}
- docsDevSwFilename MUST be the filename of the software that failed the upgrade process.
- docsDevSwServer MUST be the address of the TFTP server containing the software that failed the upgrade process
- docsDevSwOperStatus MUST be other{5}
- docsDevSwCurrentVer MUST be the current version of software that is operating on the CableHome device

If a PS element exhausts the required number of TFTP retries by issuing a total of 16 consecutive retries, the PS element MUST fall back to the last known working image, proceed to an operational state, and adhere to the following requirements:

- docsDevSwAdminStatus MUST be allowProvisioningUpgrade{2}
- docsDevSwFilename MUST be the filename of the software that failed the upgrade process
- docsDevSwServer MUST be the address of the TFTP server containing the software that failed the upgrade process
- docsDevSwOperStatus MUST be failed{4}
- docsDevSwCurrentVer MUST be the current version of software that is operating on the CableHome device

After the PS element has completed the SNMP-initiated secure software upgrade, the PS element MUST reboot and become operational with the correct software image. When the device is operational, it MUST adhere to the following requirements:

- set its docsDevSwAdminStatus to ignoreProvisioningUpgrade{3}
- set its docsDevOperStatus to completeFromMgt{3}
- reboot

The PS element MUST properly use ignoreProvisioningUpgrade status to ignore the software upgrade value that can be included in the PS element configuration file. The PS MUST become operational with the correct software image and it MUST adhere to the following requirements:

- docsDevSwAdminStatus MUST be ignoreProvisioningUpgrade{3}

EXHIBIT A

- docsDevSwFilename MAY be the filename of the software currently operating on the PS element
- docsDevSwServer MAY be the address of the TFTP server containing the software that is currently operating on the PS element
- docsDevSwOperStatus MUST be completeFromMgt{3}
- docsDevSwCurrentVer MUST be the current version of the software that is operating on the PS element

In the case where PS element successfully downloads (or detects during download), an image that is not intended for the CableHome device the:

- DocsDevSwAdminStatus MUST be allowProvisioningUpgrade{2}
- DocsDevSwFilename MUST be the filename of the software that failed the upgrade
- DocsDevSwServer MUST be the address of the TFTP server containing the software that failed the upgrade process
- DocsDevSwOperStatus MUST be other{5}
- DocsDevSwCurrentVer MUST be the current version of software that is operating on the CableHome device

In the case where PS element determines that the download image is damaged or corrupted, the PS element MUST reject the newly downloaded image. The PS element MAY re-attempt to download if the MAX number of TFTP sequence retries has not been reached. If the PS element chooses not to retry and the MAX number of TFTP sequence retries has not been reached, the PS element MUST fall back to the last known working image and proceed to an operational state, generate an appropriate event notification, as specified in Section 11.8.4.8, and adhere to the following requirements:

- DocsDevSwAdminStatus MUST be allowProvisioningUpgrade{2}
- DocsDevSwFilename MUST be the filename of the software that failed the upgrade
- DocsDevSwServer MUST be the address of the TFTP server containing the software that failed the upgrade process
- DocsDevSwOperStatus MUST be other{5}
- DocsDevSwCurrentVer MUST be the current version of software that is operating on the CableHome device

In the case where PS element determines that the image is damaged or corrupted, the PS element MUST reject the newly downloaded image. The PS element MAY re-attempt to download the new image if the MAX number of TFTP sequence retries has not been reached. On the 16th consecutive failed software download attempt, the PS element MUST fall back to the last known working image and proceed to an operational state. In this case, the PS element is required to send two notifications; one to notify that the MAX TFTP retry limit has been reached, and another to notify that the image is damaged. Immediately after the PS element reaches the operational state, the PS element MUST adhere to the following requirements:

- DocsDevSwAdminStatus MUST be allowProvisioningUpgrade{2}
- DocsDevSwFilename MUST be the filename of the software that failed the upgrade
- DocsDevSwServer MUST be the address of the TFTP server containing the software that failed the upgrade process
- DocsDevSwOperStatus MUST be other{5}
- DocsDevSwCurrentVer MUST be the current version of software that is operating on the CableHome device

EXHIBIT A

11.8.4.6.2 Configuration-file-initiated Software Download

The configuration-file-initiated software download is initiated in a standalone PS by including the Software Upgrade File Name parameter (TLV-9) AND the Software Upgrade TFTP Server parameter (TLV-21) in its PS Configuration File. An embedded PS MUST ignore TLV-9 and TLV-21 if they are present in its PS Configuration File, since the software upgrade of an embedded PS is controlled by the cable modem. If the Software Upgrade File Name parameter (TLV-9) with a valid value AND the Software Upgrade TFTP Server parameter (TLV-21) with a valid value are present in the standalone PS element's PS Configuration File, AND if the value of the Software Upgrade File Name parameter does not match the current software image file name, i.e., the value of docsDevSwFilename, the PS element MUST request the specified file, via TFTP, from the server whose address was provided in the Software Upgrade TFTP Server parameter.[129]

If a standalone PS receives a PS Configuration File in which both the Software Upgrade File Name parameter (TLV-9) and a TLV-28 setting the docsDevSwFilename object are present, AND the values of TLV-9 and docsDevSwFilename are different, the PS MUST reject the PS Configuration File, report Event ID 73040102 (Invalid TLV Format/contents), preserve all object values that existed before the attempt to process this bad configuration file, and reset.

Note: The Software Server IP Address is a separate parameter. If present, the PS element MUST attempt to download the specified file from this server. If not present, the PS element MUST attempt to download the specified file from the configuration file server.

In a case where the PS element reaches the maximum number of retries (max retries = 3) resulting from multiple loss of powers, or resets during a configuration-file-initiated upgrade, the PS element's status MUST adhere to the following requirements, after it is registered:

- docsDevSwAdminStatus MUST be allowProvisioningUpgrade{2}
- docsDevSwFilename MUST be the filename of the software that failed the upgrade process
- docsDevSwServer MUST be the address of the TFTP server containing the software that failed the upgrade process
- docsDevSwOperStatus MUST be other{5}
- docsDevSwCurrentVer MUST be the current version of software that is operating on the CableHome device

If a PS element exhausts the required number of TFTP retries by issuing a total of 16 consecutive retries, the PS element MUST fall back to the last known working image, proceed to an operational state, and adhere to the following requirements:

- docsDevSwAdminStatus MUST be allowProvisioningUpgrade{2}
- docsDevSwFilename MUST be the filename of the software that failed the upgrade process
- docsDevSwServer MUST be the address of the TFTP server containing the software that failed the upgrade process
- docsDevSwOperStatus MUST be failed{4}
- docsDevSwCurrentVer MUST be the current version of software that is operating on the CableHome device

After the PS element has completed the configuration-file-initiated secure software upgrade, the PS element MUST reboot and become operational with the correct software image. After the PS element is registered the:

- docsDevSwAdminStatus MUST be allowProvisioningUpgrade{2}

[129] Revised this paragraph and added the following paragraph per ECN CH1.1-N-03.0099-3 by GO on 12/10/03.

EXHIBIT A

- docsDevSwFilename MAY be the filename of the software currently operating on the CableHome device
- docsDevSwServer MAY be the address of the TFTP server containing the software that is currently operating on the CableHome device
- docsDevSwOperStatus MUST be completeFromProvisioning{2}
- docsDevSwCurrentVer MUST be the current version of the software that is operating on the CableHome device

11.8.4.7 Code Verification

For secure software download, the PS element MUST perform the verification checks presented in this section. If any of the verification checks fail, or if any portion of the code file is rejected due to invalid formatting, the PS element MUST immediately halt the download process, log the error if applicable, remove all remnants of the process to that step, and continue to operate with its existing code.

The following verification checks can be made in any order, as long as all of the applicable checks presented in this section are made:

1. The PS element MUST validate the manufacturer's signature information by verifying that the [PKCS #7] signingTime value is:

   a) equal-to or greater-than the manufacturer's codeAccessStart value currently held in the PS element.

   b) equal-to or greater-than the manufacturer's CVC validity start time.

   c) less-than or equal-to the manufacturer's CVC validity end time.

2. The PS element MUST validate the manufacturer's CVC by verifying that the:[130]

   a) CVC is exactly the same as it is specified in Table 11-9.

   b) CVC subject organizationName is identical to the manufacturer name currently stored in the PS element's memory.

   b) CVC validity start time is equal-to or greater-than the manufacturer's cvcAccessStart value currently held in the PS element.

3. The PS element MUST validate the certificate signature using the CL CVC CA Public Key held by the PS element. In turn, the CL CVC CA Certificate signature is validated by the CL CVC Root CA Public Key held by the PS element. Verification of the signature will authenticate the source of the public code verification key (CVK) and confirm trust in the key.

4. The PS element MUST verify the manufacturer's code file signature:

   a) The PS element MUST perform a new SHA-1 hash over the SignedContent. If the value of the messageDigest doesn't match the new hash, the PS element MUST consider the signature on the code file as invalid.

   b) If the signature does not verify, all components of the code file (including the code image), and any values derived from the verification process, MUST be rejected and SHOULD be

[130] Revised the following alpha-bullets per ECN CH1.1-N-03078 by GO on 11/7/03.

EXHIBIT A

immediately discarded.

5. If the manufacturer signature verifies, and a co-signing agent signature is required:

    a) The PS element MUST validate the co-signer's signature information by verifying that the:

    (1) co-signer's signature information is included in the code file.

    (2) [PKCS #7] signingTime value is equal-to or greater-than the corresponding codeAccessStart value currently held in the PS element.

    (3) [PKCS #7] signingTime value is equal-to or greater-than the corresponding CVC validity start time.

    (4) [PKCS #7] signingTime value is less-than or equal-to the corresponding CVC validity end time.

    b) The PS element MUST validate the co-signer's CVC, by verifying that the:[131]

    (1) CVC subject organizationName is identical to the co-signer's organization name currently stored in the PS element's memory.

    (2) CVC is exactly the same as it is specified in Table 11-10 or Table 11-11 depending on the type of co-signer (CableLabs or Service Provider).

    (3) CVC validity start time is equal-to or greater-than the cvcAccessStart value currently held in the PS element for the corresponding subject organizationName.

    c) The PS element MUST validate the certificate signature using the CL CVC CA Public Key held by the PS element. In turn, the CL CVC CA certificate signature is validated by the CL CVC Root CA Public Key held by the PS element. Verification of the signature will authenticate the source of the co-signer's public code verification key (CVK) and confirm trust in the key.

    d) The PS element MUST verify the co-signer's code file signature.

    e) The PS element MUST perform a new SHA-1 hash, over the SignedContent. If the value of the messageDigest doesn't match the new hash, the PS element MUST consider the signature on the code file as invalid.

    f) If the signature does not verify, all components of the code file (including the code image), and any values derived from the verification process, MUST be rejected and SHOULD be immediately discarded.

6. If the manufacturer's, and optionally, the co-signer's signature has verified, the code image can be trusted and installation can proceed. Before installing the code image, all other components of the code file and any values derived from the verification process, except the [PKCS #7] signingTime values and the CVC validity start values, SHOULD be immediately discarded.

7. If the code installation is unsuccessful, the PS element MUST reject the [PKCS #7] signingTime values and CVC validity start values it just received in the code file.

8. When the code installation is successful, the PS element MUST update the manufacturer's time-varying

[131] Revised the following number-bullets per ECN CH1.1-N-03078 by GO on 11/7/03.

EXHIBIT A

controls with the values from the manufacturer's signature information and CVC:

a) Update the current value of codeAccessStart with the [PKCS #7] signingTime value

b) Update the current value cvcAccessStart with the CVC validity start value

9. When the code installation is successful, and if the code file was co-signed, the PS element MUST update the co- signer's time-varying controls with the values from the co-signer's signature information and CVC:

a) Update the current value of codeAccessStart with the [PKCS #7] signingTime value

b) Update the current value of cvcAccessStart with the CVC validity start value

11.8.4.8 Error Codes

Error codes are defined to reflect the failure states possible during the secure software download code verification process.

1. Improper code file controls:

a) CVC subject organizationName for manufacturer does not match the PS element's manufacturer name.

b) CVC subject organizationName for code co-signing agent does not match the PS element's current code co-signing agent.

c) The manufacturer's [PKCS #7] signingTime value is less-than the codeAccessStart value currently held in the PS element.

d) The manufacturer's [PKCS #7] validity start time value is less-than the cvcAccessStart value currently held in the PS element.

e) The manufacturer's CVC validity start time is less-than the cvcAccessStart value currently held in the PS element.

f) The manufacturer's [PKCS #7] signingTime value is less-than the CVC validity start time.

g) Missing or improper extended key-usage extension in the manufacturer CVC

h) The co-signer's [PKCS #7] signingTime value is less-than the codeAccessStart value currently held in the PS element.

i) The co-signer's [PKCS #7] validity start time value is less-than the cvcAccessStart value currently held in the PS element.

j) The co-signer's CVC validity start time is less-than the cvcAccessStart value currently held in the PS element.

k) The co-signer's [PKCS #7] signingTime value is less-than the CVC validity start time.

l) Missing or improper extended key-usage extension in the co-signer's CVC.

EXHIBIT A

2. Code file manufacturer CVC validation failure.
3. Code file manufacturer CVS validation failure.
4. Code file co-signer CVC validation failure.
5. Code file co-signer CVS validation failure.
6. Improper Configuration File CVC format (e.g., Missing or improper key usage attribute)
7. Configuration File CVC validation failure.
8. Improper SNMP CVC format:

   a) CVC subject organizationName for manufacturer does not match the CableHome device's manufacturer name.

   b) CVC subject organizationName for code co-signing agent does not match the PS element's current code co-signing agent.

   c) The CVC validity start time is less-than or equal-to the corresponding subject's cvcAccessStart value currently held in the PS element.

   d) Missing or improper key usage attribute.

9. SNMP CVC validation failure.

11.8.4.9 Software Downgrade

The Software Downgrade defines the process of removing the upgraded version of the software image download, thus reverting the Cable Home Device to the exact previous state.

When the PS element receives a code file with a signing-time that is later than the signing-time it has in its memory, the device MUST update its internal memory with the received value.

Because the PS element will not accept code files with an earlier signing-time than this internally stored value, to upgrade a CableHome device with a new code file without denying access to past code files, the signer (e.g., the Manufacturer, the cable operator, CableLabs) can choose not to update the signing-time. In this manner, multiple code files with the same code signing-time allows an operator to freely downgrade a CableHome device's code image to a past version (that is, until the CVC is updated). This has a number of advantages for the cable operator, but these advantages will be weighed against the possibilities of a code file replay attack.

Another approach would be to sign the previous code file with a signing-time that is equal to or greater than the signing-time of the last upgrade.

11.9 PS Configuration File Security in DHCP Provisioning Mode

11.9.1 Configuration File Security Infrastructure Goals

The goals for securing the configuration file include:

EXHIBIT A

- Provide an authenticated tunnel between the PS client device and HTTPS server to ensure that configuration files are secured from the cable operator to the PS. An integrity check is automatically included when a message is authenticated.
- Encryption of configuration files while in transport to reduce the possibility of eavesdropping on firewall and PS configuration.
- Reduce the risk of an unauthorized configuration file download to the PS by an unauthorized source.

11.9.2 Configuration File Security System Design Guidelines

Table 11-25 – Security System Design Guidelines

Reference	Security System Design Guidelines
Sec14	The cable operator will have the ability to authenticate and optionally encrypt the transport of configuration files for the PS or firewall.

11.9.3 Configuration File Security System Description

In DHCP provisioning mode, the cable operator can choose to turn on security for the configuration file download. Within this section, the term configuration file refers to the PS configuration file, or the firewall configuration file. Security is provided by establishing a TLS session between the PS and the HTTPS server. CableHome requires the PS to understand this security option and to use TLS within the provisioning sequence to provide a secure session between the HTTPS Server and the PS, for the purposes of downloading the PS configuration file, and the firewall configuration file, in a secure manner. TLS provides authentication and encryption for the session, as configured by the cable operator. The session is torn down prior to sending the CableHome Syslog and/or NMS notification provisioning completed message. The configuration file download trigger, management, and contents remain as industry standards when TLS is layered under the HTTPS protocol. CableHome specifies the requirements for an [RFC 2246] complaint TLS session. The TLS options are tightened to create a minimum set of interoperable behavior for the PS. The provisioning flow with HTTP/TLS is described in detail in Section 13.

TLS provides an encrypted and authenticated transport tunnel for any application above TLS in the ISO stack. The HTTP protocol itself is not affected by the TLS layering. The italicized and underlined layers in the stack are encrypted for a standard TLS data packet. The HTTP protocol, which normally sits on TCP, sits directly on TLS.

Table 11-26 – TLS Encryption

Configuration File Data (Payload)
HTTP
TLS
TCP
IP
MAC
PHY

11.9.4 Configuration File Security Requirements

The PS MUST implement the Transport Layer Security (TLS) protocol as defined by [RFC 2246], TLS Protocol Version 1.0, with the exceptions as listed in this specification. The exceptions within this specification are intended to simplify the requirements necessary for implementation and testing purposes. Some of the exceptions place a minimum set requirements that already align with other technology used

EXHIBIT A

within the cable industry. The requirements placed will ensure the PS shall provide a consistent level of performance for the cable operators. This section also helps remove any ambiguity and define processes which are not defined in the RFCs, but is needed for CableHome purposes. This is especially true in the case of failure handling.

Note: The compression algorithm feature of TLS will not be used.

TLS version 1.0 (SSL3, TLSv1) MUST be supported. Earlier versions of TLS MUST NOT be supported by the PS. The PS MUST reject messages from the server if it attempts to use previous TLS versions.

11.9.4.1 Triggering TLS

To trigger a secure configuration file download in DHCP provisioning mode, the DHCP Ack will contain the IP address of the HTTPS server in the siaddr field. The DHCP Ack will also contain option 72 with the IP address of the HTTPS server. If the IP address in the siaddr field and the first IP address in option 72 match, the PS MUST establish a TLS session with the HTTPS server at the IP address listed in the ack, prior to requesting the configuration file. The PS MUST download the configuration file using HTTP/TLS, if the first IP address in TLV option 72 matches that IP address in siaddr, of the DHCP Ack message. If the PS does not receive a match in the DHCP ack, the PS MUST NOT initiate a TLS session, the requirements in this section are not applicable, and the PS client MUST use DHCP provisioning mode with the specified TFTP download process. The provisioning flow diagram and description table are specified in Section 13. If option 66 is included as well as option 72, and the IP address in option 72 matches the IP address in the siaddr field, the PS MUST initiate a TLS session to the HTTPS server and MUST NOT initiate download from the TFTP server listed in option 66.

If the PS receives the necessary information to initiate firewall configuration file download via HTTPS, as specified in Section 7, then the PS will need to determine if it needs to continue or set-up a TLS session with an HTTPS server.[132]

11.9.4.2 TLS Session Prerequisites

Prior to establishing a TLS session, the PS client MUST synchronize its clock with the TOD server. Details are specified in Section 13.

Additionally, the PS client MUST establish the TCP/IP connection to the HTTPS server prior to sending the TLS ClientHello. Once the configuration file download is complete, the PS MUST close the TCP/IP connection. The PS client MUST use TCP port #443, specified by IANA standards, to connect to the HTTP/TLS server. If the TCP/IP connection cannot be made after 5 attempts, with 30 seconds allowed for each attempt, the PS MUST send event 68002000.

11.9.4.3 TLS Messages[133]

Unless otherwise noted, all the messages are [RFC 2246] compliant.

11.9.4.3.1 ClientHello

The PS client MUST send a ClientHello to the HTTP/TLS server to initiate the TLS Handshake sequence. After the initial ClientHello message has been sent to the HTTP/TLS server, if the TLS session is not established after 5 attempts, with 30 seconds allowed for each attempt, the PS MUST fail the session and send event 68002100.

[132] Revised this paragraph per ECN CH1.1-N-03.0074-3 by GO on 12/5/03.
[133] Deleted section referring to ClientCertificate per ECN CH1.1-N-03.0074-3 by GO on 12/5/03.

EXHIBIT A

11.9.4.3.2 PS Processing of the Server Messages

The PS MUST be able to process the server messages, as defined in [RFC 2246], with the following exceptions:

- HelloRequest: The PS MUST ignore HelloRequest messages from a server. This protects the PS from answering rogue requests from HTTPS servers. The HTTP/TLS process can only be initiated if the appropriate DHCP options are configured by the cable operator. This assumes DHCP is trusted, even though it is not secured by CableHome.
- ServerCertificate: The HTTPS server is expected to send its device certificate to the PS within the ServerCertificate message. In addition to the [RFC 2246] requirements for this message, the PS client MUST validate and verify the HTTPS server certificate. If the HTTPS server certificate authentication fails, the TLS session is considered a failure and the PS MUST send event 68002200 with the [RFC 2246] defined error code.

11.9.4.4 TLS Ciphersuites and Compression

Within the ClientHello message, the requested ciphersuite MUST be listed. The required ciphersuite support for CableHome is a subset of [RFC 2246] to align with the technology already used within the cable industry. The cable operator will need to select the appropriate encryption and authentication algorithm on the HTTPS server to communicate to the PS that meets the security model for that operator. The ciphersuites required in this specification are a subset of those available and the PS can support additional ciphersuites.

The following cryptographic algorithms MUST be support by the PS.

- TLS_NULL_WITH_NULL_NULL
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

The compression feature of the TLS protocol is not required for CableHome. Therefore, the PS client MUST use compressionMethod.null, as the compression type.

11.9.4.5 TLS Session Tear Down

If the PS is required to download a separate firewall configuration file immediately after the PS configuration file is downloaded, and the firewall configuration file will be downloaded from the same HTTPS server as the PS configuration file was downloaded from, the TLS session is expected to remain active. The PS MUST ensure the TLS and corresponding TCP/IP session is closed with each HTTPS server after:

> The PS configuration file is downloaded, if, and only if there is no firewall configuration file to be downloaded from the same HTTPS server, immediately after the PS configuration file is processed
>
> The firewall configuration file is downloaded and processed

11.9.4.6 TLS Events[134]

[RFC 2246] defines an alert protocol to handle closure and errors for TLS. The TLS alerts and errors MUST be supported and used as defined in [RFC 2246], except the decompression_failure (30) alert will

[134] Revised the first paragraph per ECN CH1.1-N-03.0074-3 by GO on 12/5/03.

EXHIBIT A

not be used for CableHome, since compression is not supported. All TLS alerts MUST be recorded by the PS using event 68002200 with the appropriate error code defined in [RFC 2246] inserted in the Event Text <P1> field. The certificate related errors MUST be treated as critical, since the PS relies on server authentication.

If the PS client has not received a message from the HTTP/TLS server in response to any TLS message sent after 5 attempts, with 30 seconds allowed for each attempt, the TLS connection is considered a failure, and the PS MUST send event 68002100.

11.9.4.7 HTTP Download and Events

The HTTP transfer MUST only be initiated after the TLS handshake has been completed. The PS MUST communicate to the HTTP/TLS server using standard HTTP, as defined by [RFC 2616]. The PS client MUST initiate an HTTP version 1.1 request to the server for the PS configuration file, or the firewall configuration file. The PS configuration filename used in the HTTP "GET Request" MUST be the same filename the PS received in the DHCP ack. The firewall configuration filename used in the HTTP "GET Request" MUST be the same filename the PS received in the PS configuration filename, or via SNMP set.

The PS client MUST handle all status messages according to [RFC 2616]. If the PS client receives an HTTP status message indicating that the HTTP download cannot be completed, the PS MUST fail the session and send event 68003000, with the appropriate error code from [RFC 2616]. If the download cannot be completed after 5 attempts, with 240 seconds allowed for each attempt, the PS MUST fail the session and send event 68003100.

Note: A long timeout is given to include the configuration file download, which at times, can unfortunately be slow. Once the configuration file is downloaded successfully, the PS MUST send event 68003200.

11.10 Physical Security

The PS is required to maintain, in its non-volatile memory, keys and other crypto-variables related to CableHome network security. The PS MUST deter unauthorized physical access to this cryptographic material.

The level of physical protection of keying material required for the PS is specified in terms of the security levels defined in the FIPS PUBS 140-2, Security Requirements for Cryptographic Modules, standard [FIPS 140-2]. In particular, the PS MUST meet FIPS PUBS 140-2 Security Level 1 requirements.

FIPS PUBS 140-2 Security Level 1 requires minimal physical protection through the use of production-grade enclosures and recommended software practices.

11.11 Cryptographic Algorithms

11.11.1 SHA-1

The PS implementation of SHA-1 MUST use the SHA-1 hash algorithm as defined in [FIPS 180-1].

EXHIBIT A

12 MANAGEMENT PROCESSES

12.1 Introduction/Overview

This section provides examples of processes associated with the use of the tools described in Section 6 (Management Tools), and additional processes that facilitate other required management functions defined in this specification. PS Database access and other PS operations of the CableHome Management Portal (CMP) are described in Section 6. Typical CableHome MIB access rules are provided in Section 6.3.3.1.4.2.

Management-related and other descriptive processes are provided for the following scenarios:

- Management Tool Processes
- CTP Operation
    - Connection Speed Tool
    - Ping Tool
- PS Operation
- PS Database Access
- Reconfiguration
    - PS Software Download
    - PS Configuration File Download
- CableHome MIB Access
- VACM Configuration
- Management Event Messaging Configuration
    - CMP Event Notification Operation
    - CMP Event Throttling and Limiting Operation

12.1.1 Goals

This section is primarily composed of informative text, intended to aid in understanding, and does not contain requirements. The examples describe how the Management Tools are used to accomplish typical management functions. Sequence charts of additional management-related processes (i.e., those not defined in Section 6) are also provided, including management processes or process steps associated with the use of required Management Tools. All processes shown involve interaction of the PS element with Headend systems.

12.2 Management Tool Processes

Management Tool Processes are those associated with the required Management Tools defined in Section 6.

12.2.1 CTP Operation

The CableHome Test Portal (CTP) provides Connection Speed Tool and Ping Tool capabilities, described in Section 6.4.3.1 and Section 6.4.3.2, respectively.

EXHIBIT A

12.2.1.1 Remote Connection Speed Test

The Remote Connection Speed Test can be useful in validating performance levels, identifying possible configuration errors, and determining other performance-oriented characteristics:

1. The Network Management System (NMS) starts the test by initializing the test parameters and setting the Begin Test flag, via SNMP SET Request.

2. The CMP SNMP Agent updates the PS Database with the test parameters and notifies the CTP to begin the test.

3. The CTP queries the PS database for the test parameters.

4. The CTP issues a burst of UDP packets to port 7 of the specified LAN IP Device. Port 7 is reserved for the echo service.

5. The target LAN IP Device simply echoes the UDP packet payload back to the CTP

6. Once all of the packets have been received, or the test timeout period has expired, the CTP updates the PS Database with the results of the test and sets the Test Complete flag.

7. The NMS verifies that the command is complete by checking Status = complete.

8. The NMS requests the test results via SNMP GET Request.

9. The CMP SNMP agent queries the PS database for the test results and reports them in the SNMP GET Response. If the test has not completed, the test data will indicate the test is still running. The NMS must repeat the SNMP GET Request until the test results indicate the test has completed.

EXHIBIT A

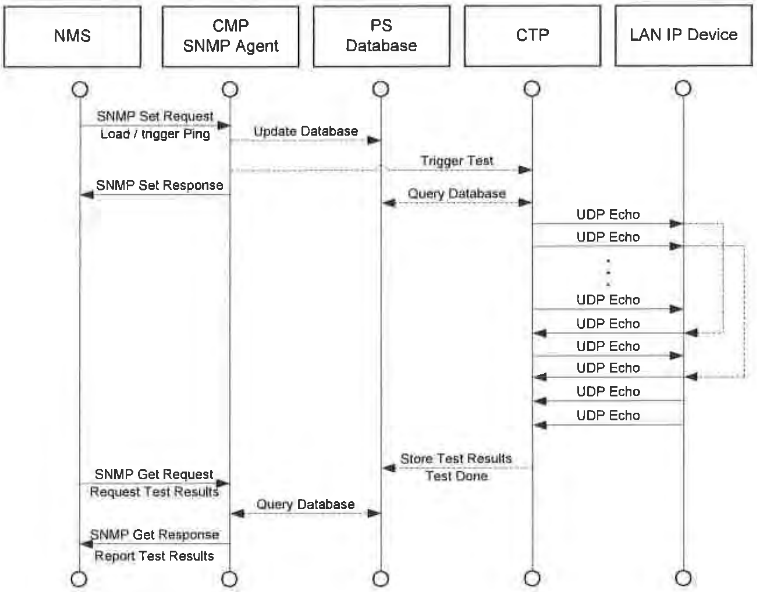


Figure 12-1 – Connection Speed Tool Process Sequence Diagram

12.2.1.2 Ping Tool Process

The Ping Tool can be useful in validating connectivity state, performance levels, and identifying possible configuration errors.

1. The NMS starts the test by initializing the test parameters and setting the Begin Test flag, via SNMP SET Request.
2. The CMP SNMP Agent updates the PS Database with the test parameters and notifies the CTP to begin the test.
3. The CTP queries the PS database for the test parameters.
4. The CTP issues an ICMP Echo Request packet to the specified LAN IP Device.
5. The target LAN IP Device responds with an ICMP Echo Response.
6. The CTP updates the PS Database with the results of the test and sets the Test Complete flag.
7. The NMS verifies that the command is complete by checking Status = complete.
8. The NMS requests the test results via SNMP GET Request.
9. The CMP SNMP agent queries the PS database for the test results and reports them in the SNMP GET

EXHIBIT A

Response. If the test has not completed, the test data will indicate the test is still running. The NMS must repeat the SNMP GET Request until the test results indicate the test has completed.

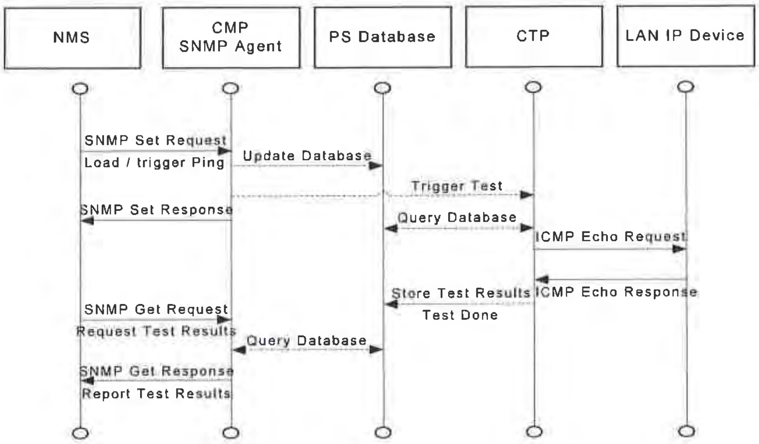


Figure 12-2 — Ping Tool Process Sequence Diagram

12.3 PS Operation

The CableHome Management Portal (CMP) provides access to the PS Database via the PS WAN-Man interface, as described in Section 6. The message sequence for a typical PS Database access operation from the PS WAN-Man interface is described below.

12.3.1 PS Database Access

Configuration and management parameters stored in the PS Database are accessed by the NMS via SNMP MIBs. Parameters are retrieved using SNMP Get-Request, Get-Next-Request, and Get-Bulk messages issued by the NMS with the PS WAN-Man address as the destination address. Parameters can be modified and actions (such as the Connection Speed and Ping tools), executed by the NMS issuing SNMP Set-Request messages with the appropriate parameters, to the PS WAN-Man address.

Figure 12-3 describes the management message sequences for a typical PS Database access from the PS WAN-Man interface. The following message sequences assumes that a secure SNMPv3 link has been established:

1. The NMS reads data from the PS database using the SNMP "GET Request" The request lists the specific objects the NMS wants from the database.

2. The CMP SNMP Agent queries the PS Database for the specified parameters.

3. The CMP SNMP reports the data to the NMS with the SNMP "GET Response".

EXHIBIT A

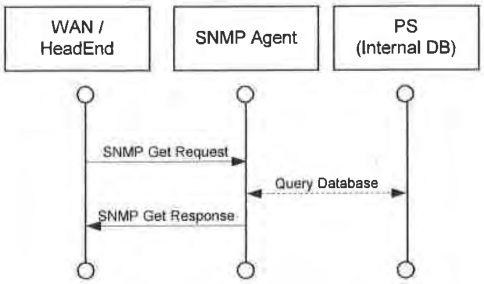


Figure 12-3 – PS Database Access from the PS WAN-Man Interface Sequence Diagram

12.3.2 Reconfiguration

12.3.2.1 PS Software Download

Figure 12-4 illustrates a software/firmware download process for a PS in SNMP Provisioning Mode, which is triggered by the NMS. The PS is instructed where to obtain the new software code file. Once download of the code file is complete, the PS will test the image for any corruption that may have occurred during the download. Authentication is performed to verify that the code file can be trusted. Following this step, a system reboot is performed.

Following the reboot, the PS resumes operation on the new software image. The PS may need to be reconfigured after the software upgrade, and the WAN interfaces may need to be provisioned again (not shown). If the PS does not accept the new software image, it will revert back to the prior (backup) software version and report the results to the NMS.

EXHIBIT A

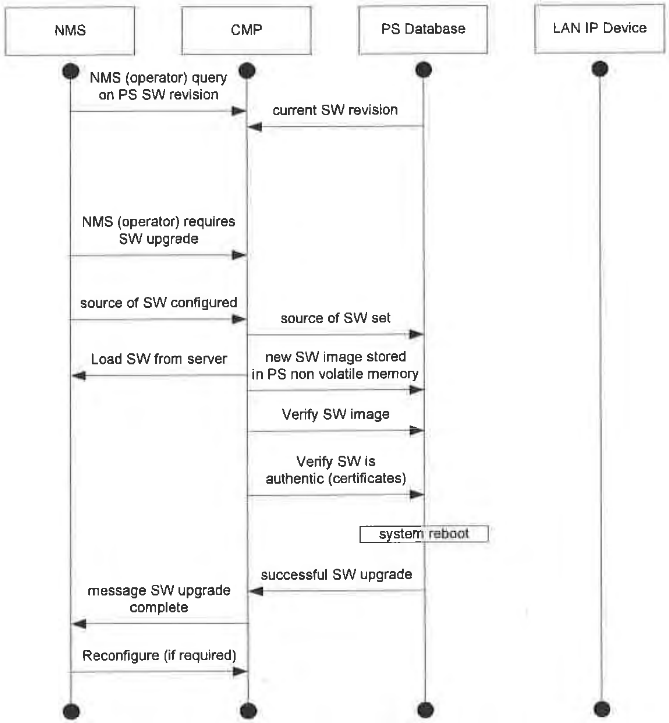

NMS
CMP
PS Database
LAN IP Device
NMS (operator) query on PS SW revision
current SW revision
NMS (operator) requires SW upgrade
source of SW configured
source of SW set
Load SW from server
new SW image stored in PS non volatile memory
Verify SW image
Verify SW is authentic (certificates)
system reboot
successful SW upgrade
message SW upgrade complete
Reconfigure (if required)

Figure 12-4 — PS Software Download Sequence Diagram

12.3.2.2 PS Configuration File Download

Figure 12-5 illustrates a reconfiguration of a PS in SNMP Provisioning Mode, via config file download, and is triggered by the NMS. The configuration file is given to the PS by writing the fileserver and filename into the PS, and triggering the PS to download the file. Once the configuration file is loaded, the commands within it are interpreted. If any of the commands are not understood, or are not applicable, they are skipped and an event is generated. When the PS has completed processing the config file, it will record the number of TLV tuples processed and skipped in the appropriate MIB objects.

EXHIBIT A

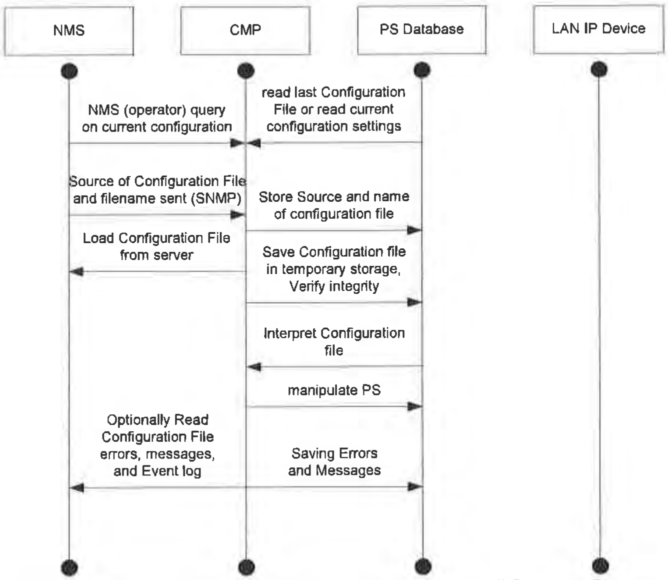

NMS
CMP
PS Database
LAN IP Device
NMS (operator) query on current configuration
read last Configuration File or read current configuration settings
Source of Configuration File and filename sent (SNMP)
Store Source and name of configuration file
Load Configuration File from server
Save Configuration file in temporary storage, Verify integrity
Interpret Configuration file
manipulate PS
Optionally Read Configuration File errors, messages, and Event log
Saving Errors and Messages

Figure 12-5 — PS Reconfiguration (Configuration File Download) Sequence Diagram

12.4 CableHome MIB Access

12.4.1 VACM Configuration

CableHome specifies MSO control of the CableHome management domain. An example of the configuration of VACM parameters is shown below.

EXHIBIT A

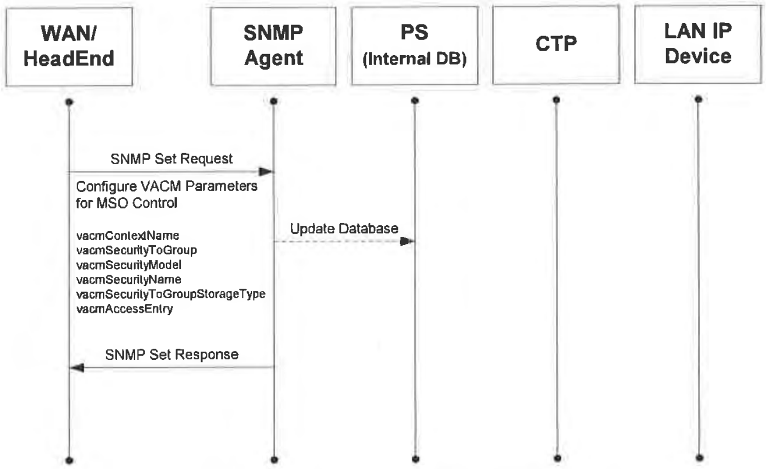


Figure 12-6 — PS Configuration (VACM Parameters) Sequence

12.4.2 Management Event Messaging Configuration

12.4.2.1 CMP Event Notification Operation

CableHome events are reported through local event logging, SNMP TRAP, SNMP INFORM messages, and SYSLOG. The event notification mechanism can be set or modified by the NMS, by issuing an SNMP Set-Request message to the PS WAN-Man address.

Figure 12-7 illustrates configuring the PS database to store events in local log files. Local log events are of two types: local non-volatile and local volatile. The NMS will read the content of the local log and write that content to the Headend event logging system. A PS reboot causes only the volatile events to be cleared from the PS database. Nonvolatile events persist across reboots.

EXHIBIT A

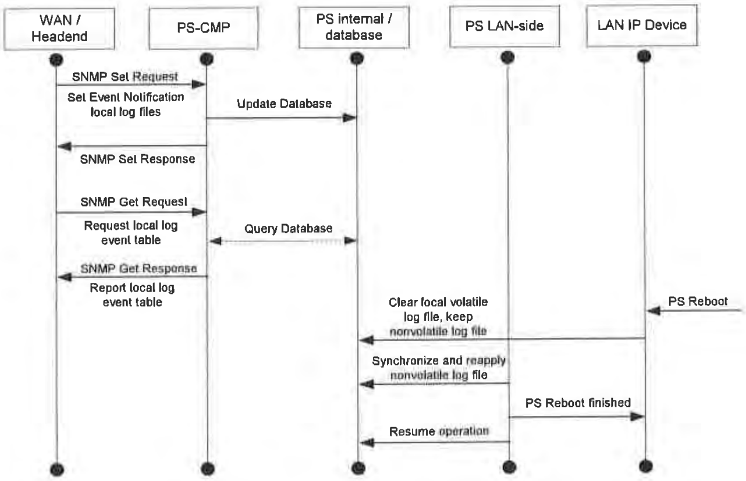


Figure 12-7 – PS Configuration (Event Control) Sequence

Figure 12-8 illustrates the download of a configuration file for a PS in SNMP Provisioning Mode. This process is triggered via an SNMP Set Request. The PS must verify this file before accepting it. In the example, a TLV error exists and is reported. Since the event notification is set to the SNMP TRAP mode, the address of the TRAP server is retrieved from the PS database and the event is sent to that TRAP server.

EXHIBIT A

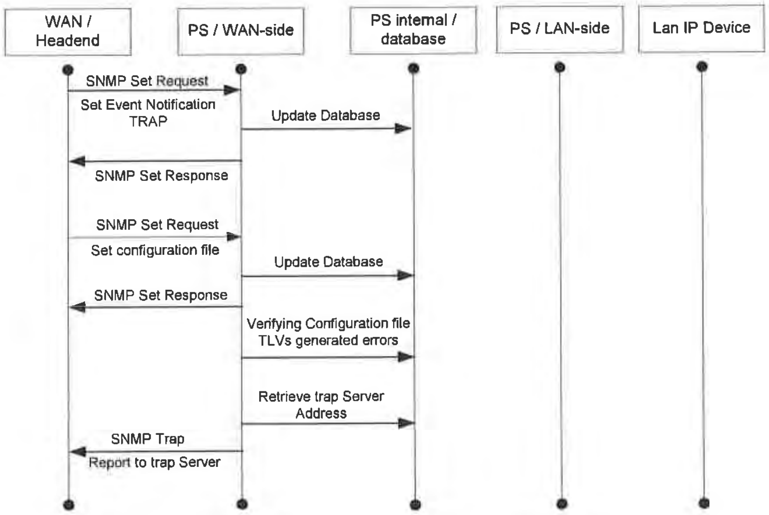


Figure 12-8 – PS Configuration File Download (with Invalid TLVs) Sequence

Figure 12-9 illustrates the process of a LAN IP Device trying to obtain an IP address from the local DHCP server (CDS). The CDS function checks the PS database for an available IP address. In this case, the CDS detects that no IP address is available from the address pool, and generates an event to SYSLOG.

EXHIBIT A

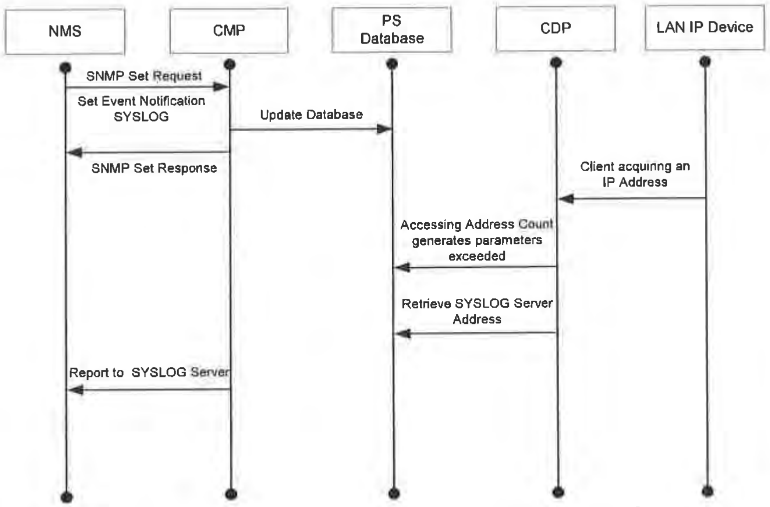

NMS
CMP
PS Database
CDP
LAN IP Device
SNMP Set Request
Set Event Notification SYSLOG
Update Database
SNMP Set Response
Client acquiring an IP Address
Accessing Address Count generates parameters exceeded
Retrieve SYSLOG Server Address
Report to SYSLOG Server

Figure 12-9 — Address Acquisition (Request Exceeds Provisioned Count) Sequence

12.4.2.2 Example CMP Event Throttling and Limiting Operation

CableHome provides an event throttling mechanism via the CMP functionality of the PS. Event throttling and limiting is very flexible and can include cases in which all events are reported, and cases in which no events are reported to the NMS. Refer to Section 6.3.3.2.4.8 for a description of the CMP Event Throttling and Limiting mechanism.

Figure 12-10 illustrates configuring the PS database to return events via the SNMP INFORM method. Initially, several INFORM messages are written to the local log file and delivered to the NMS. The event throttling mechanism sets the limit of the number of events that can be sent to the NMS within a given time frame. When that limit is reached, the PS will stop sending INFORM messages to the NMS. In order to restart the event notification, the NMS SHOULD re-enable the event reporting.

EXHIBIT A

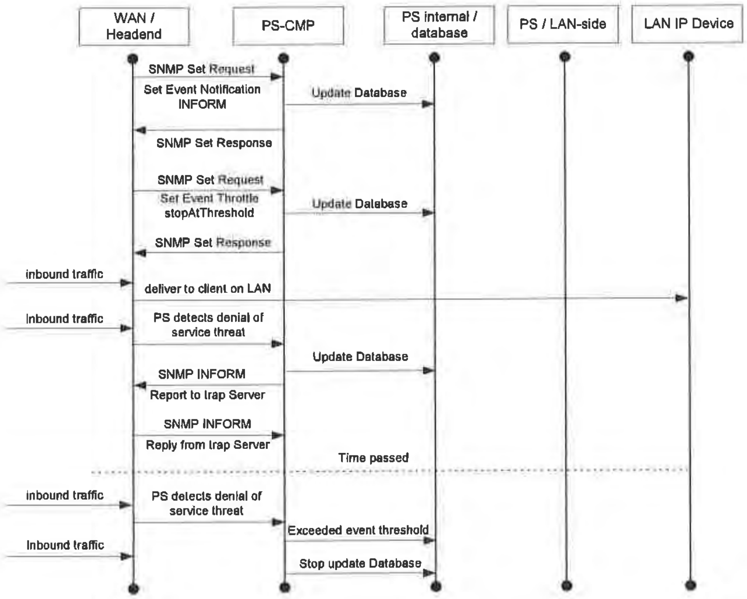


Figure 12-10 — CMP Event Throttling and Limiting Operation

EXHIBIT A

13 PROVISIONING PROCESSES

This chapter describes the processes involved when using the Provisioning Tools, described in Section 7, for initial provisioning of LAN IP Device and the PS element. CableHome specifications refer to provisioning as the following three tasks:

1. Acquiring network addresses

2. Acquiring server information

3. Secure download and processing of the PS Configuration File

Provisioning processes are described in this section for each of the following relevant CableHome cases:

- PS WAN-Man - Provisioning of the PS WAN based management functionality
- PS WAN Data - Provisioning of PS WAN-Data IP addresses to be used for creating CAT Mappings to LAN IP Devices in the LAN-Trans address realm
- LAN IP Device in the LAN-Trans Realm - Provisioning of a LAN IP Device with a translated IP address
- LAN IP Device in the LAN-Pass Realm - Provisioning of a LAN IP Device with an IP address that is passed through to the WAN

Provisioning of the DOCSIS cable modem element of an embedded PS is separate and distinct from CableHome provisioning, and is out of scope for CableHome. The reader is referred to DOCSIS specifications for descriptions of cable modem provisioning.

The functional elements with which the CableHome Portal Services element interacts during the provisioning processes listed above are identified in Figure 13-1. The Key Distribution Center (KDC) functional element is shown with a broken outline, since it is used in SNMP Provisioning Mode, but not in DHCP Provisioning Mode. The other functional elements are used in both provisioning modes.

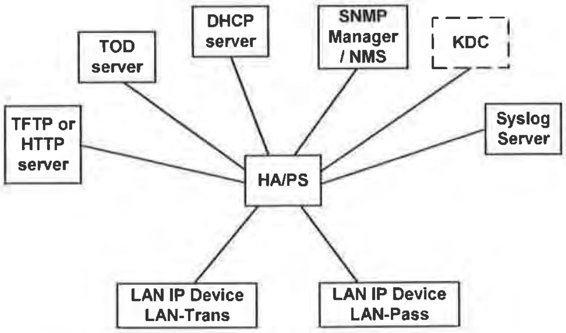


Figure 13-1 — CableHome Provisioning Functional Elements

The Trivial File Transfer Protocol (TFTP) server or the HyperText Transfer Protocol (HTTP) server provides access to the PS Configuration File for the PS and follows rules described in [RFC 1350]. The Time of Day (ToD) server provides the means for the PS to acquire the current time in UTC format as described in[RFC 868]. The Dynamic Host Configuration Protocol (DHCP) server provides the PS with

EXHIBIT A

private and/or global IP addresses following [RFC 2131], as well as providing other information via DHCP options in accordance with [RFC 2132]. The Network Management System (NMS) complies with the Simple Network Management Protocol (SNMP) versions SNMPv1, SNMPv2, and SNMPv3 as described in [RFC 2576]. The System Log (SYSLOG) server handles event messages generated by the PS and by LAN IP Devices in the home. The PS implements clients for these cable data network-based servers, and uses these client functions during the provisioning processes described in this section to accomplish the tasks listed at the beginning of this section.[135]

13.1 Provisioning Modes[136]

Section 5.5 and Section 7.2.1 introduce two valid provisioning modes supported by the Portal Services element: DHCP Provisioning Mode and SNMP Provisioning Mode. The PS operates in a third mode, Dormant CableHome Mode, if it is not configured to operate in either of the two valid provisioning modes. In this section the two valid provisioning modes are presented in more detail. Figure 13-2 illustrates a possible event flow for the two provisioning modes and the Dormant CableHome Mode. The key point of Figure 13-2 is the switch used by the PS to determine the mode in which it is to operate.

The PS operates in DHCP Provisioning Mode (DHCP Mode) if the DHCP server in the cable network provides a valid IP address for the TFTP or HTTP server in the DHCP message 'siaddr' field, provides a valid file name for the PS Configuration File in the DHCP message 'file' field, and does NOT provide DHCP option 177 sub-options 3, 6, and 51 to the PS CDC, during the DHCPACK phase of the initialization process. DHCP Provisioning Mode is intended to enable the PS to operate on a DOCSIS 1.0 or a DOCSIS 1.1 infrastructure, with little or no changes to the DOCSIS network.

SNMP Provisioning Mode in the PS is triggered when the DHCP server in the cable network does NOT provide values for 'siaddr' and 'file', and when the cable network DHCP server DOES send DHCP option 177 sub-options 3, 6, and 51. SNMP Provisioning Mode is intended to enable the PS to take advantage of advanced features of a PacketCable infrastructure.

The PS defaults to Dormant CableHome Mode if it receives none of the fields or sub-options defined as triggers for DHCP Provisioning Mode and for SNMP Provisioning Mode, or if it receives an invalid combination of the fields and sub-options.

The PS defaults to Dormant CableHome Mode if it receives none of the fields or sub-options defined as triggers for DHCP Provisioning Mode and for SNMP Provisioning Mode, or if it receives an invalid combination of the fields and sub-options.

Not all error conditions are shown in Figure 13-2 and Figure 13-3. Refer to Section 7.2.2 for a description of PS behavior in the event of incorrect Provisioning Mode decision criteria.

[135] Revised this paragraph per ECN CH1.1-N-03056 by GO on 10/28/03.

[136] Revised Figure 13-2 and added Figure 13-3 (as Part 2) per ECN CH1.1-N-03.0099-3 by GO on 12/9/03.

EXHIBIT A

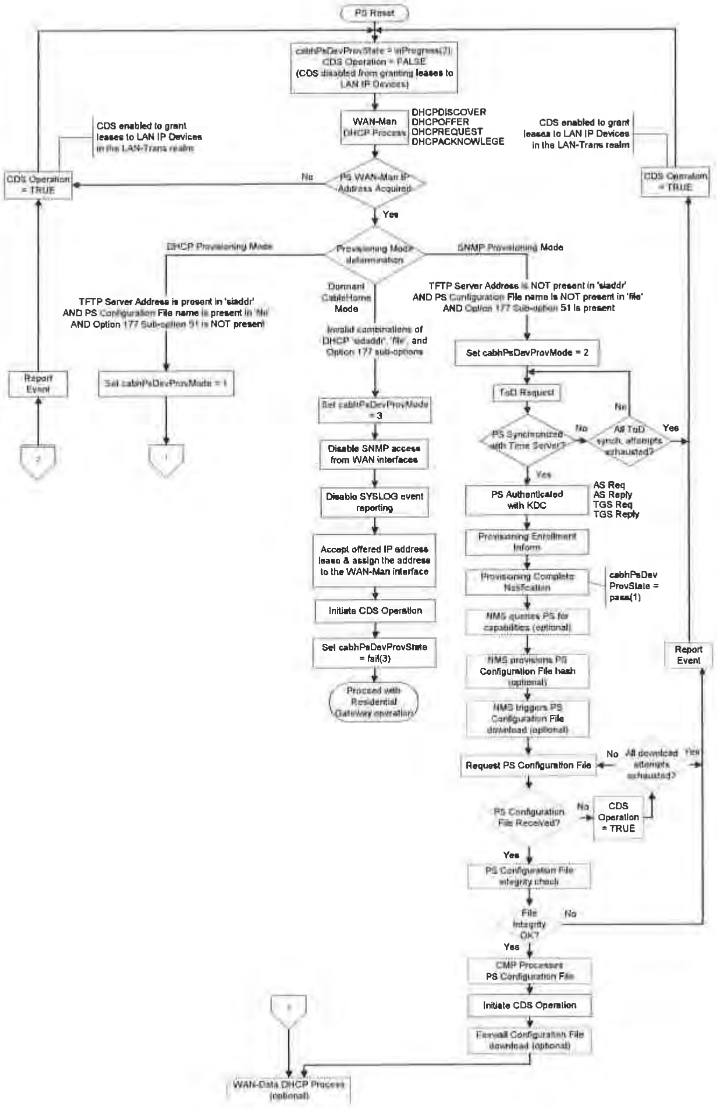

PS Reset
cabhPsDevProvState = inProgress(2)
CDS Operation = FALSE
(CDS disabled from granting leases to LAN IP Devices)
WAN-Man DHCP Process
DHCPDISCOVER
DHCPOFFER
DHCPREQUEST
DHCPACKNOWLEGE
CDS enabled to grant leases to LAN IP Devices in the LAN-Trans realm
CDS enabled to grant leases to LAN IP Devices in the LAN-Trans realm
CDS Operation = TRUE
No
PS WAN-Man IP Address Acquired
CDS Operation = TRUE
Yes
DHCP Provisioning Mode
Provisioning Mode determination
SNMP Provisioning Mode
Dormant CableHome Mode
TFTP Server Address is present in 'siaddr' AND PS Configuration File name is present in 'file' AND Option 177 Sub-option 51 is NOT present
TFTP Server Address is NOT present in 'siaddr' AND PS Configuration File name is NOT present in 'file' AND Option 177 Sub-option 51 is present
Invalid combinations of DHCP 'sdaddr', 'file', and Option 177 sub-options
Set cabhPsDevProvMode = 2
Report Event
Set cabhPsDevProvMode = 1
Set cabhPsDevProvMode = 3
ToD Request
No
PS Synchronized with Time Server?
No
All ToD synch. attempts exhausted?
Yes
2
1
Disable SNMP access from WAN interfaces
Yes
Disable SYSLOG event reporting
PS Authenticated with KDC
AS Req
AS Reply
TGS Req
TGS Reply
Provisioning Enrollment Inform
Accept offered IP address lease & assign the address to the WAN-Man interface
Provisioning Complete Notification
cabhPsDev ProvState = pass(1)
Initiate CDS Operation
NMS queries PS for capabilities (optional)
Set cabhPsDevProvState = fail(3)
Report Event
NMS provisions PS Configuration File hash (optional)
Proceed with Residential Gateway operation
NMS triggers PS Configuration File download (optional)
Request PS Configuration File
No
All download attempts exhausted?
Yes
PS Configuration File Received?
No
CDS Operation = TRUE
Yes
PS Configuration File integrity check
File integrity OK?
No
Yes
CMP Processes PS Configuration File
1
Initiate CDS Operation
Firewall Configuration File download (optional)
WAN-Data DHCP Process (optional)

Figure 13-2 – CableHome 1.1 Provisioning Modes (Part 1)

EXHIBIT A

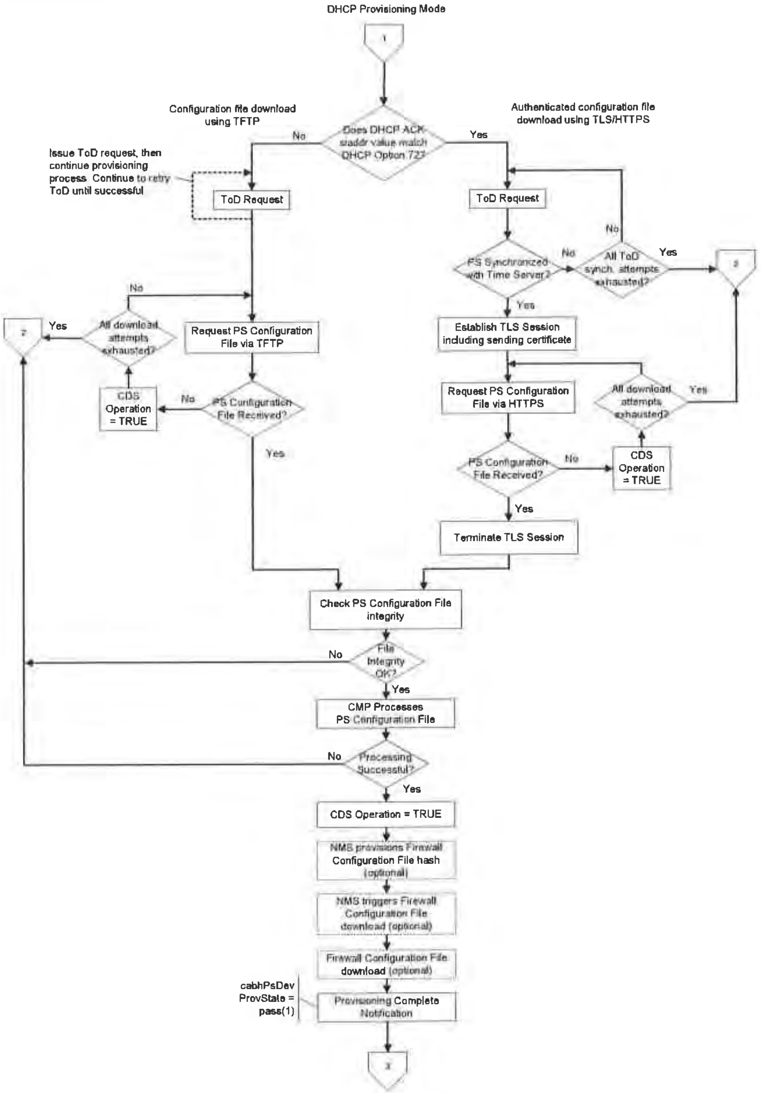

DHCP Provisioning Mode
1
Configuration file download using TFTP
Authenticated configuration file download using TLS/HTTPS
No
Does DHCP ACK siaddr value match DHCP Option 72?
Yes
Issue ToD request, then continue provisioning process. Continue to retry ToD until successful
ToD Request
ToD Request
No
PS Synchronized with Time Server?
No
All ToD synch. attempts exhausted?
Yes
2
Yes
Establish TLS Session including sending certificate
No
2
Yes
All download attempts exhausted?
Request PS Configuration File via TFTP
Request PS Configuration File via HTTPS
All download attempts exhausted?
Yes
CDS Operation = TRUE
No
PS Configuration File Received?
Yes
PS Configuration File Received?
No
CDS Operation = TRUE
Yes
Terminate TLS Session
Check PS Configuration File integrity
No
File Integrity OK?
Yes
CMP Processes PS Configuration File
No
Processing Successful?
Yes
CDS Operation = TRUE
NMS provisions Firewall Configuration File hash (optional)
NMS triggers Firewall Configuration File download (optional)
Firewall Configuration File download (optional)
cabhPsDev ProvState = pass(1)
Provisioning Complete Notification
3

Figure 13-3 – CableHome 1.1 Provisioning Modes (Part 2)

EXHIBIT A

13.2 Process for Provisioning the PS for Management: DHCP Provisioning Mode

The PS requests, from the Headend provisioning system, an IP address to be used for the exchange of management messages between the NMS and the PS. The PS parses the DHCP message returned in the DHCP OFFER and makes a determination about the provisioning mode in which it is to operate (ref. Section 7.3.3.2.4). Section 7.3.3.2.3.2 describes three WAN Address Modes supported by CableHome for the acquisition of IP addresses by the PS from the DHCP server in the cable network.

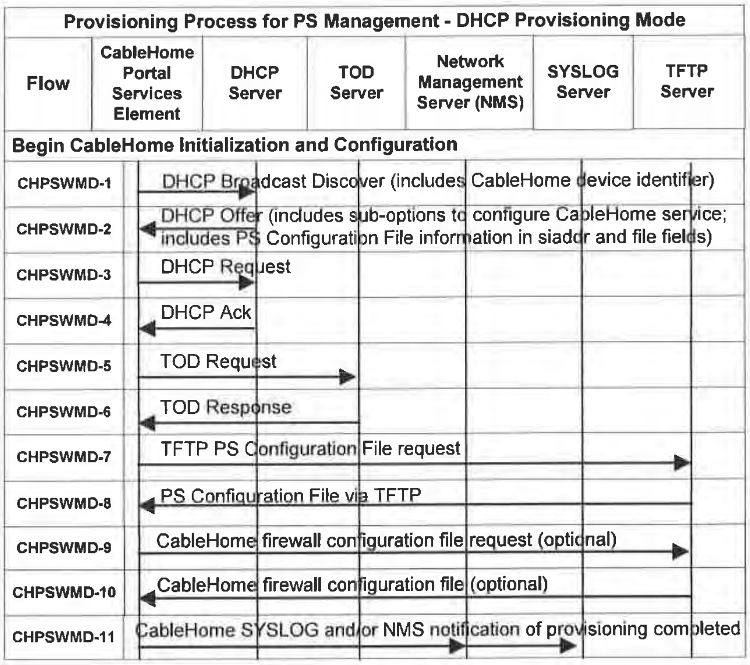
If the PS makes the determination that it is to operate in DHCP Provisioning Mode, it will use the PS Configuration File information passed in the DHCP message as a trigger to download the PS Configuration File, as described in Section 7.3. PS Configuration File download is a requirement for the PS operating in DHCP Provisioning Mode, but is optional for the PS operating in SNMP Provisioning Mode.

In DHCP Provisioning Mode, the PS (CMP) defaults to using NmAccess mode for management message exchange with the NMS, but the NMS can optionally configure the CMP for Coexistence Mode. These management messaging modes are described in Section 6.3.3.

Figure 13-4 and Figure 13-1 describe the sequence of messages needed to initialize a PS operating in DHCP Provisioning Mode. The process for provisioning for management of a PS operating in DHCP Provisioning Mode is the same for the PS embedded with a DOCSIS cable modem, as it is for the stand-alone PS. The provisioning for the Embedded PS MUST NOT occur before the cable modem provisioning process. The stand-alone PS management provisioning SHOULD occur immediately after power-up/reset.

The optional process of downloading a Firewall Configuration File is shown with shading in Figure 13-4.

EXHIBIT A



Provisioning Process for PS Management - DHCP Provisioning Mode

Flow	CableHome Portal Services Element	DHCP Server	TOD Server	Network Management Server (NMS)	SYSLOG Server	TFTP Server

Begin CableHome Initialization and Configuration

CHPSWMD-1 DHCP Broadcast Discover (includes CableHome device identifier)

CHPSWMD-2 DHCP Offer (includes sub-options to configure CableHome service; includes PS Configuration File information in siaddr and file fields)

CHPSWMD-3 DHCP Request

CHPSWMD-4 DHCP Ack

CHPSWMD-5 TOD Request

CHPSWMD-6 TOD Response

CHPSWMD-7 TFTP PS Configuration File request

CHPSWMD-8 PS Configuration File via TFTP

CHPSWMD-9 CableHome firewall configuration file request (optional)

CHPSWMD-10 CableHome firewall configuration file (optional)

CHPSWMD-11 CableHome SYSLOG and/or NMS notification of provisioning completed

Figure 13-4 – Provisioning Process for PS Management - DHCP Provisioning Mode

Table 13-1 describes the individual messages CHPSWMD-1 - CHPSWMD-12 shown in Figure 13-4.[137]

[137] Revised Table 13-1 and deleted text at the end of Table 13-1 per ECN CH1 1-N-03046 and CH1.1-N-03.0099-3 by GO on 07/03/03 and 12/9/03.

EXHIBIT A

Table 13-1 – Flow Descriptions for PS WAN-Man Provisioning Process for DHCP Provisioning Mode

Flow Step	PS WAN-Man Provisioning: DHCP Provisioning Mode	Normal Sequence	Failure Sequence
CHPSWMD-1	DHCP Broadcast Discover The CDP (CDC) sends a broadcast DHCP DISCOVER message to acquire the WAN-Man IP address as described in Section 7.3.3.2.4. The DHCP DISCOVER broadcast by the CDP (CDC) includes mandatory options listed in Table 7-10, CDC DHCP Options in DISCOVER and REQUEST Messages. The PS sets cabhPsDevProvState to status 'inProgress' (2) when the CDC sends a broadcast DHCP DISCOVER.	Begin provisioning sequence.	If unsuccessful per DHCP protocol report an error and continue to retry DHCP Broadcast Discover until successful (return to step CHPSWMD-1). If unsuccessful on the first attempt to acquire a WAN-Man IP address, the PS initiates operation of the CDS as specified in Section 7.3.3.2.4.
CHPSWMD-2	DHCP OFFER	CHPSWMD-2 MUST occur after CHPSWMD-1 completion.	If failure per DHCP protocol return to CHPSWMD-1 and report an error.
CHPSWMD-3	DHCP REQUEST The CDP MUST send the appropriate DHCP server a DHCP REQUEST message to accept the DHCP OFFER.	CHPSWMD-3 MUST occur after CHPSWMD-2 completion.	If failure per DHCP protocol return to CHPSWMD-1 and report an error.
CHPSWMD-4	DHCP ACK The DHCP server sends the CDP a DHCP ACK message which contains the IPv4 address of the PS. The PS modifies cabhPsDevProvMode based on information received in the DHCP ACK (ref.: Section 7.3.3.2.4). The PS stores the Time of Day server address in cabhPsDevTimeServerAddr. The PS modifies cabhPsDevProvMode based on information received in the DHCP ACK (ref.: Section 7.3.3.2.4).	CHPSWMD-4 MUST occur after CHPSWMD-3 completion.	If failure per DHCP protocol return to CHPSWMD-1 and report an error.
CHPSWMD-5	Time of Day (TOD) Request per [RFC 868] The PS issues a ToD Request to the Time Server identified in Option 4 of the DHCP ACK message.	CHPSWMD-5 MUST occur after CHPSWMD-4 completion.	Continue with CHPSWMD-6.
CHPSWMD-6	TOD Response The ToD server is expected to reply with the current time in UTC format.	CHPSWMD-6 MUST occur after CHPSWMD-5 completion.	Attempt synchronization with the next Time of Day server listed in DHCP Option 4 of the DHCP ACK. If an unsuccessful synchronization attempt has been made with each ToD server as part of an initial attempt to synchronize Time of Day, set cabhPsDevTodSyncStatus = false(2), attempt to acquire system time from the cable modem (embedded PS only), update cabhPsDevDateTime, update CDS lease times, and continue with CHPSWMD-7. Refer to Section 7.5.4. for additional details.

EXHIBIT A

Flow Step	PS WAN-Man Provisioning: DHCP Provisioning Mode	Normal Sequence	Failure Sequence
CHPSWMD-7	TFTP Request The PS operating in DHCP Provisioning Mode sends the TFTP Server a TFTP Get Request to request the specified configuration data file as described in Section 7.4.4.	CHPSWMD-7 MUST occur after CHPSWMD-5 completion. CHPSWMD-7 MAY occur before CHPSWMD-6 completion.	Continue to CHPSWMD-8.
CHPSWMD-8	TFTP server sends PS Configuration File After the PS Configuration File is received, the hash is checked. Refer to Section 7.4.4.1. The PS Configuration File is then processed. Refer to Section 7.4.4 for PS Configuration File contents. Optionally, the IP Address of the firewall Configuration File TFTP server, the firewall Configuration File filename and the hash of the firewall Configuration File are included in the PS Configuration File if there is a firewall Configuration File to be loaded, and this is the method selected to specify it.	CHPSWM-8 MUST occur after CHPSWM-7 completion.	If the TFTP download fails, take action, depending upon the nature of the error, as described in Section 7.4.4.4.
CHPSWMD-9	TFTP Request - Firewall Configuration File (optional) If the PS receives Firewall Configuration File information (Firewall TFTP server and Firewall Configuration File name) in the PS Configuration File, the PS sends the Firewall Configuration TFTP Server a TFTP Get Request to request a Firewall Configuration File (see Section 11.6.4.2). If the PS does not receive Firewall Configuration File information in the PS Configuration file, the PS provisioning process (DHCP Provisioning Mode) MUST skip steps CHPSWMD-9 and CHPSMWD-10 and continue with step CHPSWMD-11.	If CHPSWMD-9 occurs, it MUST occur after CHPSWMD-8 completion.	If TFTP fails, continue with PS operation but report an error and continue to retry CHPSWMD-9.
CHPSWMD-10	TFTP server sends firewall configuration file (optional) If step CHPSWMD-9 occurs, the TFTP Server sends the PS a TFTP Response containing the requested file. After the firewall configuration file is received the hash of the configuration file is calculated and compared to the value received in the PS Configuration File. The file is then processed. Refer to Section 11.6.4.	CHPSWMD-10 MUST occur after CHPSWMD-9 completion.	If the TFTP fails, continue with PS operation but report an error and continue to retry CHPSWMD-9. If processing of the firewall configuration file produces an error, continue and report the error as an event.

EXHIBIT A

Flow Step	PS WAN-Man Provisioning: DHCP Provisioning Mode	Normal Sequence	Failure Sequence
CHPSWMD-11	Provisioning Complete If requested by the provisioning system the PS is required to inform the provisioning system of the status of PS provisioning. The provisioning system could request the PS to send a SYSLOG message or an SNMP trap, or both. If the PS successfully completes all required steps from CHPSWMD-1 through CHPSWMD-10 and the PS received a SYSLOG server address in the DHCP OFFER, the PS MUST send a provisioning complete message to the SYSLOG server with provisioning state set to PASS. If the PS successfully completes all required provisioning steps from CHPSWMD-1 through CHPSWMD-10 and the PS received valid parameters the Notification Receiver, the PS MUST send a provisioning complete notification (cabhPsDevInitTrap) with appropriate parameters to the Notification Receiver. The PS MUST update the value of cabhPsDevProvState with status 'pass' (1) when provisioning flow steps CHPSWMD-1 through CHPSWMD-11 complete successfully.	CHPSWMD-11 MUST occur after CHPSWMD-10 completion.	If the SNMP trap fails, the provisioning server may not know the provisioning process has completed unless it polls the cabhPsProvState object.

13.3 Process for Provisioning the PS for Management: DHCP Provisioning Mode with HTTP/TLS

The PS requests from the Headend provisioning system, an IP address to be used for the exchange of management messages between the NMS and the PS. The PS parses the DHCP message returned in the DHCP OFFER and makes a determination about the provisioning mode in which it is to operate (ref. Section 7.3.3.2.4). Section 7.3.3.2.3.2 describes three WAN Address Modes supported by CableHome for the acquisition of IP addresses by the PS from the DHCP server in the cable network.

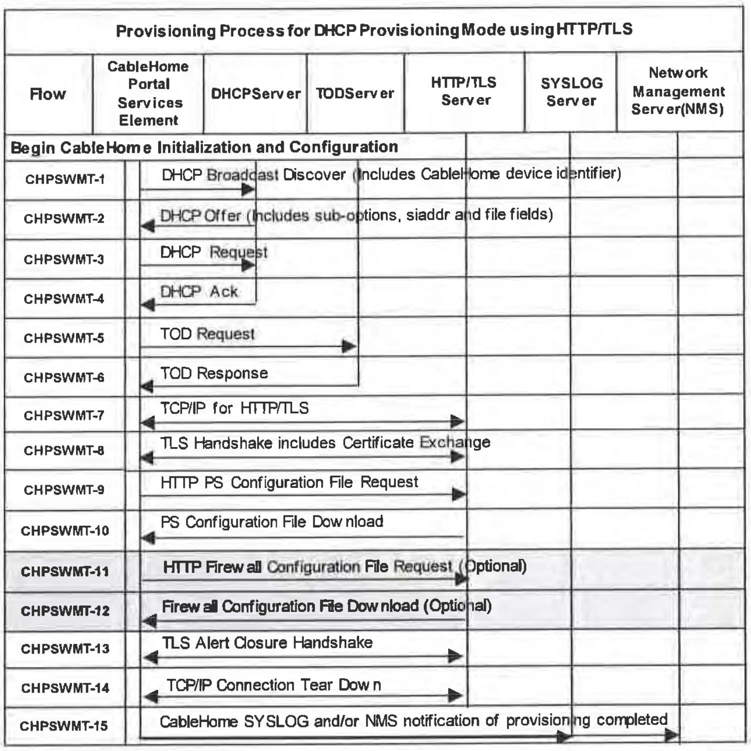
If the PS makes the determination that it is to operate in DHCP Provisioning Mode, it will use the PS Configuration File information passed in the DHCP message, as a trigger to download the PS Configuration File. If DHCP option code 72 is present in the DHCP ACK message, and if its contents match the IP address in the siaddr field, the download will occur, using HTTP over TLS, as specified in Section 11.9.

In DHCP Provisioning Mode, the PS (CMP) defaults to using NmAccessTable mode for management message exchange with the NMS, but the NMS can optionally configure the CMP for Coexistence Mode. These management messaging modes are described in Section 6.3.3.

Figure 13-5 and Table 13-2 describe the sequence of messages needed to initialize a PS operating in DHCP Provisioning Mode with HTTP/TLS. The process for provisioning and management of the PS operating in DHCP Provisioning Mode is the same for the PS embedded with a DOCSIS cable modem as it is for the stand-alone PS. The provisioning for the Embedded PS MUST NOT occur before the cable modem provisioning process. The stand-alone PS management provisioning SHOULD occur immediately after power-up/reset.

The optional process of downloading a Firewall Configuration File is shown with shading in Figure 13-5.

EXHIBIT A



Provisioning Process for DHCP Provisioning Mode using HTTP/TLS						
Flow	CableHome Portal Services Element	DHCPServer	TODServer	HTTP/TLS Server	SYSLOG Server	Network Management Server(NMS)
Begin CableHome Initialization and Configuration						
CHPSWMT-1	DHCP Broadcast Discover (Includes CableHome device identifier)					
CHPSWMT-2	DHCP Offer (Includes sub-options, siaddr and file fields)					
CHPSWMT-3	DHCP Request					
CHPSWMT-4	DHCP Ack					
CHPSWMT-5	TOD Request					
CHPSWMT-6	TOD Response					
CHPSWMT-7	TCP/IP for HTTP/TLS					
CHPSWMT-8	TLS Handshake includes Certificate Exchange					
CHPSWMT-9	HTTP PS Configuration File Request					
CHPSWMT-10	PS Configuration File Dow nload					
CHPSWMT-11	HTTP Firew all Configuration File Request (Optional)					
CHPSWMT-12	Firew all Configuration File Dow nload (Optional)					
CHPSWMT-13	TLS Alert Closure Handshake					
CHPSWMT-14	TCP/IP Connection Tear Dow n					
CHPSWMT-15	CableHome SYSLOG and/or NMS notification of provisioning completed					

Figure 13-5 – Provisioning Process DHCP Provisioning Mode using HTTP/TLS

Table 13-2 describes the individual messages CHPSWMT-1 - CHPSWMT-12 shown in Figure 13-4. Refer to Section 11.9 PS Configuration File Security in DHCP Provisioning Mode for more information.[138] [139]

[138] Revised this paragraph and the following Table 13-2 per ECN CH1.1-N-03046 by GO on 07/07/03.

[139] Revised Table 13-2 per ECN CH1.1-N-03.0099-3 by GO on 12/9/03.

EXHIBIT A

Table 13-2 – Flow Descriptions for DHCP Provisioning Mode using HTTP/TLS

Flow Step	PS WAN-Man Provisioning: DHCP Provisioning Mode	Normal Sequence	Failure Sequence
CHPSWMT-1	DHCP Broadcast Discover The CDP (CDC) sends a broadcast DHCP DISCOVER message to acquire the WAN-Man IP address as described in Section 7.3.3.2.4. The DHCP DISCOVER broadcast by the CDP (CDC) includes mandatory options listed in Table 7-10, CDC DHCP Options in DISCOVER and REQUEST Messages. The PS sets cabhPsDevProvState to status 'inProgress' (2) when the CDC sends a broadcast DHCP DISCOVER.	Begin provisioning sequence.	If unsuccessful per DHCP protocol report an error and continue to retry DHCP Broadcast Discover until successful (return to step CHPSWMT-1). If unsuccessful on the first attempt to acquire a WAN-Man IP address, the PS initiates operation of the CDS as specified in Section 7.3.3.2.4.
CHPSWMT-2	DHCP OFFER	CHPSWMT-2 MUST occur after CHPSWMT-1 completion.	If failure per DHCP protocol return to CHPSWMT-1 and report an error.
CHPSWMT-3	DHCP REQUEST The CDP sends the appropriate DHCP server a DHCP REQUEST message to accept the DHCP OFFER.	CHPSWMT-3 MUST occur after CHPSWMT-2 completion.	If failure per DHCP protocol return to CHPSWMT-1 and report an error.
CHPSWMT-4	DHCP ACK The DHCP server sends the CDP a DHCP ACK message which contains the IPv4 address of the PS. The PS stores the Time of Day server address in cabhPsDevTimeServerAddr. If the IP address in the siaddr field of the DHCP ACK matches the first IP address in option 72, the PS initiates a TLS session and downloads the configuration file from the HTTP server. The PS modifies cabhPsDevProvMode based on information received in the DHCP ACK. Refer to Table 11-9 PS Configuration File Security in DHCP Provisioning Mode.	CHPSWMT-4 MUST occur after CHPSWMT-3 completion.	If failure per DHCP protocol return to CHPSWMT-1 and report an error.
CHPSWMT-5	Time of Day (TOD) Request per [RFC 868] The PS synchronizes its time with the time server selected from DHCP Option 4 (Time Server Option) in the DHCP ACK. Refer to Section 7.5.4 Time of Day Client Function Requirements.	CHPSWMT-5 MUST occur after CHPSWMT-4 completion.	Continue with CHPSWMT-6.

EXHIBIT A

Flow Step	PS WAN-Man Provisioning: DHCP Provisioning Mode	Normal Sequence	Failure Sequence
CHPSWMT-6	TOD Response The ToD server is expected to reply with the current time in UTC format.	CHPSWMT-6 MUST occur after CHPSWMT-5 completion.[1]	Attempt synchronization with the next Time of Day server listed in DHCP Option 4 of the DHCP ACK. If an unsuccessful synchronization attempt has been made with each ToD server as part of an initial attempt to synchronize Time of Day, set cabhPsDevTodSyncStatus = false(2), update cabhPsDevDateTime, update CDS lease times, and continue with CHPSWMT-7. Refer to Section 7.5.4. for additional details.
CHPSWMT-7	TCP/IP Setup The PS operating in DHCP Provisioning Mode establishes. a TCP/IP session to exchange HTTP messages with the HTTP server in the cable operator's provisioning system.	CHPSWMT-7 MUST occur after CHPSWMT-5 completion. CHPSWMT-7 MAY occur before CHPSWMT-6 completion.	If failure per TCP/IP retry per the specification. If retries all fail return to CHPSWMT-1 and report an error.
CHPSWMT-8	TLS Handshake The PS operating in DHCP Provisioning Mode establishes a TLS session with the HTTPS server.	CHPSWMT-8 MUST occur after CHPSWMT-7 completion.	If failure for TLS retry per the specification. If retries all fail return to CHPSWMT-1 and report an error.
CHPSWMT-9	HTTP Configuration File Request The PS operating in DHCP Provisioning Mode requests the configuration file from the HTTP server.	CHPSWMT-9 MUST occur after CHPSWMT-8 completion.	If failure for HTTP retry per the specification. If retries all fail return to CHPSWMT-1 and report an error.
CHPSWMT-10	HTTPS server sends PS Configuration File The PS Configuration File is processed. Refer to Section 7.4.4 for PS Configuration File contents. Optionally, the IP Address of the firewall Configuration File HTTP server and the firewall Configuration File filename of the firewall Configuration File are included in the PS Configuration File.	CHPSWMT-10 MUST occur after CHPSWMT-9 completion.	If the HTTP download fails, report an error and return to CHPSWMT- 9 (continue to retry PS Config File download). If processing of the PS Config File produces an error, continue with CHPSWMT-13 and report the error as an event.

EXHIBIT A

Flow Step	PS WAN-Man Provisioning: DHCP Provisioning Mode	Normal Sequence	Failure Sequence
CHPSWMT-11	HTTP Request - Firewall Configuration File (Optional) If the PS receives Firewall Configuration File information (Firewall TFTP server and Firewall Configuration File name) in the PS Configuration File, the PS requests the Firewall Configuration File from the HTTP Server. If the PS does not receive Firewall Configuration File information in the PS Configuration file, the PS provisioning process (DHCP Provisioning Mode) MUST skip steps CHPSWMT-11 and CHPSMWT-12 and continue with step CHPSWMT-13.	If CHPSWMT-11 occurs, it MUST occur after CHPSWMT-10 completion.	If HTTP fails, continue with PS operation but report an error and continue to retry CHPSWMT-13.
CHPSWMT-12	HTTP server sends firewall configuration file (Optional) If step CHPSWMD-11 occurs, the HTTP Server sends the PS a HTTP Response containing the requested firewall configuration file.	CHPSWMT-12 MUST occur after CHPSWMT-11 completion.	If the HTTP fails, continue with PS operation but report an error and continue to retry CHPSWMD-11. If processing of the firewall configuration file produces an error, continue and report the error as an event.
CHPSWMT-13	TLS Alert Closure Handshake The PS tears down the TLS session immediately prior to sending the provisioning complete message.	CHPSWMT-13 MUST occur after CHPSWMT-12 completion	Continue to CHPSWMT-14. If failure for HTTP retry per the specification. If retries all fail report an error.
CHPSWMT-14	TCP/IP Tear Down The TCP/IP session between the PS and the HTTP Server is torn down.	CHPSWMT-14 MUST occur after CHPSWMT-13 completion.	If the TCP/IP tear down fails report an error. Continue to 15.

EXHIBIT A

Flow Step	PS WAN-Man Provisioning: DHCP Provisioning Mode	Normal Sequence	Failure Sequence
CHPSWMT-15	Provisioning Complete If requested by the provisioning system the PS is required to inform the provisioning system of the status of PS provisioning. The provisioning system could request the PS to send a SYSLOG message or an SNMP trap, or both. If the PS successfully completes all required steps from CHPSWMT-1 through CHPSWMT-14 and the PS received a SYSLOG server address in the DHCP OFFER, the PS MUST send a provisioning complete message to the SYSLOG server with provisioning state set to PASS. If the PS successfully completes all required provisioning steps from CHPSWMT-1 through CHPSWMT-12 and the PS received valid parameters for docsDevNmAccessGroup identifying the Trap Receiver (docsDevNmAccessIP) and configuring the provisioning complete trap (cabhPsDevInitTrap) for 'read only with Traps' (set docsDevNmAccess control to '4'. Refer to [RFC 2669]), the PS MUST send a provisioning complete trap (cabhPsDevInitTrap) with appropriate parameters to the Trap Receiver. If the PS provisioning timer expires before all required steps from CHPSWMT-1 through CHPSWMT-14 are completed and the PS received a SYSLOG server address in the DHCP OFFER, the PS MUST send a provisioning complete message to the SYSLOG server with provisioning state set to FAIL. If the PS provisioning timer expires before all required steps from CHPSWMD-1 through CHPSWMD-14 are completed and the PS received valid parameters for docsDevNmAccessGroup identifying the Trap Receiver (docsDevNmAccessIP) and configuring the provisioning complete trap (cabhPsDevInitTrap) for 'read only with Traps' (set docsDevNmAccess control to '4'. Refer to [RFC 2669].), the PS MUST send a provisioning failed trap (cabhPsDevInitRetryTrap) to the Trap receiver. The PS updates the value of cabhPsDevProvState with status 'pass' (1) when provisioning flow steps CHPSWMT-1 through CHPSWMT-14 complete successfully. Refer to Section 7.5.4.	CHPSWMT-15 MUST occur after CHPSWMT-14 completion.	If the SNMP trap fails, the provisioning server may not know the provisioning process has completed unless it polls the cabhPsDevProvState object.

13.4 Provisioning the PS for Management: SNMP Provisioning Mode

The PS requests a WAN-Man network address from the Headend DHCP server to be used for the exchange of management messages between the PS management functions and the cable network NMS. If the PS determines based on the procedure described in Section 7.3.3.2.4 that it is to operate in SNMP Provisioning Mode, the PS will secure its management messages using SNMPv3, following the authentication procedure described in Section 11.3.2.

The cable network NMS may optionally instruct the PS (CMP) operating in SNMP Provisioning Mode to download a PS Configuration File from the TFTP server. Notification of completion of the provisioning

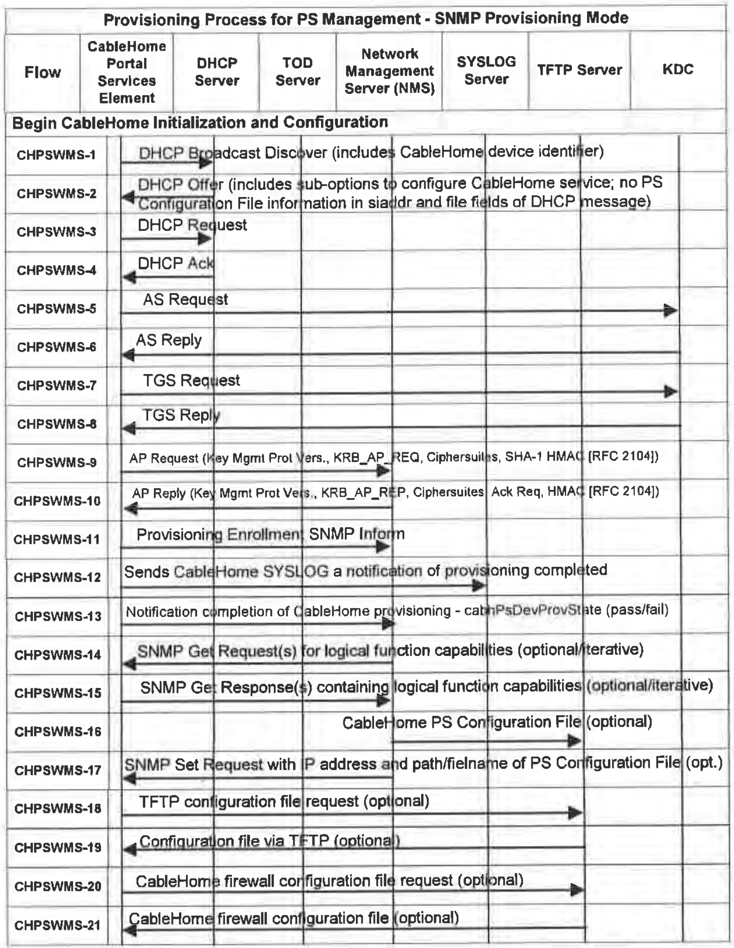
EXHIBIT A

process is provided through the Event Reporting process described in Section 6.3.3.2. The PS will operate without a PS Configuration File if it is not triggered to download the file.

Figure 13-6 illustrates message flows that are to be used to accomplish the provisioning of the PS when it operates in SNMP Provisioning Mode. The provisioning process for the PS WAN-Man interface is the same for the Embedded PS as it is for the Stand-alone PS. The Standalone PS provisioning SHOULD occur immediately after power-up/reset.

The provisioning process for the WAN-Man interface of a PS operating in SNMP Provisioning Mode MUST occur via the sequence depicted in Figure 13-6 and described in detail in Table 13-3. Optional steps are shown with a shaded background in Figure 13-6. These optional steps may be done immediately following step CHPSWMS-13, at a later time, or not at all.

EXHIBIT A



Provisioning Process for PS Management - SNMP Provisioning Mode

Flow	CableHome Portal Services Element	DHCP Server	TOD Server	Network Management Server (NMS)	SYSLOG Server	TFTP Server	KDC

Begin CableHome Initialization and Configuration

CHPSWMS-1	DHCP Broadcast Discover (includes CableHome device identifier)
CHPSWMS-2	DHCP Offer (includes sub-options to configure CableHome service; no PS Configuration File information in siaddr and file fields of DHCP message)
CHPSWMS-3	DHCP Request
CHPSWMS-4	DHCP Ack
CHPSWMS-5	AS Request
CHPSWMS-6	AS Reply
CHPSWMS-7	TGS Request
CHPSWMS-8	TGS Reply
CHPSWMS-9	AP Request (Key Mgmt Prot Vers., KRB_AP_REQ, Ciphersuites, SHA-1 HMAC [RFC 2104])
CHPSWMS-10	AP Reply (Key Mgmt Prot Vers., KRB_AP_REP, Ciphersuites Ack Req, HMAC [RFC 2104])
CHPSWMS-11	Provisioning Enrollment SNMP Inform
CHPSWMS-12	Sends CableHome SYSLOG a notification of provisioning completed
CHPSWMS-13	Notification completion of CableHome provisioning - cabhPsDevProvState (pass/fail)
CHPSWMS-14	SNMP Get Request(s) for logical function capabilities (optional/iterative)
CHPSWMS-15	SNMP Get Response(s) containing logical function capabilities (optional/iterative)
CHPSWMS-16	CableHome PS Configuration File (optional)
CHPSWMS-17	SNMP Set Request with IP address and path/fielname of PS Configuration File (opt.)
CHPSWMS-18	TFTP configuration file request (optional)
CHPSWMS-19	Configuration file via TFTP (optional)
CHPSWMS-20	CableHome firewall configuration file request (optional)
CHPSWMS-21	CableHome firewall configuration file (optional)

Figure 13-6 – Provisioning Process for PS Management - SNMP Provisioning Mode

Table 13-3 describes the individual steps of the provisioning process depicted in Figure 13-6.[140]

[140] Revised Table 13-3 per ECN CH1.1-N-03046 and CH1.1-N-03 0099-3 by GO on 07/07/03 and 12/10/03

EXHIBIT A

Table 13-3 – Flow Descriptions for PS WAN-Man Provisioning Process for SNMP Provisioning Mode

Flow Step	PS WAN-Man Provisioning: SNMP Provisioning Mode	Normal Sequence	Failure Sequence
CHPSWMS- 1	DHCP Broadcast Discover The CDP (CDC) broadcasts a DHCP DISCOVER message to acquire the WAN-Man IP address as described in Section 7.3.3.2.4 CDC Requirements. The DHCP DISCOVER broadcast by the CDC includes mandatory options listed in Table 7-10, CDC DHCP Options in DISCOVER and REQUEST Messages. The PS starts monitoring time elapsed AND sets cabhPsDevProvState to status 'inProgress' (2) when the CDC broadcasts its initial DHCP DISCOVER message.	Begin provisioning sequence.	If failure per DHCP protocol report an error and continue to retry DHCP Broadcast Discover until successful (return to CHPSWMS-1). If the first attempt to acquire an address lease from the cable operator's DHCP server fails, initiate operation of the CDS as specified in Section 7.3.3.2.4 CDC Requirements.
CHPSWMS- 2	DHCP OFFER	CHPSWMS-2 MUST occur after CHPSWMS-1 completion.	If failure per DHCP protocol return to CHPSWMS-1 and report an error.
CHPSWMS- 3	DHCP REQUEST The CDP sends to the appropriate DHCP server a DHCP REQUEST message to accept the DHCP OFFER.	CHPSWMS-3 MUST occur after CHPSWMS-2 completion.	If failure per DHCP protocol return to CHPSWMS-1.
CHPSWMS- 4	DHCP ACK The DHCP server sends the CDC a DHCP ACK message which contains the IPv4 address of the PS WAN-Man Interface and is expected to include the CableHome option code 177 with sub-options 3, 6, & 51 AND no PS configuration file information in the siaddr and file fields of the DHCP message. The PS modifies cabhPsDevProvMode based on information received in the DHCP ACK (ref.: Section 7.3.3.2.4). The PS stores the Time of Day server address in cabhPsDevTimeServerAddr.	CHPSWMS-4 MUST occur after CHPSWMS-3 completion.	If failure per DHCP protocol return to CHPSWMS-1 and report an error.
CHPSWMS- 5	Time of Day (TOD) Request per [RFC 868] The PS issues a ToD Request message to the Time Server identified in the DHCP Option 4 of the DHCP ACK message.	CHPSWMS-5 MUST occur after CHPSWMS-4 completion.	Continue with CHPSWMS-6.
CHPSWMS- 6	TOD Response The ToD server is expected to reply with the current time in UTC format.	CHPSWMS-6 MUST occur after CHPSWMS-5 completion.	Retry Time Server synchronization up to a total of four attempts; if not successful in four attempts, attempt synchronization with the next Time Server listed in Option 4 of DHCP ACK; if not successful after four attempts with each Time Server report an error, and return to CHPSWMS-1

EXHIBIT A

Flow Step	PS WAN-Man Provisioning: SNMP Provisioning Mode	Normal Sequence	Failure Sequence
CHPSWMS- 7	AS Request[1] The PS sends the AS Request message to the MSO CableHome KDC provided in DHCP Option 177 suboption 51, to request a Kerberos ticket.	CHPSWMS-7 MUST occur after CHPSWMS-6 completion.	Return to CHPSWMS-1. PS initiates operation of CDS.
CHPSWMS- 8	AS Reply The AS Reply Message is received from the MSO CableHome KDC containing the Kerberos ticket	CHPSWMS-8 MUST occur after CHPSWMS-7 completion.	Return to CHPSWMS-1. PS initiates operation of CDS.
CHPSWMS- 9	TGS Request If the PS obtained a Ticket Granting Ticket (TGT) during step CHPSWMS-8, the PS sends the TGS Request message to the MSO KDC server whose address was passed to the PS (CDC) in DHCP Option 177 sub-option 51.	CHPSWMS-9 MUST occur after CHPSWMS-8 completion.	Return to CHPSWMS-1. PS initiates operation of CDS.
CHPSWMS-10	TGS Reply The TGS Reply message containing the ticket is received from the MSO CableHome KDC.	CHPSWMS-10 MUST occur after CHPSWMS-9 completion.	Return to CHPSWMS-1. PS initiates operation of CDS.
CHPSWMS-11	AP Request The PS sends the AP Request message to the NMS (SNMP manager) to request keying information for SNMPv3, as described in Section 11.3 PS Authentication Infrastructure.	CHPSWMS-11 MUST occur after CHPSWMS-10 completion.	Return to CHPSWMS-1. PS initiates operation of CDS.
CHPSWMS-12	AP reply The AP Reply message is received from the NMS containing the keying information for SNMPv3.Note: The PS MUST establish SNMPv3 keys AND populate the associated SNMPv3 tables before it sends an SNMPv3 Inform message. The keys and tables are established using the information in the AP Reply. Refer to Section 11.3 PS Authentication Infrastructure.	CHPSWMS-12 MUST occur after CHPSWMS-11 completion.	Return to CHPSWMS-1. PS initiates operation of CDS.
CHPSWMS-13	SNMP Inform After the PS operating in SNMP Provisioning Mode establishes SNMPv3 keys, it MUST send an SNMPv3 INFORM (cabhPsDevProvEnrollTrap) requesting enrollment to the SNMP ENTITY whose IP address was provided in Option 177 suboption 3, in the DHCP ACK message.	CHPSWMS-13 MUST occur after CHPSWMS-12 completion.	Return to CHPSWMS-1.
CHPSWMS-14	SYSLOG message If the PS received a SYSLOG server address in the DHCP ACK, the PS MUST send the SYSLOG a "provisioning complete" message. This notification will include the pass-fail result of the provisioning operation. The general format of this message is defined in Table II-1 Defined Events for CableHome, Event ID 73001100 (see Message Notes and Details).	CHPSWMS-14 MUST occur after CHPSWMS-13 completion.	

EXHIBIT A

Flow Step	PS WAN-Man Provisioning: SNMP Provisioning Mode	Normal Sequence	Failure Sequence
CHPSWMS-15	SNMP Inform The PS MUST send the NMS an SNMP INFORM (cabhPsDevInitTrap) containing a "provisioning complete" notification. FAIL occurs when the Configuration File processing fails. Otherwise the provisioning state is PASS. The PS MUST update the value of cabhPsDevProvState with status 'pass' (1) when provisioning flow steps CHPSWMS-1 through CHPSWMS-15 complete successfully. The PS MUST update the value of cabhPsDevProvState with status 'fail' (3) and report an event indicating provisioning process failure if the PS Provisioning Timer expires before the value of cabhPsDevProvState is updated with status 'pass'.	CHPSWMS-15 MUST occur after CHPSWMS-14 completion.	If the PS does not receive a response to the Provisioning Complete inform, the PS MUST retry to send the cabhPsDevInitTrap inform, for a total of 5 attempts, at an interval of 10 seconds. If all 5 attempts to send the cabhPsDevInitTrap fail, the PS MUST re-start the initialization process: return to CHPSWMS-1 and report an error.
Optional Steps			
CHPSWMS-16	SNMP Get If any additional device capabilities are needed by the provisioning system, the provisioning system requests these from the PS via SNMPv3 Get Requests. Iterative: The NMS sends the PS one or more SNMPv3 GET requests to obtain any needed PS capability information. The Provisioning Application may use a GETBulk request to obtain several pieces of information in a single message.	CHPSWMS-16 is not expected to occur before CHPSWMS-15 completion.	Return to CHPSWMS- 1.
CHPSWMS-17	SNMP Get Response Iterative: The PS replies to the NMS Get-request or Get-bulk request messages with a Get Response for each Get Request. After all the Gets, or the GetBulk, finish, the NMS sends the requested data to the provisioning application.	If CHPSWMS-16 occurs, CHPSWMS-17 MUST occur after CHPSWMS-16 completes.	N/A
CHPSWMS-18	Configuration File Create Optional: The provisioning system uses information from PS provisioning steps CHPSWMS-16 and CHPSWMS-17 to create a PS configuration file. The provisioning system runs a hash on the contents of the configuration file. The hash is sent to the PS in the next step.	If CHPSWMS-17 occurs, CHPSWMS-18 MUST occur after CHPSWMS-17 completes.	N/A
CHPSWMS-19	SNMP Set The provisioning system might instruct the NMS to send an SNMP Set message to the PS containing the IP Address of the TFTP server, the PS Configuration File filename and the hash of the configuration file as described in Section 7.4.4.1 Configuration File Format Requirements (SNMP Provisioning Mode). Optionally, the IP Address of the Firewall Configuration File TFTP server, the Firewall Configuration File filename and the hash of the firewall Configuration File are included in the SNMP set if there is a firewall Configuration File to be loaded, and this method is selected to specify it.	If CHPSWMS-18 occurs, CHPSWMS-19 MUST occur after CHPSWMS-18 completes.	Return to CHPSWMS- 1 if the set was received, but there was a processing error.

EXHIBIT A

Flow Step	PS WAN-Man Provisioning: SNMP Provisioning Mode	Normal Sequence	Failure Sequence
CHPSWMS-20	TFTP Request If the NMS triggers the PS to download a PS Configuration File as described in Section 7.4.4.1, the PS sends the TFTP Server a TFTP Get Request to request the specified PS Configuration File.	If CHPSWMS-19 occurs, CHPSWMS-20 MUST occur after CHPSWMS-19 completes.	Continue with CHPSWMS-19.
CHPSWMS-21	TFTP server sends Configuration File After the PS receives the PS Configuration File, the PS calculates the hash of the PS Configuration File and compares it to the value received in step CHPSWMS-19. The PS then processes the PS Configuration File. Optionally, the IP Address of the Firewall Configuration File TFTP server, the Firewall Configuration File filename and the hash of the firewall configuration file are included in the PS Configuration File if there is a firewall Configuration File to be loaded, and this is the method selected to specify it.	If CHPSWMS-20 occurs, CHPSWMS-21 occurs after CHPSWMS-20 completes.	If the TFTP download fails, report an error, proceed to CHPSWMS-22, and continue to retry CHPSWMS-20 (continue to retry PS Configuration File download). If processing of the Configuration File produces an error, continue and report the error as an event.
CHPSWMS-22	TFTP Request - Firewall Configuration File (optional) The PS sends the Firewall Configuration TFTP Server a TFTP Get Request to request the specified firewall configuration data file.	If CHPSWMS-22 occurs, it MUST occur after CHPSWMS-21 completes.	Return to CHPSWMS- 1.
CHPSWMS-23	TFTP server sends Firewall Configuration File The TFTP Server sends the PS a TFTP Response containing the requested file. After the PS receives the Firewall Configuration File the PS calculates the hash of the Firewall Configuration File and compares it to the value received in step CHPSWMS-21. The file is then processed. Refer to Section for description of PS configuration file contents.	If CHPSWMS-22 occurs, CHPSWMS-23 MUST occur after CHPSWMS-22 completes.	If the TFTP download fails, continue with PS operation but report an error and continue to retry CHPSWMS-22. If processing of the firewall configuration file produces an error, continue and report the error as an event.

Notes to Table 13-3:

1. Steps CHPSWMS-5-CHPSWMS-8 are optional in some cases. Refer to Section 11 for details.
2. The SNMP Get and following SNMP Get Response operations are optional, depending on whether additional information is required to form a PS Configuration File, and also depending on whether a PS Configuration File is needed.

13.4.1 PS WAN-Man Configuration File Download

The PS operating in SNMP Provisioning Mode might contain sufficient factory default information to provide for operation of either or both LAN and WAN sides without a PS Configuration File being downloaded. If the PS is operating in SNMP Provisioning Mode the NMS might trigger the download of a PS Configuration File for initial provisioning to replace the factory defaults or to provide additional information.[141]

The firewall Configuration File contains information to provision the firewall function. The indication to download a firewall Configuration File will come in either the PS Configuration File or via an SNMP Set during initialization.

[141] Revised this paragraph per ECN CH1.1-N-03046 by GO on 07/07/03.

EXHIBIT A

13.4.2 PS Provisioning Timer

A provisioning timer is provided to ensure that the PS will continue to cycle through the provisioning process should any operation not complete. The timer object, cabhPsDevProvTimer, has a default initialization of 5 minutes.[142]

13.4.3 Provisioning Enrollment/Provisioning Complete Informs

For the PS operating in SNMP Provisioning Mode only, the provisioning enrollment inform (cabhPsDevProvEnrollTrap) enables the Provisioning Server to determine that the PS is ready for the PS Configuration File.

In either DHCP Provisioning Mode or SNMP Provisioning Mode, the provisioning complete trap (cabhPsDevInitTrap) indicates whether the provisioning sequence has completed successfully or not.

13.4.4 SYSLOG Provisioning

The syslog server IP address MUST be provisioned through the DHCP process. The syslog event will not be sent if the syslog server IP address is not configured.

13.4.5 Provisioning State and Error Reporting

As indicated in Table 13-1 and Table 13-3, failure of the steps in the provisioning process generally results in the process restarting at the first step, CHPSWMD-1 or CHPSWMS-1.

13.5 PS WAN-Data Provisioning Process

The PS requests zero or more WAN-Data network address(es) from the DHCP server in the cable network to be used for the exchange of data between elements connected to the Internet and LAN IP Devices.

There is no difference in PS WAN-Data operation between the DHCP and SNMP Provisioning Modes.

The following diagrams illustrate the message flows that are to be used to accomplish the provisioning of PS WAN-Data addresses. The provisioning process for the PS WAN-Data addresses is the same for the PS embedded with a DOCSIS cable modem as it is for the stand-alone PS.

If the provisioning process for the PS WAN-Data address(es) occurs, it MUST follow the sequence depicted in Table 13-6 and described in detail in Table 13-4.[143]

[142] Deleted two paragraphs below per ECN CH1.1-N-03046 by GO on 07/07/03.
[143] Revised Table 13-4 per ECN CH1.1-N-03046 by GO on 07/07/03.

EXHIBIT A

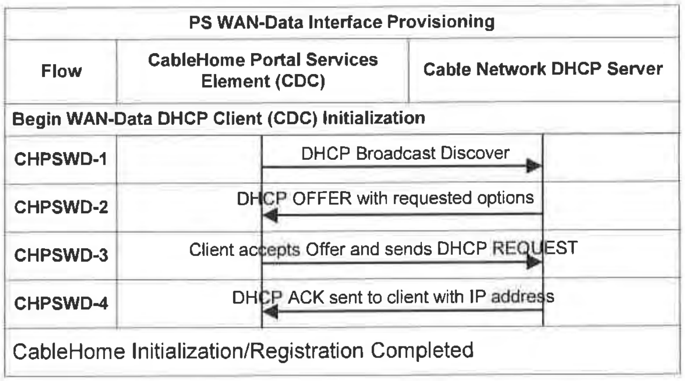

PS WAN-Data Interface Provisioning
Flow
CableHome Portal Services Element (CDC)
Cable Network DHCP Server
Begin WAN-Data DHCP Client (CDC) Initialization
CHPSWD-1
DHCP Broadcast Discover
CHPSWD-2
DHCP OFFER with requested options
CHPSWD-3
Client accepts Offer and sends DHCP REQUEST
CHPSWD-4
DHCP ACK sent to client with IP address
CableHome Initialization/Registration Completed

Figure 13-7 – PS WAN-Data Provisioning Process

Table 13-4 – Flow Descriptions for PS WAN-Data Provisioning Process

Flow Step	PS WAN-Data Address Provisioning	Normal Sequence	Failure Sequence
CHPSWD-1	DHCP Broadcast Discover The PS broadcasts a DHCP DISCOVER message including the mandatory options listed in Table 7-10, CDC DHCP Options in DISCOVER and REQUEST Messages.	Proceed to CHPSWD-2.	If failure per DHCP protocol repeat CHPSWD-1.
CHPSWD-2	DHCP OFFER The DHCP Server at the Headend receives the DHCP DISCOVER packet, assigns an IP address from the WAN-Data pool, builds a DHCP OFFER packet, and transmits the DHCP OFFER to the DHCP Relay Agent [RFC 3046] in the CMTS.	Proceed to CHPSWD-3.	If failure, the client will time out per DHCP protocol and CHPSWD-1 will be repeated.
CHPSWD-3	DHCP REQUEST The CDP sends a DHCP REQUEST message to the selected DHCP server to accept the DHCP OFFER in accordance with client requirements of [RFC 2131].	CHPSWD-3 MUST occur after CHPSWD-2 completion.	If failure per DHCP protocol return to CHPSWD-1.
CHPSWD-4	DHCP ACK The DHCP server sends the CDP a DHCP ACK message which contains the IPv4 address for the PS WAN Data interface.	CHPSWD-4 MUST occur after CHPSWD-3 completion. Provisioning complete with completion of CHPSWD-4.	If failure per DHCP protocol return to CHPSWD-1.

13.6 Provisioning Process: BP in the LAN-Trans Realm

CableHome Boundary Point (BP) logical elements are required to implement two protocols used during their provisioning process: DHCP [RFC 2131] and BP_Init messaging, defined in Section 6.5.3.2 MBP LAN Messaging Function.

The CDP (CDS) function of the PS element responds to DHCP messages issued by BPs in the LAN-Pass realm according to the requirements defined in Section 7.3.3.1.4 CDS Function Requirements. The PS

EXHIBIT A

CMP function responds to the BP_Init message received from BPs. This is described in Section 6.3.3.4 CMP LAN Messaging Function.

This section describes the provisioning process for the case where the NMS has provisioned the PS to operate in C-NAT or C-NAPT Primary Packet Handling mode (see Section 8). There is no difference in LAN-Trans realm BP provisioning process between the DHCP and SNMP Provisioning Modes.

The provisioning process for a BP in the LAN-Trans realm MUST occur via the sequence depicted in Figure 13-8 and described in detail in Table 13-5.[144] [145]

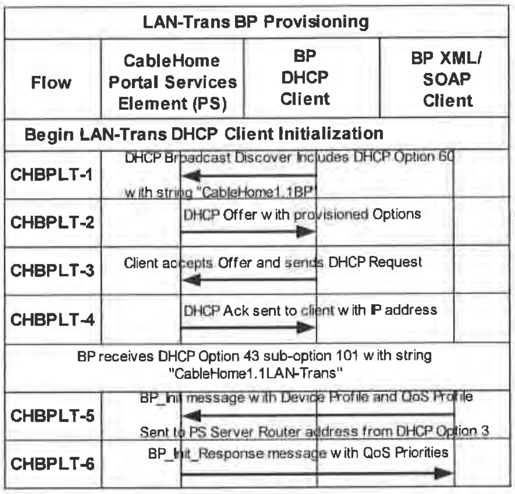

LAN-Trans BP Provisioning
Flow
CableHome Portal Services Element (PS)
BP DHCP Client
BP XML/ SOAP Client
Begin LAN-Trans DHCP Client Initialization
CHBPLT-1
DHCP Broadcast Discover Includes DHCP Option 60 with string "CableHome1.1BP"
CHBPLT-2
DHCP Offer with provisioned Options
CHBPLT-3
Client accepts Offer and sends DHCP Request
CHBPLT-4
DHCP Ack sent to client with IP address
BP receives DHCP Option 43 sub-option 101 with string "CableHome1.1LAN-Trans"
CHBPLT-5
BP_Init message with Device Profile and QoS Profile Sent to PS Server Router address from DHCP Option 3
CHBPLT-6
BP_Init_Response message with QoS Priorities

Figure 13-8 – Provisioning Process for a BP in the LAN-Trans Realm

[144] Revised Figure 13-8 and Table 13-5 per ECN CH1.1-N-03046 by GO on 07/07/03.
[145] Revised Table 13-5 per ECN CH1.1-N-03.0091-1 by GO on 12/5/03.

EXHIBIT A

Table 13-5 – Flow Descriptions for LAN-Trans BP Provisioning Process

Flow Step	Client LAN-Trans Address Provisioning	Normal Sequence	Failure Sequence
CHBPLT-1	DHCP Broadcast Discover The DHCP Client[1] sends a broadcast DHCP DISCOVER message on its local LAN[2]. The BP is required to include DHCP Option 60 containing string "CableHome1.1BP"	Proceed to CHBPLT-2.	If failure per DHCP protocol repeat CHBPLT -1.
CHBPLT-2	DHCP Offer The PS receives the DHCPDISCOVER message on its LAN interface and examines the chaddr field. If: - there is a LAN-Trans address available, and - there is no administrative consideration which motivates denying the LAN-Trans address to the client then the PS sends a DHCP OFFER message to the client to offer it the LAN-Trans address as either unicast or link-specific broadcast (according to the BROADCAST bit of the flags field of the DHCP DISCOVER). If the DHCP discover included DHCP Option 60 containing the string"CableHome1.1BP" the PS is required to include DHCP Option 43 sub-option 101 containing the string"CableHome1.1LANTrans" in the DHCP Offer message.	Proceed to CHBPLT-3.	If failure, the client will time out per DHCP protocol and CHBPLT -1 will be repeated.
CHBPLT-3	DHCP Request The LAN IP Device's DHCP client receives the DHCP OFFER message. When a LAN IP Device's DHCP client wishes to accept a DHCP OFFER, it is expected that it will format and send a DHCP REQUEST packet using link-specific broadcast according to [RFC 2131].	Proceed to CHBPLT-4.	If failure, the client will time out per DHCP protocol and CHBPLT -1 will be repeated.
CHBPLT-4	DHCP ACK The PS receives the DHCP REQUEST on its LAN interface. If the indicated LAN-Trans address is still assignable, the PS then sends DHCP ACK to the client as either unicast or link-specific broadcast (according to the BROADCAST bit of the flags field of the DHCP REQUEST). The DHCP ACK includes DHCP Option 43 sub-option 101 with the string "CableHome1.1LAN-Trans". This is an indication to the BP that it is in the LAN-Trans address realm and received the PS Server Router IP address in DHCP Option 3. The BP is therefore required to send its BP_Init messages to the PS Server Router IP address.	Proceed to CHBPLT-5.	If failure, the client will time out per DHCP protocol and CHBPLT -1 will be repeated.
CHBPLT-5	BP_Init The BP sends a BP_Init SOAP/XML message with its Device and QoS Profiles to the PS Server Router IP address.	Proceed to CHBPLT-6.	If the BP does not receive BP_Init_Response, it retries BP_Init for a total of three attempts
CHBPLT-6	BP_Init_Response The PS sends a BP_Init_Response SOAP/XML message to the BP.	Provisioning Complete.	

[1] If the client is aware of its previous IP address (e.g., following reboot), it may omit the DHCPDISCOVER and proceed with step 3.

[2] If the client is located on a non-broadcast network it is expected to unicast the message to the DHCP Server.

EXHIBIT A

13.7 Provisioning Process: LAN IP Device in the LAN-Pass Realm

Some home LAN applications will not function properly with a translated network address. To accommodate these applications CableHome enables the PS to operate in Passthrough (transparent bridging) mode. As described in Section 8.3.3.1 Packet Handling Modes, bridging occurs when the cable network NMS sets the Primary Packet-handling mode (cabhCapPrimaryMode) to Passthrough, or by writing individual LAN IP Device MAC addresses into the Passthrough Table (cabhCapPassthroughTable). Figure 13-9 describes the process for the request and assignment of a network address to LAN IP Devices for which the PS has been pre-provisioned to bridge traffic. When the PS has been configured to bridge traffic for a LAN IP Device, DHCP DISCOVERs and DHCP REQUESTs issued by that LAN IP Device will be served by the cable network DHCP server, not by the CDS.

A non-CableHome compliant LAN IP Device is assumed to implement a DHCP client and request an IP address lease using DHCP [RFC 2131]. A CableHome compliant LAN IP Device, i.e., one that implements BP functionality defined in this specification, is required to implement a DHCP client and request an IP address lease via DHCP. The BP logical element of a CableHome compliant LAN IP Device is also required to exchange BP_Init messaging with the PS, as described in Section 6.5.3.2 MBP LAN Messaging Function. This section describes the required BP messaging. The DHCP messaging assumed to occur between a non-compliant LAN IP Device and a DHCP server will typically follow the first four steps of the required BP DHCP messaging. However, a non-compliant LAN IP Device is not likely to include the DHCP Option 61 string "CableHome 1.1 BP <*hardware address*>".

The provisioning process for a BP in the LAN-Pass realm is required to occur via the sequence depicted in Figure 13-9 and described in detail in Table 13-6.[146]

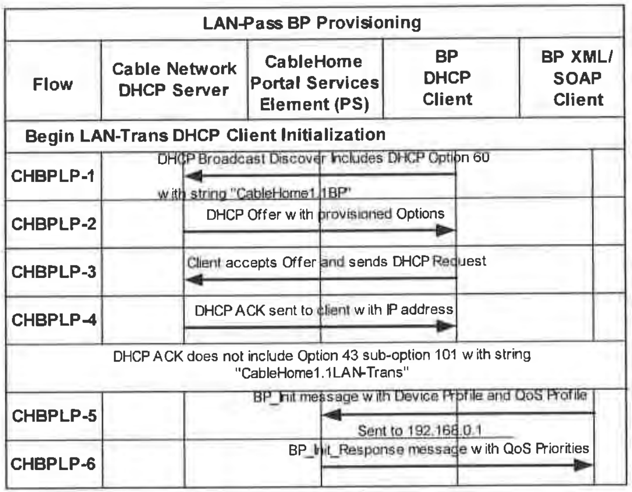

LAN-Pass BP Provisioning
Flow
Cable Network DHCP Server
CableHome Portal Services Element (PS)
BP DHCP Client
BP XML/ SOAP Client
Begin LAN-Trans DHCP Client Initialization
CHBPLP-1
DHCP Broadcast Discover Includes DHCP Option 60
with string "CableHome1.1BP"
CHBPLP-2
DHCP Offer with provisioned Options
CHBPLP-3
Client accepts Offer and sends DHCP Request
CHBPLP-4
DHCP ACK sent to client with IP address
DHCP ACK does not include Option 43 sub-option 101 with string "CableHome1.1LAN-Trans"
CHBPLP-5
BP_Init message with Device Profile and QoS Profile
Sent to 192.168.0.1
CHBPLP-6
BP_Init_Response message with QoS Priorities

Figure 13-9 – Provisioning Process for BP in the LAN-Pass Realm

[146] Revised Figure 13-9 and Table 13-6 per ECN CH1.1-N-03046 by GO on 07/07/03

EXHIBIT A

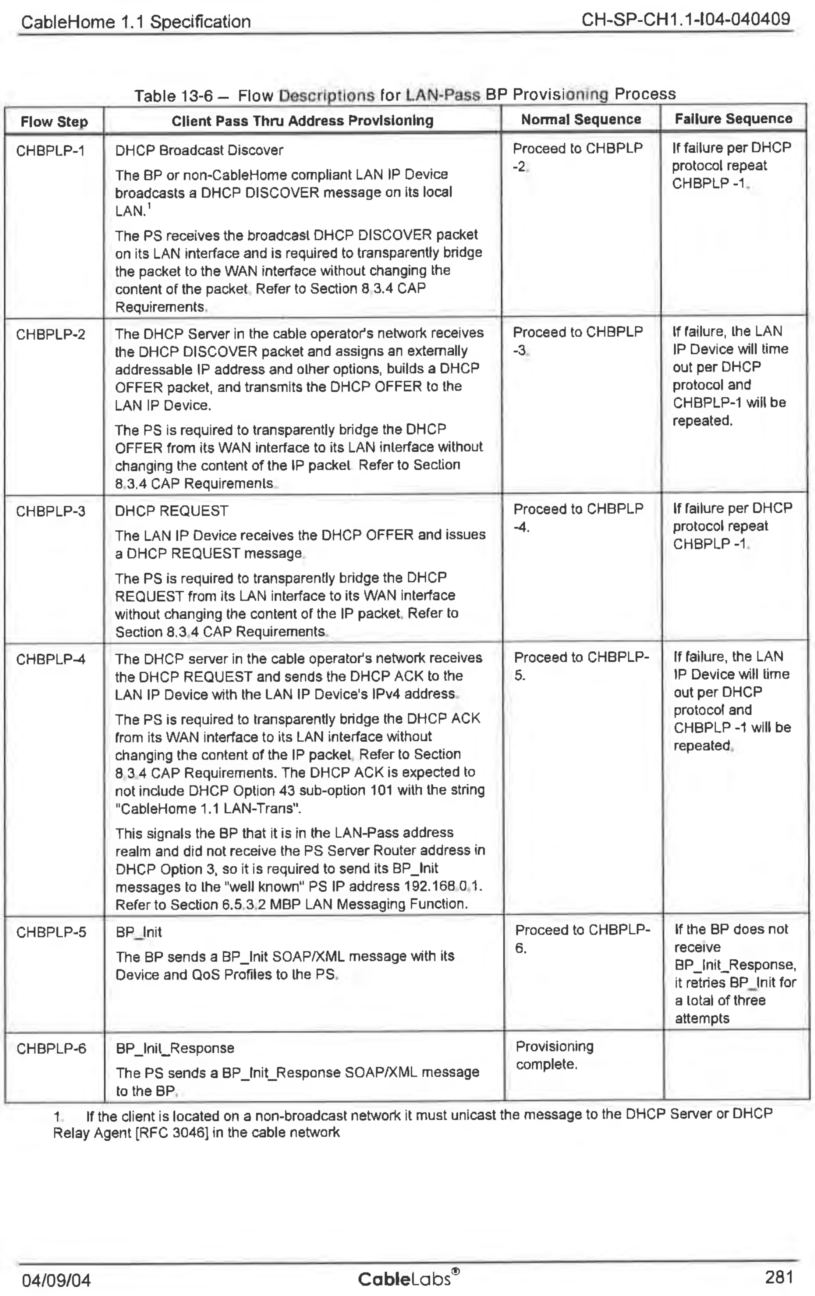


Table 13-6 – Flow Descriptions for LAN-Pass BP Provisioning Process

Flow Step	Client Pass Thru Address Provisioning	Normal Sequence	Failure Sequence
CHBPLP-1	DHCP Broadcast Discover The BP or non-CableHome compliant LAN IP Device broadcasts a DHCP DISCOVER message on its local LAN.[1] The PS receives the broadcast DHCP DISCOVER packet on its LAN interface and is required to transparently bridge the packet to the WAN interface without changing the content of the packet. Refer to Section 8.3.4 CAP Requirements.	Proceed to CHBPLP -2.	If failure per DHCP protocol repeat CHBPLP -1.
CHBPLP-2	The DHCP Server in the cable operator's network receives the DHCP DISCOVER packet and assigns an externally addressable IP address and other options, builds a DHCP OFFER packet, and transmits the DHCP OFFER to the LAN IP Device. The PS is required to transparently bridge the DHCP OFFER from its WAN interface to its LAN interface without changing the content of the IP packet. Refer to Section 8.3.4 CAP Requirements.	Proceed to CHBPLP -3.	If failure, the LAN IP Device will time out per DHCP protocol and CHBPLP-1 will be repeated.
CHBPLP-3	DHCP REQUEST The LAN IP Device receives the DHCP OFFER and issues a DHCP REQUEST message. The PS is required to transparently bridge the DHCP REQUEST from its LAN interface to its WAN interface without changing the content of the IP packet. Refer to Section 8.3.4 CAP Requirements.	Proceed to CHBPLP -4.	If failure per DHCP protocol repeat CHBPLP -1.
CHBPLP-4	The DHCP server in the cable operator's network receives the DHCP REQUEST and sends the DHCP ACK to the LAN IP Device with the LAN IP Device's IPv4 address. The PS is required to transparently bridge the DHCP ACK from its WAN interface to its LAN interface without changing the content of the IP packet. Refer to Section 8.3.4 CAP Requirements. The DHCP ACK is expected to not include DHCP Option 43 sub-option 101 with the string "CableHome 1.1 LAN-Trans". This signals the BP that it is in the LAN-Pass address realm and did not receive the PS Server Router address in DHCP Option 3, so it is required to send its BP_Init messages to the "well known" PS IP address 192.168.0.1. Refer to Section 6.5.3.2 MBP LAN Messaging Function.	Proceed to CHBPLP-5.	If failure, the LAN IP Device will time out per DHCP protocol and CHBPLP -1 will be repeated.
CHBPLP-5	BP_Init The BP sends a BP_Init SOAP/XML message with its Device and QoS Profiles to the PS.	Proceed to CHBPLP-6.	If the BP does not receive BP_Init_Response, it retries BP_Init for a total of three attempts
CHBPLP-6	BP_Init_Response The PS sends a BP_Init_Response SOAP/XML message to the BP.	Provisioning complete.	

[1] If the client is located on a non-broadcast network it must unicast the message to the DHCP Server or DHCP Relay Agent [RFC 3046] in the cable network

EXHIBIT A

Appendix I MIB Objects[147]

This appendix lists all MIB objects required by CableHome 1.1, as indicated in Section 6.3.3.1.4.1, *SNMP Protocol Requirements* and Section 6.3.3.1.4.7, *CableHome MIB Requirements*, and indicates requirement for persistence of each listed object.

The term 'persistent' as it applies to this Appendix is defined below:

> *Persistent*: The requirement for the PS to retain the value of a configurable (by the manager or by the PS itself) MIB object across a PS reboot or reset.

For MIB objects with entry 'Yes' in the Persistent column, the object's value immediately following a PS reboot or reset, MUST be the same as its value immediately preceding the reboot or reset.

For MIB objects with entry 'No' in the Persistent column, the object's value MUST be set to its factory default value (DEFVAL) or, if it has no default value, it MUST be set to zero or null as appropriate, immediately following a PS reboot or reset.

For MIB objects with entry "-" in the Persistent column, one of the following apply:

- the value of the object immediately following PS reboot, or reset is left to vendor implementation because there is no specific requirement for its value following PS reboot or reset, or
- the value of the object is deterministic, based upon the MIB description. (the object's value is fixed or can be derived from known values after the PS reboot or reset)

MIB NAME/Parameter	Max-Access	Persistent	# of Persistent Entries
mib-2[RFC 1213] **system**			
sysDescr	read-only	-	N/A
sysObjectID	read-only	-	N/A
sysUpTime	read-only	-	N/A
sysContact	read-write	Yes	1
sysName	read-write	Yes	1
sysLocation	read-write	Yes	1
sysServices	read-only	-	N/A
Interfaces [RFC 2863]			
ifNumber	read-only	-	N/A
ifTable/ifEntry			
ifIndex	read-only	-	N/A
ifDescr	read-only	-	N/A
ifType	read-only	-	N/A
ifMtu	read-only	-	N/A

[147] Revised matrix per ECN CH1.1-N-03035, CH1.1-N-03051, CH1.1-N-03059, and CH1.1-N-03.0105-2 by GO on 07/3/03, 07/7/03, 07/31/03, and 12/5/03.

EXHIBIT A

MIB NAME/Parameter	Max-Access	Persistent	# of Persistent Entries
ifSpeed	read-only	-	N/A
ifPhysAddress	read-only	-	N/A
ifAdminStatus	read-write	No	N/A
ifOperStatus	read-only	-	N/A
ifLastChange	read-only	-	N/A
ifInOctets	read-only	-	N/A
ifInUcastPkts	read-only	-	N/A
ifInDiscards	read-only	-	N/A
ifInErrors	read-only	-	N/A
ifInUnknownProtos	read-only	-	N/A
ifOutOctets	read-only	-	N/A
ifOutUcastPkts	read-only	-	N/A
ifOutDiscards	read-only	-	N/A
ifOutErrors	read-only	-	N/A
ip [RFC 2011]			
ipForwarding	read-write	No	N/A
ipDefaultTTL	read-write	No	N/A
ipInReceives	read-only	-	N/A
ipInHdrErrors	read-only	-	N/A
ipInAddrErrors	read-only	-	N/A
ipForwDatagrams	read-only	-	N/A
ipInUnknownProtos	read-only	-	N/A
ipInDiscards	read-only	-	N/A
ipInDelivers	read-only	-	N/A
ipOutRequests	read-only	-	N/A
ipOutDiscards	read-only	-	N/A
ipOutNoRoutes	read-only	-	N/A
ipReasmTimeout	read-only	-	N/A
ipReasmReqds	read-only	-	N/A
ipReasmOKs	read-only	-	N/A
ipReasmFails	read-only	-	N/A
ipFragOKs	read-only	-	N/A
ipFragFails	read-only	-	N/A
ipFragCreates	read-only	-	N/A
ipNetToMediaTable/ipNetToMediaEntry			
ipNetToMediaIfIndex	read-only	No	N/A
ipNetToMediaPhyAddress	read-only	No	N/A
ipNetToMediaNetAddress	read-only	No	N/A
ipNetToMediaType	read-only	No	N/A
icmp			
icmpInMsgs	read-only	-	N/A
icmpInErrors	read-only	-	N/A
icmpInDestUnreachs	read-only	-	N/A
icmpInTimeExcds	read-only	-	N/A

EXHIBIT A

MIB NAME/Parameter	Max-Access	Persistent	# of Persistent Entries
icmpInParmProbs	read-only	-	N/A
icmpInSrcQuenchs	read-only	-	N/A
icmpInRedirects	read-only	-	N/A
icmpInEchos	read-only	-	N/A
icmpInEchosReps	read-only	-	N/A
icmpInTimestamps	read-only	-	N/A
icmpInTimestampsReps	read-only	-	N/A
icmpInAddrMasks	read-only	-	N/A
icmpInAddrMaskReps	read-only	-	N/A
icmpOutMsgs	read-only	-	N/A
icmpOutErrors	read-only	-	N/A
icmpOutDestUnreachs	read-only	-	N/A
icmpOutTimeExcds	read-only	-	N/A
icmpOutParmProbs	read-only	-	N/A
icmpOutSrcQuenchs	read-only	-	N/A
icmpOutRedirects	read-only	-	N/A
icmpOutEchos	read-only	-	N/A
icmpOutEchosReps	read-only	-	N/A
icmpOutTimestamps	read-only	-	N/A
icmpOutTimestampReps	read-only	-	N/A
icmpOutAddrMasks	read-only	-	N/A
icmpOutAddrMaskReps	read-only	-	N/A
udp [RFC 2013]			
udpInDatagrams	read-only	-	N/A
udpNoPorts	read-only	-	N/A
udpInErrors	read-only	-	N/A
udpOutDatagrams	read-only	-	N/A
udpTable/udpEntry			
udpLocalAddress	read-only	-	N/A
udpLocalPort	read-only	-	N/A
transmission [draft-ietf-ipcdn-bpiplus-mib-05] **docsIfMib** **docsBpi2MIB** **docsBpi2MIBObjects** **docsBpi2CmObjects** **docsBpi2CmCertObjects**			
docsBpi2CodeDownloadGroup			
docsBpi2CodeDownloadStatusCode	read-only	-	N/A
docsBpi2CodeDownloadStatusString	read-only	-	N/A
docsBpi2CodeMfgOrgName	read-only	-	N/A
docsBpi2CodeMfgCodeAccessStart	read-only	-	N/A
docsBpi2CodeMfgCvcAccessStart	read-only	-	N/A
docsBpi2CodeCoSignerOrgName	read-only	-	N/A
docsBpi2CodeCoSignerCodeAccessStart	read-only	-	N/A

EXHIBIT A

MIB NAME/Parameter	Max-Access	Persistent	# of Persistent Entries
docsBpi2CodeCoSignerCvcAccessStart	read-only	-	N/A
docsBpi2CodeCvcUpdate	read-write	Yes	1
snmp [RFC 3418]			
snmpInPkts	read-only	-	N/A
snmpInBadVersions	read-only	-	N/A
snmpInBadCommunityNames	read-only	-	N/A
snmpInBadCommunityUses	read-only	-	N/A
snmpInASNParseErrs	read-only	-	N/A
snmpEnableAuthenTraps	read-write	No	N/A
snmpSilentDrops	read-only	-	N/A
IfMIB [RFC 2863] **IfMIBObjects**			
ifXTable/ifXEntry			
ifName	read-only	-	N/A
ifInMulticastPkts	read-only	-	N/A
ifInBroadcastPkts	read-only	-	N/A
ifOutMulticastPkts	read-only	-	N/A
ifOutBroadcastPkts	read-only	-	N/A
ifLinkUpDownTrapEnable	read-write	No	N/A
ifHighSpeed	read-only	-	N/A
ifPromiscuousMode	read-write	No	N/A
ifConnectorPresent	read-only	-	N/A
ifAlias	read-write	No	N/A
ifCounterDiscontinuityTime	read-only	-	N/A
ifStackTable/ifStackEntry			
ifStackHigherLayer	read-only	-	N/A
ifStackLowerLayer	read-only	-	N/A
ifStackStatus	read-only	-	N/A
docsDev [RFC 2669] **docsDevMIBObjects**			
docsDevNmAccessTable/docsDevNmAccessEntry			
docsDevNmAccessIndex	not-accessible	-	N/A
docsDevNmAccessIp	read-create	No	N/A
docsDevNmAccessIpMask	read-create	No	N/A
docsDevNmAccessCommunity	read-create	No	N/A
docsDevNmAccessControl	read-create	No	N/A
docsDevNmAccessInterfaces	read-create	No	N/A
docsDevNmAccessStatus	read-create	No	N/A
docsDevNmAccessTrapVersion	read-create	No	N/A

EXHIBIT A

MIB NAME/Parameter	**Max-Access**	**Persistent**	**# of Persistent Entries**
docsDevSoftware			
docsDevSwServer	read-write	Yes	1
docsDevSwFilename	read-write	Yes	1
docsDevSwAdminStatus	read-write	Yes	1
docsDevSwOperStatus	read-only	Yes	1
docsDevSwCurrentVers	read-only	-	N/A
docsDevEvent			
docsDevEvControl	read-write	No	N/A
docsDevEvSyslog	read-write	No	N/A
docsDevEvThrottleAdminStatus	read-write	No	N/A
docsDevEvThrottleInhibited	read-only	-	N/A
docsDevEvThrottleThreshold	read-write	No	N/A
docsDevEvThrottleInterval	read-write	No	N/A
docsDevEvControlTable/docsDevEvControlEntry			
docsDevEvPriority	not-accessible	-	N/A
docsDevEvReporting	read-write	No	N/A
docsDevEventTable/docsDevEventEntry			
docsDevEvIndex	not-accessible	-	N/A
docsDevEvFirstTime	read-only	Yes	10
docsDevEvLastTime	read-only	Yes	10
docsDevEvCounts	read-only	Yes	10
docsDevEvLevel	read-only	Yes	10
docsDevEvId	read-only	Yes	10
docsDevEvText	read-only	Yes	10
docsDevFilter			
docsDevFilterIpTable/docsDevFilterIpEntry			
docsDevFilterIpIndex	not-accessible	-	N/A
docsDevFilterIpStatus	read-create	Yes	20
docsDevFilterIpControl	read-create	Yes	20
docsDevFilterIpIfIndex	read-create	Yes	20
docsDevFilterIpDirection	read-create	Yes	20
docsDevFilterIpBroadcast	read-create	No	N/A
docsDevFilterIpSaddr	read-create	Yes	20
docsDevFilterIpSmask	read-create	Yes	20
docsDevFilterIpDaddr	read-create	Yes	20
docsDevFilterIpDmask	read-create	Yes	20
docsDevFilterIpProtocol	read-create	Yes	20
docsDevFilterIpSourcePortLow	read-create	Yes	20
docsDevFilterIpSourcePortHigh	read-create	Yes	20
docsDevFilterIpDestPortLow	read-create	Yes	20
docsDevFilterIpDestPortHigh	read-create	Yes	20
docsDevFilterIpMatches	read-only	-	N/A

EXHIBIT A

MIB NAME/Parameter	Max-Access	Persistent	# of Persistent Entries
docsDevFilterIpTos	read-create	No	N/A
docsDevFilterIpTosMask	read-create	No	N/A
docsDevFilterIpContinue	read-only	-	N/A
docsDevFilterIpPolicyId	read-create	No	N/A
private **enterprises** **cableLabs** **clabProject** **clabProjCableHome** **cabhPsDevMib** **cabhPsDevBase**			
cabhPsDevDateTime	read-write	No	N/A
cabhPsDevResetNow	read-write	No	N/A
cabhPsDevSerialNumber	read-only	-	N/A
cabhPsDevHardwareVersion	read-only	-	N/A
cabhPsDevWanManMacAddress	read-only	-	N/A
cabhPsDevWanDataMacAddress	read-only	-	N/A
cabhPsDevTypeIdentifier	read-only	-	N/A
cabhPsDevSetToFactory	read-write	No	N/A
cabhPsDevTodSyncStatus	read-only	-	N/A
cabhPsDevProvMode	read-only	-	N/A
cabhPsDevLastSetToFactory	read-only	-	N/A
cabhPsDevProv			
cabhPsDevProvisioningTimer	read-write	No	N/A
cabhPsDevProvConfigFile	read-write	No	N/A
cabhPsDevProvConfigHash	read-write	No	N/A
cabhPsDevProvConfigFileSize	read-only	-	N/A
cabhPsDevProvConfigFileStatus	read-only	-	N/A
cabhPsDevProvConfigTLVProcessed	read-only	-	N/A
cabhPsDevProvConfigTLVRejected	read-only	-	N/A
cabhPsDevProvSolicitedKeyTimeout	read-write	Yes	1
cabhPsDevProvState	read-only	-	N/A
cabhPsDevProvAuthState	read-only	-	N/A
cabhPsDevTimeServerAddrType	read-only	-	N/A
cabhPsDevTimeServerAddr	read-only	-	N/A
cabhPsDevAttrib **cabhPsDevPsAttrib**			
cabhPsDevPsDeviceType	read-only	-	N/A
cabhPsDevPsManufacturerURL	read-only	-	N/A
cabhPsDevPsModelURL	read-only	-	N/A
cabhPsDevPsModelUPC	read-only	-	N/A
cabhPsDevAttrib **cabhPsDevBpAttrib**			

EXHIBIT A

MIB NAME/Parameter	Max-Access	Persistent	# of Persistent Entries
cabhPsDevBpProfileTable/ cabhPsDevBpProfileEntry			
cabhPsDevBpIndex	not-accessible	-	N/A
cabhPsDevBpDeviceType	read-only	-	N/A
cabhPsDevBpManufacturer	read-only	-	N/A
cabhPsDevBpManufacturerURL	read-only	-	N/A
cabhPsDevBpSerialNumber	read-only	-	N/A
cabhPsDevBpHardwareVersion	read-only	-	N/A
cabhPsDevBpHardwareOptions	read-only	-	N/A
cabhPsDevBpModelName	read-only	-	N/A
cabhPsDevBpModelNumber	read-only	-	N/A
cabhPsDevBpModelURL	read-only	-	N/A
cabhPsDevBpModelUPC	read-only	-	N/A
cabhPsDevBpModelSoftwareOs	read-only	-	N/A
cabhPsDevBpModelSoftwareVersion	read-only	-	N/A
cabhPsDevBpLanInterfaceType	read-only	-	N/A
cabhPsDevBpNumberInterfacePriorities	read-only	-	N/A
cabhPsDevBpPhysicalLocation	read-only	-	N/A
cabhPsDevBpPhysicalAddress	read-only	-	N/A
cabhPsDevPsStats			
cabhPsDevLanIpTrafficCountersReset	read-write	No	N/A
cabhPsDevLanIpTrafficCountersLastReset	read-only	-	N/A
cabhPsDevLanIpTrafficEnabled	read-write	No	N/A
cabhPsDevLanIpTrafficTable/cabhPsDevLanIpTrafficEntry			
cabhPsDevLanIpTrafficIndex	not-accessible	-	N/A
cabhPsDevLanIpTrafficInetAddressType	read-only	-	N/A
cabhPsDevLanIpTrafficInetAddress	read-only	-	N/A
cabhPsDevLanIpTrafficInOctets	read-only	-	N/A
cabhPsDevLanIpTrafficOutOctets	read-only	-	N/A
cabhSecMib			
cabhSecCertObjects			
cabhSecCertPsCert	read-only	-	1
cabhSec2FwObjects **cabhSec2FwBase**			
cabhSec2FwEnable	read-write	Yes	N/A
cabhSec2FwPolicyFileURL	read-write	No	N/A
cabhSec2FwPolicyFileHash	read-write	No	N/A
cabhSec2FwPolicyFileOperStatus	read-only	-	N/A
cabhSec2FwPolicyFileCurrentVersion	read-write	Yes	N/A
cabhSec2FwClearPreviousRuleset	read-write	No	N/A
cabhSec2FwPolicySelection	read-write	Yes	N/A
cabhSec2FwEventSetToFactory	read-write	No	N/A

EXHIBIT A

MIB NAME/Parameter	Max-Access	Persistent	# of Persistent Entries
cabhSec2FwEventLastSetToFactory	read-only	-	N/A
cabhSec2FwPolicySuccessfulFileURL	read-only	Yes	1
cabhSec2FwEvent			
cabhSec2FwEventControlTable/			
cabhSec2FwEventControlEntry/			
cabhSec2FwEventType	not-accessible	-	N/A
cabhSec2FwEventEnable	read-write	No	N/A
cabhSec2FwEventThreshold	read-write	No	N/A
cabhSec2FwEventInterval	read-write	No	N/A
cabhSec2FwEventCount	read-only	-	N/A
cabhSec2FwEventLogReset	read-write	No	N/A
cabhSec2FwEventLogLastReset	read-only	-	N/A
cabhSec2FwLogTable/			
cabhSec2FwLogEntry			
cabhSec2FwLogIndex	not-accessible	-	N/A
cabhSec2FwLogEventType	read-only	-	N/A
cabhSec2FwLogEventPriority	read-only	-	N/A
cabhSec2FwLogEventId	read-only	-	N/A
cabhSec2FwLogTime	read-only	-	N/A
cabhSec2FwLogIpProtocol	read-only	-	N/A
cabhSec2FwLogIpSourceAddr	read-only	-	N/A
cabhSec2FwLogIpDestAddr	read-only	-	N/A
cabhSec2FwLogIpSourcePort	read-only	-	N/A
cabhSec2FwLogIpDestPort	read-only	-	N/A
cabhSec2FwLogMessageType	read-only	-	N/A
cabhSec2FwLogReplayCount	read-only	-	N/A
cabhSec2FwLogMIBPointer	read-only	-	N/A
cabhSec2FwFilter			
cabhSec2FwFilterScheduleTable/			
cabhSec2FwFilterScheduleEntry			
cabhSec2FwFilterScheduleStartTime	read-create	Yes	1
cabhSec2FwFilterScheduleEndTime	read-create	Yes	1
cabhSec2FwFilterScheduleDOW	read-create	Yes	1
cabhSec2FwFactoryDefault			
cabhSec2FwFactoryDefaultTable/			
cabhSec2FwFactoryDefaultEntry			
cabhSec2FwFactoryDefaultIndex	not-accessible		
cabhSec2FwFactoryDefaultControl		-	N/A

EXHIBIT A

MIB NAME/Parameter	Max-Access	Persistent	# of Persistent Entries
cabhSec2FwFactoryDefaultIfIndex		-	N/A
cabhSec2FwFactoryDefaultDirection		-	N/A
cabhSec2FwFactoryDefaultSaddr		-	N/A
cabhSec2FwFactoryDefaultSmask		-	N/A
cabhSec2FwFactoryDefaultDaddr		-	N/A
cabhSec2FwFactoryDefaultDmask		-	N/A
cabhSec2FwFactoryDefaultProtocol		-	N/A
cabhSec2FwFactoryDefaultSourcePortLow		-	N/A
cabhSec2FwFactoryDefaultSourcePortHigh		-	N/A
cabhSec2FwFactoryDefaultDestPortLow		-	N/A
cabhSec2FwFactoryDefaultDestPortHigh		-	N/A
cabhSec2FwFactoryDefaultIFilterContinue		-	N/A
cabhSecKerbBase			
cabhSecKerbPKINITGracePeriod	read-write	No	N/A
cabhSecKerbTGSGracePeriod	read-write	No	N/A
cabhSecKerbUnsolicitedKeyMaxTimeout	read-write	No	N/A
cabhSecKerbUnsolicitedKeyMaxRetries	read-write	No	N/A
cabhCapMib **cabhCapObjects** **cabhCapBase**			
cabhCapTcpTimeWait	read-write	No	N/A
cabhCapUdpTimeWait	read-write	No	N/A
cabhCapIcmpTimeWait	read-write	No	N/A
cabhCapPrimaryMode	read-write	No	N/A
cabhCapSetToFactory	read-write	No	N/A
cabhCapLastSetToFactory	read-only	-	N/A
cabhCapMap			
cabhCapMappingTable/cabhCapMappingEntry			
cabhCapMappingIndex	not-accessible	-	N/A
cabhCapMappingWanAddrType	read-create	Yes[1]	16
cabhCapMappingWanAddr	read-create	Yes[1]	16
cabhCapMappingWanPort	read-create	Yes[1]	16
cabhCapMappingLanAddrType	read-create	Yes[1]	16
cabhCapMappingLanAddr	read-create	Yes[1]	16
cabhCapMappingLanPort	read-create	Yes[1]	16
cabhCapMappingMethod	read-only	-	N/A
cabhCapMappingProtocol	read-create	Yes[1]	16
cabhCapMappingRowStatus	read-create	Yes	16
cabhCapPassthroughTable/cabhCapPassthroughEntry			
cabhCapPassthroughIndex	not-accessible	-	N/A
cabhCapPassthroughMacAddr	read-create	Yes	16
cabhCapPassthroughRowStatus	read-create	Yes	16

EXHIBIT A

MIB NAME/Parameter	Max-Access	Persistent	# of Persistent Entries
[1] cabhCapMappingEntry objects are persistent if provisioned by the NMS and non-persistent if created dynamically based on outbound traffic. Refer to Section 8.3.4.4.			
cabhCdpMib			
cabhCdpObjects			
cabhCdpBase			
cabhCdpSetToFactory	read-write	No	N/A
cabhCdpLanTransCurCount	read-only	-	N/A
cabhCdpLanTransThreshold	read-write	No	N/A
cabhCdpLanTransAction	read-write	No	N/A
cabhCdpWanDataIpAddrCount	read-write	No	N/A
cabhCdpLastSetToFactory	read-only	-	N/A
cabhCdpAddr			
cabhCdpLanAddrTable/cabhCdpLanAddrEntry			
cabhCdpLanAddrIpType	not-accessible	-	N/A
cabhCdpLanAddrIp	not-accessible	-	N/A
cabhCdpLanAddrClientID	read-create	Yes	16
cabhCdpLanAddrLeaseCreateTime	read-only	-	N/A
cabhCdpLanAddrLeaseExpireTime	read-only	-	N/A
cabhCdpLanAddrMethod	read-only	Yes	16
cabhCdpLanAddrHostName	read-only	Yes	16
cabhCdpLanAddrRowStatus	read-create	Yes	16
cabhCdpWanDataAddrTable/cabhCdpWanDataAddrEntry			
CabhCdpWanDataAddrIndex	not-accessible	-	N/A
CabhCdpWanDataAddrClientId	read-create	No	N/A
CabhCdpWanDataAddrIpType	read-only	-	N/A
CabhCdpWanDataAddrIp	read-only	-	N/A
CabhCdpWanDataAddrRowStatus	read-create	No	N/A
CabhCdpWanDataAddrLeaseCreateTime	read-only	-	N/A
CabhCdpWanDataAddrLeaseExpireTime	read-only	-	N/A
cabhCdpWanDnsServerTable/cabhCdpWanDnsServerEntry			
cabhCdpWanDnsServerOrder	not-accessible	-	N/A
cabhCdpWanDnsServerIpType	read-only	-	N/A
cabhCdpWanDnsServerIp	read-only	-	N/A
cabhCdpServer			
cabhCdpLanPoolStartType	read-write	Yes	1
cabhCdpLanPoolStart	read-write	Yes	1
cabhCdpLanPoolEndType	read-write	Yes	1
cabhCdpLanPoolEnd	read-write	Yes	1
cabhCdpServerNetworkNumberType	read-write	Yes	1
cabhCdpServerNetworkNumber	read-write	Yes	1
cabhCdpServerSubnetMaskType	read-write	Yes	1

EXHIBIT A

MIB NAME/Parameter	Max-Access	Persistent	# of Persistent Entries
cabhCdpServerSubnetMask	read-write	Yes	1
cabhCdpServerTimeOffset	read-write	Yes	1
cabhCdpServerRouterType	read-write	Yes	1
cabhCdpServerRouter	read-write	Yes	1
cabhCdpServerDnsAddressType	read-write	Yes	1
cabhCdpServerDnsAddress	read-write	Yes	1
cabhCdpServerSyslogAddressType	read-write	Yes	1
cabhCdpServerSyslogAddress	read-write	Yes	1
cabhCdpServerDomainName	read-write	Yes	1
cabhCdpServerTTL	read-write	Yes	1
cabhCdpServerInterfaceMTU	read-write	Yes	1
cabhCdpServerVendorSpecific	read-write	Yes	1
cabhCdpServerLeaseTime	read-write	Yes	1
cabhCdpServerDhcpAddressType	read-only	-	N/A
cabhCdpServerDhcpAddress	read-only	-	N/A
cabhCdpServerControl	read-write	No	N/A
cabhCdpServerCommitStatus	read-only	-	N/A
cabhCtpMib **cabhCtpObjects** **cabhCtpBase**			
cabhCtpSetToFactory	read-write	No	N/A
cabhCtpLastSetToFactory	read-only	-	N/A
cabpCtpConnSpeed			
cabhCtpConnSrcIpType	read-write	No	N/A
cabhCtpConnSrcIp	read-write	No	N/A
cabhCtpConnDestIpType	read-write	No	N/A
cabhCtpConnDestIp	read-write	No	N/A
cabhCtpConnProto	read-write	No	N/A
cabhCtpConnNumPkts	read-write	No	N/A
cabhCtpConnPktSize	read-write	No	N/A
cabhCtpConnTimeOut	read-write	No	N/A
cabhCtpConnControl	read-write	No	N/A
cabhCtpConnStatus	read-only	-	N/A
cabhCtpConnPktsSent	read-only	-	N/A
cabhCtpConnPktsRecv	read-only	-	N/A
cabhCtpConnRTT	read-only	-	N/A
cabhCtpConnThroughput	read-only	-	N/A
cabhCtpPing			
cabhCtpPingSrcIpType	read-write	No	N/A
cabhCtpPingSrcIp	read-write	No	N/A
cabhCtpPingDestIpType	read-write	No	N/A
cabhCtpPingDestIp	read-write	No	N/A
cabhCtpPingNumPkts	read-write	No	N/A
cabhCtpPingPktSize	read-write	No	N/A
cabhCtpPingTimeBetween	read-write	No	N/A

EXHIBIT A

MIB NAME/Parameter	Max-Access	Persistent	# of Persistent Entries
cabhCtpPingTimeOut	read-write	No	N/A
cabhCtpPingControl	read-write	No	N/A
cabhCtpPingStatus	read-only	-	N/A
cabhCtpPingNumSent	read-only	-	N/A
cabhCtpPingNumRecv	read-only	-	N/A
cabhCtpPingAvgRTT	read-only	-	N/A
cabhCtpPingMaxRTT	read-only	-	N/A
cabhCtpPingMinRTT	read-only	-	N/A
cabhCtpPingNumIcmpError	read-only	-	N/A
cabhCtpPingIcmpError	read-only	-	N/A
cabhQosMib **cabhPriorityQosMibObjects** **cabhPriorityQosBase**			
cabhPriorityQosMasterTable/ cabhPriorityQosMasterEntry			
cabhPriorityQosMasterApplicationId	not-accessible	-	N/A
cabhPriorityQosMasterDefaultCHPriority	read-create	Yes	16
cabhPriorityQosMasterRowStatus	read-create	Yes	16
cabhPriorityQosSetToFactory	read-write	No	N/A
cabhPriorityQosLastSetToFactory	read-only	-	N/A
cabhPriorityQosBp			
cabhPriorityQosBpTable/cabhPriorityQosBpEntry			
cabhPriorityQosBpIpAddrType	read-only	-	N/A
cabhPriorityQosBpIpAddr	read-only	-	N/A
cabhPriorityQosBpApplicationId	read-only	-	N/A
cabhPriorityQosBpDefaultCHPriority	read-only	-	N/A
cabhPriorityQosBpDestTable/cabhPriorityQosBpDestEntry			
cabhPriorityQosBpDestIndex	not-accessible	-	N/A
cabhPriorityQosBpDestIpAddrType	read-only	-	N/A
cabhPriorityQosBpDestIpAddr	read-only	-	N/A
cabhPriorityQosBpDestPort	read-only	-	N/A
cabhPriorityQosBpDestIpPortPriority	read-only	-	N/A
cabhPriorityQosPs			
cabhPriorityQosPsIfAttribTable/cabhPriorityQosPsIfAttribEntry			
cabhPriorityQosPsIfAttribIfNumPriorities	read-only	-	N/A
cabhPriorityQosPsIfAttribIfNumQueues	read-only	-	N/A

EXHIBIT A

MIB NAME/Parameter	Max-Access	Persistent	# of Persistent Entries
experimental			
snmpUSMDHObjectsMIB [RFC 2786]			
usmDHKeyObjects			
usmDHPublicObjects			
usmDHParamaters	read-write	No	N/A
usmDHUserKeyTable/usmDHUserKeyEntry			
usmDHUserAuthKeyChange	read-create	No	N/A
usmDHUserOwnAuthKeyChange	read-create	No	N/A
usmDHUserPrivKeyChange	read-create	No	N/A
usmDHUserOwnPrivKeyChange	read-create	No	N/A
usmDHKickstartGroup			
usmDHKickstartTable/usmDHKickstartEntry			
usmDHKickstartIndex	not-accessible	-	N/A
usmDHKickstartMyPublic	read-only	-	N/A
usmDHKickstartMgrPublic	read-only	-	N/A
usmDHKickstartSecurityName	read-only	-	N/A
snmpV2			
snmpModules			
snmpMIB			
snmpMIBObjects			
snmpSet			
snmpSetSerialNo	read-write	No	N/A
snmpFrameworkMIB [RFC 3411]			
snmpEngine			
snmpEngineID	read-only	Yes	1
snmpEngineBoots	read-only	Yes	1
snmpEngineTime	read-only	-	N/A
snmpEngineMaxMessageSize	read-only	-	N/A
snmpMPDMIB [RFC 3412]			
snmpMPDObjects			
snmpMPDStats			
snmpUnknownSecurityModels	read-only	-	N/A
snmpInvalidMsgs	read-only	-	N/A
snmpUnknownPDUHandlers	read-only	-	N/A
snmpTargetMIB [RFC 3413]			
snmpTargetObjects			
snmpTargetSpinLock	read-write	No	N/A
snmpTargetAddrTable/snmpTargetAddrEntry			
snmpTargetAddrName	not-accessible	-	N/A
snmpTargetAddrTDomain	read-create	No	N/A
snmpTargetAddrTAddress	read-create	No	N/A

EXHIBIT A

MIB NAME/Parameter	**Max-Access**	**Persistent**	**# of Persistent Entries**
snmpTargetAddrTimeout	read-create	No	N/A
snmpTargetAddrRetryCount	read-create	No	N/A
snmpTargetAddrTagList	read-create	No	N/A
snmpTargetAddrParams	read-create	No	N/A
snmpTargetAddrStorageType	read-create	No	N/A
snmpTargetAddrRowStatus	read-create	No	N/A
snmpTargetParamsTable/snmpTargetParamsEntry			
snmpTargetParamsName	not-accessible	-	N/A
snmpTargetParamsMPModel	read-create	No	N/A
snmpTargetParamsSecurityModel	read-create	No	N/A
snmpTargetParamsSecurityName	read-create	No	N/A
snmpTargetParamsSecurityLevel	read-create	No	N/A
snmpTargetParamsStorageType	read-create	No	N/A
snmpTargetParamsRowStatus	read-create	No	N/A
snmpUnavailableContexts	read-only	-	N/A
snmpUnknownContexts	read-only	-	N/A
snmpNotificationMIB [RFC 3413] **snmpNotifyObjects**			
snmpNotifyTable/snmpNotifyEntry			
snmpNotifyName	not-accessible	-	N/A
snmpNotifyTag	read-create	No	N/A
snmpNotifyType	read-create	No	N/A
snmpNotifyStorageType	read-create	No	N/A
snmpNotifyRowStatus	read-create	No	N/A
snmpNotifyFilterProfileTable/snmpNotifyFilterProfileEntry			
snmpNotifyFilterProfileName	read-create	No	N/A
snmpNotifyFilterProfileStorType	read-create	No	N/A
snmpNotifyFilterProfileRowStatus	read-create	No	N/A
snmpNotifyFilterTable/snmpNotifyFilterEntry			
snmpNotifyFilterSubtree	not-accessible	-	N/A
snmpNotifyFilterMask	read-create	No	N/A
snmpNotifyFilterType	read-create	No	N/A
snmpNotifyFilterStorageType	read-create	No	N/A
snmpNotifyFilterRowStatus	read-create	No	N/A
snmpUsmMIB [RFC 3414] **usmStats**			
usmStatsUnsupportedSecLevels	read-only	-	N/A
usmStatsNotInTimeWindows	read-only	-	N/A
usmStatsUnknownUserNames	read-only	-	N/A
usmStatsUnknownEngineIDs	read-only	-	N/A
usmStatsWrongDigests	read-only	-	N/A

EXHIBIT A

MIB NAME/Parameter	**Max-Access**	**Persistent**	**# of Persistent Entries**
usmStatsDecryptionErrors	read-only	-	N/A
usmUser			
usmUserSpinLock	read-write	No	N/A
usmUserTable/usmUserEntry			
usmUserEngineID	not-accessible	-	N/A
usmUserName	not-accessible	-	N/A
usmUserSecurityName	read-only	-	N/A
usmUserCloneFrom	read-create	No	N/A
usmUserAuthProtocol	read-create	No	N/A
usmUserAuthKeyChange	read-create	No	N/A
usmUserOwnAuthKeyChange	read-create	No	N/A
usmUserPrivProtocol	read-create	No	N/A
usmUserPrivKeyChange	read-create	No	N/A
usmUserOwnPrivKeyChange	read-create	No	N/A
usmUserPublic	read-create	No	N/A
usmUserStorageType	read-create	No	N/A
usmUserStatus	read-create	No	N/A
SNMP-VIEW-BASED-ACM-MIB [RFC 3415] **snmpVacmMIB** **vacmMIBObjects**			
vacmContextTable/vacmContextEntry			
vacmContextName	read-only	-	N/A
vacmSecurityToGroupTable/vacmSecurityToGroupEntry			
vacmSecurityModel	not-accessible	-	N/A
vacmSecurityName	not-accessible	-	N/A
vacmGroupName	read-create	No	N/A
vacmSecurityToGroupStorageType	read-create	No	N/A
vacmSecurityToGroupStatus	read-create	No	N/A
vacmAccessTable/vacmAccessEntry			
vacmAccessContextPrefix	not-accessible	-	N/A
vacmAccessSecurityModel	not-accessible	-	N/A
vacmAccessSecurityLevel	not-accessible	-	N/A
vacmAccessContextMatch	read-create	No	N/A
vacmAccessReadViewName	read-create	No	N/A
vacmAccessWriteViewName	read-create	No	N/A
vacmAccessNotifyViewName	read-create	No	N/A
vacmAccessStorageType	read-create	No	N/A
vacmAccessStatus	read-create	No	N/A
vacmMIBViews			
vacmViewSpinLock	read-write	No	N/A

EXHIBIT A

MIB NAME/Parameter	Max-Access	Persistent	# of Persistent Entries
vacmViewTreeFamilyTable/vacmViewTreeFamilyEntry			
vacmViewTreeFamilyViewName	not-accessible	-	N/A
vacmViewTreeFamilySubtree	not-accessible	-	N/A
vacmViewTreeFamilyMask	read-create	No	N/A
vacmViewTreeFamilyType	read-create	No	N/A
vacmViewTreeFamilyStorageType	read-create	No	N/A
vacmViewTreeFamilyStatus	read-create	No	N/A
snmpCommunityMIB [RFC 2576] **snmpCommunityMIBObjects**			
snmpCommunityTable/snmpCommunityEntry			
snmpCommunityIndex	not-accessible	-	N/A
snmpCommunityName	read-create	No	N/A
snmpCommunitySecurityName	read-create	No	N/A
snmpCommunityContextEngineID	read-create	No	N/A
snmpCommunityContextName	read-create	No	N/A
snmpCommunityTransportTag	read-create	No	N/A
snmpCommunityStorageType	read-create	No	N/A
snmpCommunityStatus	read-create	No	N/A
snmpTargetAddrExtTable/snmpTargetAddrExtEntry			
snmpTargetAddrTMask	read-create	No	N/A
snmpTargetAddrMMS	read-create	No	N/A
clabSecCertObject			
clabSrvcPrvdrRootCACert	read-only	-	N/A
clabCVCRootCACert	read-only	-	N/A
clabCVCCACert	read-only	-	N/A
clabMfgCVCCert	read-only	-	N/A

EXHIBIT A

Appendix II Format and Content for Event, SYSLOG and SNMP Trap[148]

The table in this appendix summarizes the format and content for local log event entries, syslog messages, and SNMP traps.

Each row in the table specifies an event that the PS must be capable of generating. These events are to be reported by the PS by any or all of the following three means: local event logging as implemented by the local event table in [RFC 2669], SYSLOG, and SNMP trap. The SYSLOG format is specified in Section 6.3.3.2.4.4 of this document and SNMP trap format is defined in this appendix, following Table II-1.

The first and second columns of Table II-1 indicate in which stage the event happens. The third column indicates the priority assigned to the event. These priorities are the same as reported in the docsDevEvLevel object in [RFC 2669] and in the LEVEL field of a syslog message.

The fourth column specifies the event text, which is reported in the docsDevEvText object of the [RFC 2669] and the text field of a syslog message. The fifth column provides additional information about the event text of the fourth column. For example, some of the event text fields are constants and some event text fields include variable information. Some of the variables are only required in the SYSLOG, as described in the fifth column. The sixth column specifies the error code set.

The seventh column indicates an unique identification number for the event, which is assigned to the docsDevEvId object and the <eventId> field of a syslog message. The eighth column specifies the SNMP trap, which notifies this event to a SNMP event receiver.

The rules to uniquely generate an event ID from the error code are described in Section 6.3.3.2.4.4. The event IDs in the table are in decimal format.

To better illustrate the table, the following is an example using the first row in the section of Software Upgrade events.

The first and second columns are "SW Upgrade" and "SOFTWARE UPGRADE INIT". The event priority is "Notice." The event text is "Software Download INIT - Via NMS". The fifth column reads "For SYSLOG only, append: MAC addr: <P1> P1 = PS Mac Address". This is a note about the SYSLOG. That is to say, the syslog text body will be like "Software Download INIT - Via NMS - MAC addr: x1 x2 x3 x4 x5 x6".

The last column "TRAP NAME" is cabhPsDevSwUpgradeInitTrap, the format for which is given at the end of this appendix.

[148] Revised Table II-1 per ECN CH1.1-N-03.0103-3 and CH1.1-N-03.0097-5 by GO on 12/5/03 and 12/9/03.

EXHIBIT A

Table II-1 – Defined Events for CableHome

PROCESS	SUB-PROCESS	PS PRIORITY	EVENT TEXT	MESSAGE NOTES AND DETAILS	Error Code SET	EventID	TRAP NAME
DHCP Errors before provisioning complete							
Init	CDC	Critical	DHCP FAILED - Discover sent, no offer received		D01.0	68000100	
Init	CDC	Critical	DHCP FAILED - Request sent, No response		D02.0	68000200	
Init	CDC	Critical	DHCP FAILED - Requested Info not supported.		D03.0	68000300	
Init	CDC	Error	DHCP ERROR - Response does not contain ALL the valid fields OR the PS is unable to determine provisioning mode		D03.1	68000301	
Init	CDC	Warning	DHCP ERROR - Unable to obtain all WAN-Data IP addresses the PS was configured to obtain		P02.0	68000302	cabhPsDevCdpWanDataIpTrap
TOD Errors before provisioning complete							
Init	TOD	Warning	TOD Request sent - no response received		D04.1	68000401	cabhPsDevInitTrap
Init	TOD	Warning	TOD Response received - invalid data format		D04.2	68000402	cabhPsDevInitTrap
TFTP Errors before provisioning complete							
Init	TFTP	Error	TFTP failed - Request sent - No Response		D05.0	68000500	cabhPsDevInitTrap (Trap is relevant for SNMP Prov Mode only.)
Init	TFTP	Error	TFTP failed - configuration file NOT FOUND	For SYSLOG only: append: File name = <P1> P1 = requested file name	D06.0	68000600	cabhPsDevInitTrap (Trap is relevant for SNMP Prov Mode only.)

EXHIBIT A

PROCESS	SUB-PROCESS	PS PRIORITY	EVENT TEXT	MESSAGE NOTES AND DETAILS	Error Code SET	EventID	TRAP NAME
Init	TFTP	Error	TFTP Failed - OUT OF ORDER packets		D07.0	68000700	cabhPsDevInitTrap (Trap is relevant for SNMP Prov Mode only.)
Init	TFTP	Error	TFTP file complete - but failed SHA-1 hash check	For SYSLOG only: append: File name = <P1> P1 = filename of TFTP file	D08.0	68000800	cabhPsDevInitTrap (Trap is relevant for SNMP Prov Mode only.)
Init	TFTP	Error	TFTP Failed Exceeded maximum number of retries	For Syslog only: append: Retry limit = <P1> P1 = maximum number of retries	D09.0	68000900	cabhPsDevInitTrap (Trap is relevant for SNMP Prov Mode only.)
TFTP Success							
Init	TFTP	Notice	TFTP success		D10.0	68001000	
TLS							
Init	TCP/IP	Critical	PS failed to connect to HTTP/TLS server		D20.0	68002000	
Init	TLS	Critical	TLS Connection timed out and maximum number of retries exceeded		D21.0	68002100	
Init	TLS	Critical	TLS FATAL ERROR <P1>	P1= Error code from [RFC 2246]	D22.0	68002200	
HTTP							
Init	HTTP	Critical	Configuration File Download failed, but will retry. HTTP Error. <P1>	P1= Status codes from [RFC 2616]	D30.0	68003000	
Init	HTTP	Critical	Configuration file download failed. Due to connection timed out and maximum number of retries. Operation aborted.		D31.0	68003100	

EXHIBIT A

PROCESS	SUB-PROCESS	PS PRIORITY	EVENT TEXT	MESSAGE NOTES AND DETAILS	Error Code SET	EventID	TRAP NAME
Init	HTTP	Critical	Secure Configuration file download successfully completed.		D32.0	68003200	
TLV Parsing							
Init	TLV PARSING	Warning	TLV-27 or TLV-28 - unrecognized OID		I401.0	73040100	cabhPsDevInitTLVUnknownTrap
Init	TLV PARSING	Warning	Unknown TLV <P1>	For SYSLOG only, <P1> = the complete TLV in hexadecimal	I401.1	73040101	cabhPsDevInitTLVUnknownTrap
Init	TLV PARSING	Error	Invalid TLV Format/contents <P1>	For SYSLOG only, <P1> = the complete TLV in hexadecimal	I401.2	73040102	
Provisioning							
Init	Provisioning Complete	Notice	Provisioning complete	For SYSLOG only, append MAC Addr: <P1>. P1 = PS MAC address	I11.0	73001100	cabhPsDevInitTrap
SW UPGRADE INIT*							
SW Upgrade	SW UPGRADE INIT	Notice	SW Download INIT - Via NMS	For SYSLOG only, append: SW file: <P1> - SW server: < P2>. P1 = SW file name and P2 = Tftp server IP address	E101.0	69010100	cabhPsDevSwUpgradeInitTrap
SW Upgrade	SW UPGRADE INIT	Notice	SW Download INIT - Via Config file <P1>	P1 = CM config file nameFor SYSLOG only, append: SW file: <P2> - SW server: < P3>. P2 = SW file name and P3 = Tftp server IP address	E102.0	69010200	cabhPsDevSwUpgradeInitTrap
SW UPGRADE GENERAL FAILURE*							
SW Upgrade	SW UPGRADE GENERAL FAILURE	Error	SW Upgrade Failed during download - Max retry exceed (3)	For SYSLOG only, append: SW file: <P1> - SW server: < P2>. P1 = SW file name and P2 = Tftp server IP address	E103.0	69010300	cabhPsDevSwUpgradeFailTrap
SW Upgrade	SW UPGRADE GENERAL FAILURE	Error	SW Upgrade Failed Before Download - Server not Present	For SYSLOG only, append: SW file: <P1> - SW server: < P2>. P1 = SW file name and P2 = Tftp server IP address	E104.0	69010400	cabhPsDevSwUpgradeFailTrap

EXHIBIT A

PROCESS	SUB-PROCESS	PS PRIORITY	EVENT TEXT	MESSAGE NOTES AND DETAILS	Error Code SET	EventID	TRAP NAME
SW Upgrade	SW UPGRADE GENERAL FAILURE	Error	SW upgrade Failed before download - File not Present	For SYSLOG only, append: SW file: <P1> - SW server: < P2>. P1 = SW file name and P2 = TFTP server IP address	E105.0	69010500	cabhPsDevSwUpgrade FailTrap
SW Upgrade	SW UPGRADE GENERAL FAILURE	Error	SW upgrade Failed before download -TFTP Max Retry Exceeded	For SYSLOG only, append: SW file: <P1> - SW server: < P2>. P1 = SW file name and P2 = TFTP server IP address	E106.0	69010600	cabhPsDevSwUpgrade FailTrap
SW Upgrade	SW UPGRADE GENERAL FAILURE	Error	SW upgrade Failed after download -Incompatible SW file	For SYSLOG only, append: SW file: <P1> - SW server: < P2>. P1 = SW file name and P2 = Tftp server IP address	E107.0	69010700	cabhPsDevSwUpgrade FailTrap
SW Upgrade	SW UPGRADE GENERAL FAILURE	Error	SW upgrade Failed after download - SW File corruption	For SYSLOG only, append: SW file: <P1> - SW server: < P2>. P1 = SW file name and P2 = TFTP server IP address	E108.0	69010800	cabhPsDevSwUpgrade FailTrap
SW Upgrade	SW UPGRADE GENERAL FAILURE	Error	Disruption during SW download - Power Failure	For SYSLOG only, append: SW file: <P1> - SW server: < P2>. P1 = SW file name and P2 = Tftp server IP address	E109.0	69010900	cabhPsDevSwUpgrade FailTrap
SW UPGRADE SUCCESS*							
SW Upgrade	SW UPGRADE SUCCESS	Notice	SW download Successful - Via NMS	For SYSLOG only, append: SW file: <P1> - SW server: < P2>. P1 = SW file name and P2 = Tftp server IP address	E111.0	69011100	cabhPsDevSwUpgrade SuccessTrap
SW Upgrade	SW UPGRADE SUCCESS	Notice	SW download Successful - Via Config file	For SYSLOG only, append: SW file: <P1> - SW server: < P2>. P1 = SW file name and P2 = Tftp server IP address	E112.0	69011200	cabhPsDevSwUpgrade SuccessTrap
DHCP failure after provisioning complete							
DHCP	CDC	Error	DHCP RENEW sent - No response		D101.0	68010100	cabhPsDevDHCPFailT rap
DHCP	CDC	Error	DHCP REBIND sent - No response		D102.0	68010200	cabhPsDevDHCPFailT rap

EXHIBIT A

PROCESS	SUB-PROCESS	PS PRIORITY	EVENT TEXT	MESSAGE NOTES AND DETAILS	Error Code SET	EventID	TRAP NAME
DHCP	CDC	Error	DHCP RENEW sent - Invalid DHCP option		D103.0	68010300	cabhPsDevDHCPFailTrap
DHCP	CDC	Error	DHCP REBIND sent - Invalid DHCP option		D104.0	68010400	cabhPsDevDHCPFailTrap
TOD failure after provisioning complete							
TOD	TOD	Warning	TOD Request sent - no response received		D04.3	68000403	cabhPsDevTODFailTrap
TOD	TOD	Warning	TOD Response received - invalid data format		D04.4	68000404	cabhPsDevTODFailTrap
VERIFICATION OF CODE FILE							
SW Upgrade	SW UPGRADE GENERAL FAILURE	Error	Improper Code File Controls	For SYSLOG only, append: Code File: <P1> - Code File Server: <P2>. P1= Code file name, P2 = code file server IP address	E201.0	69020100	cabhPsDevSwUpgradeFailTrap
SW Upgrade	SW UPGRADE GENERAL FAILURE	Error	Code File Manufacturer CVC Validation Failure	For SYSLOG only, append: Code File: <P1> - Code File Server: <P2>. P1= Code file name, P2 = code file server IP address	E202.0	69020200	cabhPsDevSwUpgradeFailTrap
SW Upgrade	SW UPGRADE GENERAL FAILURE	Error	Code File Manufacturer CVS Validation Failure	For SYSLOG only, append: Code File: <P1> - Code File Server: <P2>. P1= Code file name, P2 = code file server IP address	E203.0	69020300	cabhPsDevSwUpgradeFailTrap
SW Upgrade	SW UPGRADE GENERAL FAILURE	Error	Code File Co-Signer CVC Validation Failure	For SYSLOG only, append: Code File: <P1> - Code File Server: <P2>. P1= Code file name, P2 = code file server IP address	E204.0	69020400	cabhPsDevSwUpgradeFailTrap
SW Upgrade	SW UPGRADE GENERAL FAILURE	Error	Code File Co-Signer CVS Validation Failure	For SYSLOG only, append: Code File: <P1> - Code File Server: <P2>. P1= Code file name, P2 = code file server IP address	E205.0	69020500	cabhPsDevSwUpgradeFailTrap
VERIFICATION OF CVC							
SW Upgrade	VERIFICATION OF CVC	Error	Improper Configuration File CVC Format - TFTP Server: <P1> - Config File: <P2>	P1 = TFTP Server IP Address P2 = Config File Name	E206.0	69020600	cabhPsDevSwUpgradeCVCFailTrap

EXHIBIT A

PROCESS	SUB-PROCESS	PS PRIORITY	EVENT TEXT	MESSAGE NOTES AND DETAILS	Error Code SET	EventID	TRAP NAME
SW Upgrade	VERIFICATION OF CVC	Error	Configuration File CVC Validation Failure - TFTP Server: <P1> - Config File: <P2>	P1 = TFTP Server IP AddressP2 = Config File Name	E207.0	69020700	cabhPsDevSwUpgradeCVCFailTrap
SW Upgrade	VERIFICATION OF CVC	Error	Improper SNMP CVC Format - Snmp manager: <P1>	P1= IP Address of SNMP Manager	E208.0	69020800	cabhPsDevSwUpgradeCVCFailTrap
SW Upgrade	VERIFICATION OF CVC	Error	SNMP CVC Validation Failure - Snmp manager: <P1>	P1=IP Addr of SNMP manager	E209.0	69020900	cabhPsDevSwUpgradeCVCFailTrap
CDP Events							
CDP	CDS	Notice	Attempt to allocate more LAN TRANS IP addresses than allowed		P01.0	80000100	cabhPsDevCDPThreshold Trap
CDP	CDS	Notice	Unable to provision DHCP LAN client- IP address pool exhausted		P03.0	80000300	cabhPsDevCdpLanIpPoolTrap
CSP Events							
CSP	Firewall	Notice	Change in state for cabhSec2FwEventEnable for Type 1. The new value is <P1>	P1=value of cabhSec2FwEventTypeEnable for Type 1	P101.1	80010101	cabhPsDevCSPTrap
CSP	Firewall	Notice	Change in state for cabhSec2FwEventEnable for Type 2. The new value is <P1>	P1=value of cabhSec2FwEventTypeEnable for Type 2	P101.2	80010102	cabhPsDevCSPTrap
CSP	Firewall	Notice	Change in state for cabhSec2FwEventEnable for Type 3. The new value is <P1>	P1=value of cabhSec2FwEventTypeEnable for Type 3	P101.3	80010103	cabhPsDevCSPTrap
CSP	Firewall	Notice	Change in state for cabhSec2FwEventEnable for Type 4. The new value is <P1>	P1=value of cabhSec2FwEventTypeEnable for Type 4	P101.4	80010104	cabhPsDevCSPTrap

EXHIBIT A

PROCESS	SUB-PROCESS	PS PRIORITY	EVENT TEXT	MESSAGE NOTES AND DETAILS	Error Code SET	EventID	TRAP NAME
CSP	Firewall	Notice	Change in state for cabhSec2FwEventEnable for Type 5. The new value is <P1>	P1=value of cabhSec2FwEventTypeEnable for Type 5	P101.5	80010105	cabhPsDevCSPTrap
CSP	Firewall	Notice	Change in state for cabhSec2FwEventEnable for Type 6. The new value is <P1>	P1=value of cabhSec2FwEventTypeEnable for Type 6	P101.6	80010106	cabhPsDevCSPTrap
CSP	Firewall	Warning	Firewall Type 1 event threshold exceeded		P102.1	80010201	cabhPsDev CSPTrap
CSP	Firewall	Warning	Firewall Type 2 event threshold exceeded		P102.2	80010202	cabhPsDev CSPTrap
CSP	Firewall	Warning	Firewall Type 3 event threshold exceeded		P102.3	80010203	cabhPsDev CSPTrap
CSP[149]	Firewall	Warning	Firewall Type 4 event threshold exceeded, Set of <P1> failed, <P2>	P1 = MIB object attempted to be changed (e.g., "cabhSec2FwPolicyFileURL") P2 = Textual description of failure	P102.4	80010204	cabhPsDev CSPTrap
CSP	Firewall	Warning	Firewall Type 5 event threshold exceeded		P102.5	80010205	cabhPsDev CSPTrap
CSP	Firewall	Warning	Firewall Type 6 event threshold exceeded		P102.6	80010206	cabhPsDev CSPTrap
CSP	Firewall TFTP	Critical	TFTP download of firewall policy file failed: request sent, no response	P1 = requested firewall policy file URL	P130.0	80013000	cabhPsDevCSPTrap
CSP	Firewall TFTP	Critical	TFTP failed - firewall policy file not found	P1 = requested firewall policy file URL	P131.0	80013100	cabhPsDevCSPTrap
CSP	Firewall TFTP	Critical	TFTP failed - invalid firewall policy file	P1 = requested firewall policy file URL	P132.0	80013200	cabhPsDevCSPTrap
CSP	Firewall TFTP	Critical	Firewall policy file download complete but failed SHA-1 has check	P1 = requested firewall policy file URL, P2 = firewall policy file has value	P133.0	80013300	cabhPsDevCSPTrap
CSP	Firewall TFTP	Critical	Firewall policy file download exceeded maximum allowable number of TFTP retries	P1 = requested firewall policy file URL	P134.0	80013400	cabhPsDevCSPTrap

[149] Revised this row per ECN CH1.1-N-04.0115-1 by KB on 4/5/04.

EXHIBIT A

PROCESS	SUB-PROCESS	PS PRIORITY	EVENT TEXT	MESSAGE NOTES AND DETAILS	Error Code SET	EventID	TRAP NAME
CSP	Firewall TFTP	Notice	Firewall policy file TFTP download success	P1 = requested firewall policy file URL For SYSLOG only: append: Retry limit = <P2> P2 = maximum allowable number of retry attempts	P135.0	80013500	cabhPsDevCSPTrap
CAP Events							
CAP	C-NAT	Warning	CAP unable to make C-NAT mapping. No WAN-data IP address available		P201.0	80020100	cabhPsDevCAPTrap
CAP	C-NAPT	Warning	CAP unable to make C-NAPT mapping. No WAN IP address available		P250.0	80025000	cabhPsDevCAPTrap
CTP Events							
CTP	Connection Speed Tool	Notice	Connection Speed Tool test completed successfully	P1 = IP address of source P2 = IP address of destination P3 = protocol P4 = throughput	P301.0	80030100	cabhPsDevCtpTrap
CTP	Connection Speed Tool	Notice	Connection Speed Tool test timed out	P1 = IP address of source P2 = IP address of destination P3 = protocol P4 = value of timer (millisec)	P302.0	80030200	cabhPsDevCtpTrap
CTP	Connection Speed Tool	Notice	Connection Speed Tool test aborted	P1 = IP address of source P2 = IP address of destination P3 = protocol P4 = value of timer (millisec)	P303.0	80030300	cabhPsDevCtpTrap
CTP	Ping Tool	Notice	Ping Tool test completed successfully	P1 = IP address of source P2 = IP address of destination P3 = average round trip time	P320.0	80032000	cabhPsDevCtpTrap

EXHIBIT A

PROCESS	SUB-PROCESS	PS PRIORITY	EVENT TEXT	MESSAGE NOTES AND DETAILS	Error Code SET	EventID	TRAP NAME
CTP	Ping Tool	Notice	Ping Tool test timed out	P1 = IP address of source P2 = IP address of destination P3 = number of requests sent P4 = number of responses received	P321.0	80032100	cabhPsDevCtpTrap
CTP	Ping Tool	Notice	Ping Tool test aborted	P1 = IP address of source P2 = IP address of destination P3 = number of requests sent P4 = number of responses received	P322.0	80032200	cabhPsDevCtpTrap

Notes to Table II-1:

* Software upgrade (secure software download) events apply to stand-alone Portal Services only. Software upgrade is controlled by the DOCSIS cable modem in an embedded PS, so software upgrade event reporting is managed by the cable modem in an embedded PS. For more information, refer to Section 11.8, Secure Software Download for the PS.[150]

[150] Revised the Notes to Table II-1 per ECN CH1.1-03.0091-1 by GO on 12/5/03.

EXHIBIT A

II.1 Trap Descriptions

All traps specified by CableHome 1.1 are defined in the PS DEV MIB specification, [CH5].

EXHIBIT A

Appendix III Security Threats & Preventative Measures

When developing a security technology, it is important to understand what the primary threats for a given application or environment. This information can then be used to select the most effective security tools and technologies for protection and prevention against malicious attacks.

The following primary home networking security threats to subscribers and multiple system operators (MSOs) have been identified:

> Theft of Service: Theft of service comes in two forms; unauthorized access to cable services and unauthorized duplication of service content.
>
> Unauthorized access involves a subscriber or 3rd party (such as a neighbor) having access to cable services for which they have not paid. Devices could be "cloned" or modified to appear as a qualified device on the subscriber's home network. This could also degrade service delivery performance as these devices consume additional transport resources on the HFC and home networks.
>
> Unauthorized duplication usually involves a subscriber or 3rd party (such as a neighbor) making illegal copies of service content. In some cases, these copies are distributed to other consumers without the approval of the MSO or content provider.
>
> Denial of Service (DOS) Attacks: Denial of service attacks can occur when a 3rd party entity (attacker, disgruntled customer, etc.) disrupts the normal communication and delivery of services between MSOs and their subscribers. Offending data transmissions coming from what appears to be a valid device/ source, could be injected into the home network and severely degrade its normal functions. These offending data transmissions could also extend to the MSO's HFC network causing performance problems there.
>
> Service Confidentiality: The service confidentiality threat involves a 3rd party (neighbors, attacker, etc.) monitoring/receiving information about a subscriber and the services they use. This could result in passwords or device configuration information being stolen, allowing attackers to gain further access to a subscriber's network resources and confidential files/data.

There are a number of different methods that can be used to prevent the home network security threats mentioned above. Unfortunately, one method cannot prevent them all, but a combination may be the best line of defense. The following preventative measures can be used:

> Authentication: Authentication involves the verification that the sending and receiving entities are as claimed. This includes the service source, the receiving device, and the subscriber.
>
> Authentication helps prevent theft of service by validating end devices and users, but it does not prevent content from being illegally copied or, prevent unauthorized access by 3rd parties who are monitoring the link. It does do a good job at preventing DOS attacks because traffic can be rejected if it does not come from a valid source. By itself, authentication does not provide any service confidentiality support, encryption must be used.
>
> Copy Protection: Copy protection methods limit the ability of a receiving device to make unauthorized copies of service content.
>
> Copy protection helps prevent theft of service by limiting how many copies can be made, but it does not prevent unauthorized access to services. It also does not prevent DOS or service

EXHIBIT A

confidentiality protection. In general, this preventive measure is implemented at higher application layers.

Data Encryption: Data encryption prevents the unauthorized disclosure/access of data.

Data encryption does an excellent job at providing data confidentiality and protection against theft of service. Encryption prevents making data unable to read without the correct decrypting key. However, it does not validate the source/receiving entities and it does not provide copy protection after the data has been decrypted. It also does not prevent DOS attacks.

Firewall: Firewall applications prevent network traffic from passing from one domain to another, unless it meets certain criteria set by the subscriber or MSO. In home networks, firewalls are typically located on residential gateway devices that connect the HFC network to the home network.

A firewall application helps prevent DOS attacks and confidentiality attacks from the wide-area network (WAN) side of the firewall, but it does not prevent these kind of attacks coming from the home network side of the firewall. It also does not provide theft of service protection.

Management Message Security: This method of prevention involves authentication and encryption of network management messages only. Network management messages are used for device configuration, network monitoring/control, service provisioning, and Quality of Service (QoS) reservations.

Management message security provides a good mechanism to prevent DOS attacks by authenticating and encrypting management messages. Subscriber 's personal and network configuration information is also protected from confidentiality attacks, but service content is not. Also, management message security does not prevent theft of service content by unauthorized entities.

EXHIBIT A

Appendix IV Applications Through CAT and Firewall

In the normal operation of address translation and firewall functionality, a number of protocols and applications may be prohibited from working as expected. Firewalls may purposely filter out certain applications and protocols for security purposes. The firewall policy can be explicitly set by the cable operator to allow as many ports to be opened as needed by the customer without opening ports that are not needed for communication between the LAN and WAN. Limiting the open ports and session initiation between the LAN and WAN may provide protection to the home LAN from attacks. If the ports are not allowed to be opened by the firewall policy, an attacker can not use these ports to attack the LAN. The purpose of this appendix is to provide a minimum level of support for commonly used applications under specific scenarios, and to assist the cable operator with common port configuration.

[RFC 3235], Network Address Translator (NAT)-Friendly Application Design Guidelines, outlines a number of guidelines for creating applications in such a manner that they will not be compromised when running in the presence of Network Address Translation functionality. It is strongly recommended that developers of applications that will run within a CableHome environment adhere to these guidelines.

The existence of NAT and Firewall functionality are known to disrupt a number of protocols and applications when the end nodes/hosts are not in the same address realm and must traverse an IP Network Address Translator (NAT/CAT) and/or Firewall enroute to bridge the realms. In many cases, the CAT and Firewall can not provide the application and protocol transparency desired without the assistance of an Application Level Gateway (ALG). CableHome 1.1 assumes an ALG is implemented in the CableHome Residential Gateway that enables applications listed within this appendix to work through the CAT.

Applications though the firewall are described in terms of protocol, specific port numbers, LAN-WAN relationship scenarios and addressing realms. The protocols are divided into two tables; one table is to list the protocols which can be managed by policy alone and is labeled Applications Requiring Firewall Policy Exclusively; the second table is to list the protocols which can only be managed with the combination of policy and ALGs and is labeled Applications Requiring Firewall Policy and an ALG.

According to the policy specified within Section 11 of this document, the tables contain information comments for the reader to be able to map the required applications to those with particular policy requirements for CableHome and PacketCable. CableHome requires factory default settings for the ports to be opened through the firewall for normal CableHome Residential gateway operations. The items marked with PacketCable in the comments column will be included, in addition to the factory defaults in enable PacketCable through the firewall. The firewall settings to enable PacketCable are listed in the comments column of each table and are specified within Section 11 in the configuration file section.

In addition to the specified applications, the PS SHOULD support online gaming applications through the CAT and CableHome firewall. Online gaming is considered a typical user application. However, CableHome does not specify games, as gaming is a dynamic industry and the online game ports depend upon the current popularity of particular games.

IV.1 Relationship Scenarios

The specific scenarios may define the number of hosts communicating with each other through the PS, along with the requirements for each protocol and application. Each application/protocol and specific scenario requires support of the CH CAT and firewall to function correctly. The scenarios include an "xxx to xxx" definition that indicates the number of LAN hosts communicating to WAN hosts (ex. "One to Many" defines One LAN host communicating with Many WAN hosts concurrently.). These scenarios include:

EXHIBIT A

- “One to One” relationship for a single instance
- “One to One” relationship for multiple instances (the number of required instances may be identified)
- “One to Many” relationship for a single instance
- “One to Many” relationship for multiple instances (the number of required instances may be identified)
- “Many to One” relationship for a single instance
- “Many to One” relationship for multiple instances (the number of required instances will be identified if necessary)

Note: The “Many to Many” scenario will be the same as a “One to One” relationship for multiple instances, a “One to Many” relationship for multiple instances, and/or a “Many to One” relationship for multiple instances.

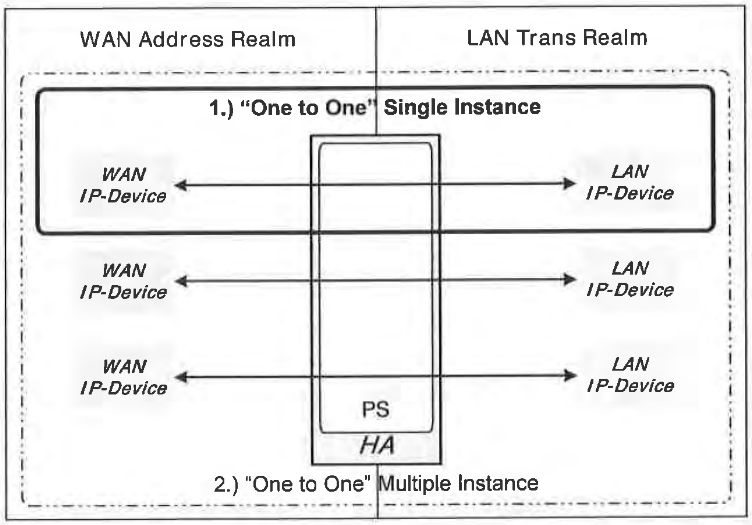


Figure IV-1 – “One to One” Scenarios

EXHIBIT A

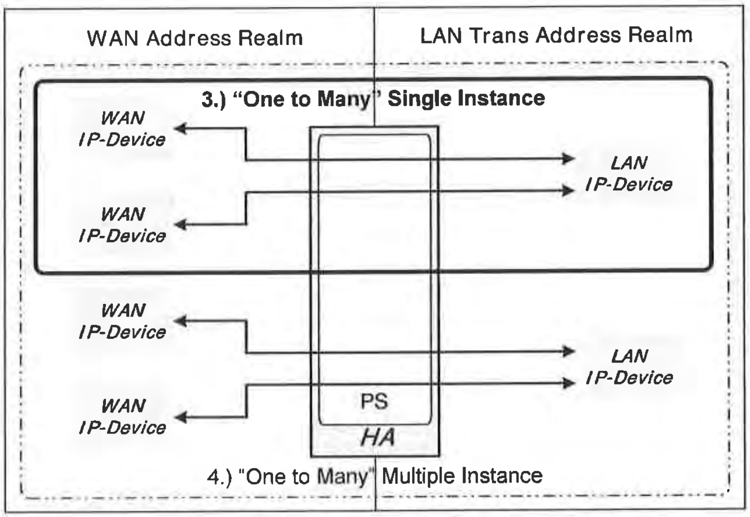


Figure IV-2 – "One to Many" Scenarios

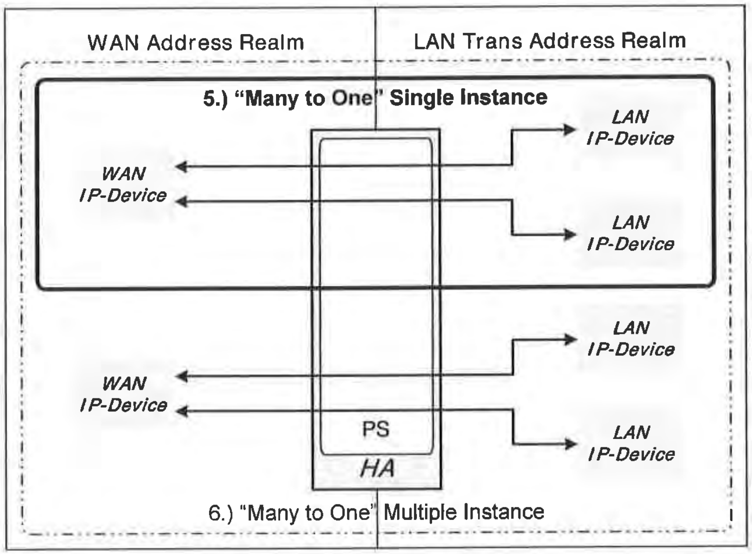


Figure IV-3 – "Many to One" Scenarios

EXHIBIT A

IV.2 Applications Requiring Firewall Policy Exclusively

Table IV-1 and Table IV-2 identify the applications and protocols that MUST be supported through the CAT and Firewall. This does not preclude the support of additional applications and protocols. A CAT/Firewall that can support these applications and protocols will be able to support most other applications and protocols that do not embed address, port, or other information affected by network address translation, and do not negotiate inbound sessions.

The following list of protocols and applications in Table IV-1 MUST work through CAT and CableHome Firewall implementations. The firewall MUST NOT begin operations until after the provisioning complete message is sent by the PS, therefore the protocols needed for the PS to provision are not noted in this table.

Note: Applications only requiring Firewall policy configuration exclusively MUST be supported in all six (6) relationship scenarios unless noted in the comments column.

Table IV-1 – Protocols required to work through CAT and CH Firewall

Application / Protocol	Ports	Comments
AOL IM	TCP/5190, 5191, 5192, 5193 & 13784	Internet Default
CU-SeeMe	TCP/7648, 7649; UDP/7648, 7649, 24032	
DHCP		Internet Default
DNS	UDP/53	PacketCable and CableHome
FTPS	989 & 990	
HTTP	TCP/80	Internet Default
HTTPS	TCP/443	Internet Default
IGMP and IP Multicast		CH 1.0 appendix requirement
imap	143	
imap3	220	
IPSec	IKE > UDP/500 - ESP > raw IP/50	IKE key exchange, Tunnel mode, one to one single instance (CAT support key) IKE key exchange, Transport mode, one to one single instance (Passthrough mode) PacketCable & LAN Peer Passthrough mode
IRC	TCP/6665-6669	
Kerberos	1293	PacketCable and CableHome PS Address Realm
L2TP	UDP/1701	
MediaPlayer (Windows)	TCP/ 80;1755	
Microsoft Messenger	3330 - 3332	Internet Default mcs-calypsoicf 3330 mcs-messaging 3331 mcs-mailsvr 3332
MGCP	2427, 2727	PacketCable
Peer to Peer (eDonkey)	TCP/4662 UDP/4665	eDonkey

EXHIBIT A

Application / Protocol	Ports	Comments
Peer to Peer (FastTrack P2P Protocol)	TCP/1214	KaZaA, Grokster, etc.
Peer to Peer (Gnutella P2P Protocol)	TCP/6346	Gnutella, LimeWire, BearShare, Morpheus, etc.
Peer to Peer (WinMX)	TCP/6699 UDP/6257	WinMX
PING ICMP Echo Request	raw IP/1	CableHome
POP3	TCP/110	Internet Default
PPTP	Control Port > TCP/1723 & GRE > raw IP/47	
RealAudio/RealMedia	TCP: 80;443;554	
RSVP		PacketCable
RTSP	TCP/554	
RTCP		PacketCable
RTP		PacketCable
SMTP	TCP/25	Internet Default
SNMP	TCP/161 UDP/161	CableHome PS Address Realm and PacketCable
SNMP trap	TCP/162 UDP/162	CableHome PS Address Realm and PacketCable
SSH	TCP/22 UDP/22	Internet Default
Syslog	UDP/514	CableHome PS Address Realm and PacketCable
Telnet	UDP/23	Outbound session requests. Internet Default
TFTP	UDP/69	PacketCable
Traceroute	raw IP/1	Internet Default Reply from all hops between source and destination must be supported
Yahoo Messenger	TCP: 5050, 80 or any available	Internet Default

Note: Some port numbers listed in this section were previously unassigned by IANA, but have been recently assigned and now belong to another application. RTP & Quicktime both list 6970 - 6999, IANA has now assigned 6998 & 6999 to iatp-highpri and iatp-normalpri. CableHome makes no attempt to correct his conflict.

IV.3 Application Requiring Firewall Policy and an ALG

There are many cases in which the CAT and Firewall can not provide the application and protocol transparency desired. Since CAT modifies end node addresses (within the IP header of a packet) en-route, some applications are unable to function through the CAT without the assistance of an ALG.. Where

EXHIBIT A

possible, application specific ALGs MUST be used in conjunction with CAT and the appropriate Firewall policy to provide the desired application level transparency. The function of an ALG is application specific, so a list of applications, protocols and the scenarios that MUST be supported is found below.

Table IV-2 – Apps requiring Firewall policy and an ALG

Application / Protocol	**Ports**	**(1) One to One Single**	**(2) One to One Multi**	**(3) One to Many Single**	**(4) One to Many Multi**	**(5) Many to One Single**	**(6) Many to One Multi**	**Comments**
FTP	20/tcp, 21/tcp	X	X	X	X	X	X	
Microsoft Netmeeting (H.323)	TCP/389 ILS 522 ULS 1503 T.120 1720 call setup 1731 audio call ctrl Dynamic TCP call control Dynamic UDP 1024-65535 RTP over UDP	X	X	X	X	X	X	
MSN Messenger (H.323)	1863/tcp	X	X	X	X	X	X	Internet Default
Net2Phone	6801/udp (also calls for opening 2 additional unspecified ports UDPPORT=6801 UDPPORT=XXXX TCPPORT=XXXX The Network Administrator needs to make sure UDPPORT 6801 is open. For the other UDPPORT and TCPPORT, the administrator can use anything in the range from 1 - 30000.)	X	X	X	X			
Quicktime 5	RTSP/TCP/554 RTP/UDP 6970-6999	X	X	X	X	X	X	Supporting Quicktime without an ALG via port 80 provides less than optimal performance
Window Messenger (SIP)		X	X					Available on Windows XP only

EXHIBIT A

Appendix V CableHome Media Access Priority Mapping Examples

CableHome 1.1 defines a prioritized QoS system in which traffic over the shared media is prioritized based on the assigned packet priority. Since different shared media technologies support varying numbers of media access priorities, CableHome 1.1 defines a mapping scheme to translate Generic CableHome Priorities to a set of values called CableHome Media Access Priorities. CableHome Media Access Priority values describe the level of preference that a packet should get when accessing the shared media. The number of preference levels correspond to the available number of media access priorities supported by a given media technology. The higher the CableHome Media Access priority value for the packet, the higher the preference it should get to access the shared media. CableHome Media Access Priority mapping is separate and distinct from native media access priority mappings defined for the shared media technologies. These native mappings are accomplished at layer-2 of each device. Therefore, regardless of the shared media technology, the packets must be given the desired relative preferential access to the shared media, as required by the CableHome Media Access Priority mapping. Table V-1, Table V-2, and Table V-3 provide mapping examples for a few of the shared media access technologies.

V.1 Ethernet

Ethernet does not provide differentiation between packets and hence only supports one priority.

Table V-1 – Ethernet Mappings

Generic CableHome Priority	CableHome Media Access Priority mapping	Native Ethernet Media Access priority mapping
0	0	0
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0

As shown in Table V-1, no special mapping adjustments are required.

V.2 HomePlug

HomePlug supports 4 media access priorities.

Table V-2 – HomePlug Mappings

Generic CableHome Priority	CableHome Media Access Priority mapping	Native HomePlug Media Access priority mapping
0	0	1
1	0	0

EXHIBIT A

Generic CableHome Priority	CableHome Media Access Priority mapping	Native HomePlug Media Access priority mapping
2	1	0
3	1	1
4	2	2
5	2	2
6	3	3
7	3	3

As shown in Table V-2, HomePlug mapping gives channel access preference to Generic CableHome Priority 0, relative to Generic CableHome Priorities 1 and 2. However, CableHome Media Access Priority mapping requires that Generic CableHome Priority 2 be given higher access, relative to Generic CableHome Priorities 0 and 1, and Generic CableHome Priorities 0 and 1 be given equal access rights. Hence, the vendor must insure that the packets are given the desired relative preferential access to the shared media as required by the CableHome Media Access Priority mapping.

V.3 HomePNA

HomePNA supports 8 media access priorities.

Table V-3 – HomePNA Mappings

Generic CableHome Priority	CableHome Media Access Priority mapping	Native HomePNA Media Access priority mapping
0	0	2
1	1	0
2	2	1
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7

As shown in Table V-3, HomePNA mapping gives channel access preference to Generic CableHome Priority 0 relative to Generic CableHome Priorities 1 and 2. However, CableHome Media Access Priority mapping requires that Generic CableHome Priority 2 be given higher access relative to Generic CableHome Priorities 0 and 1, and Generic CableHome Priority 1 be given higher access relative to Generic CableHome Priority 0. Hence, the vendor must insure that the packets are given the desired relative preferential access to the shared media as required by the CableHome Media Access Priority mapping.

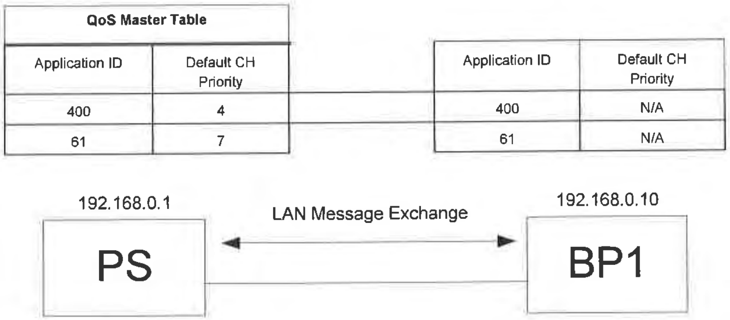
EXHIBIT A

Appendix VI LAN Management Message Example[151]

This appendix shows examples of BP_Init and BP_Init_Response messages. The format of BP_Init and BP_Init_Response messages is defined in Section 6.3.3.4.4.2.1 BP_Init Message Format and Section 6.3.3.4.4.2.2 BP_Init_Response Message Format respectively. The examples in this appendix are created according to the format definitions.

VI.1 Initial LAN Message

This section illustrates BP_Init and BP_Init_Response messages exchanged between a PS and a BP just after the BP receives DHCP ACK. Figure VI-1 describes the parameters used for the examples of BP_Init and BP_Init_Response messages. In Figure VI-1, BP1 sends the BP_Init message described in Section VI.1.1 after receiving DHCP ACK sent by PS, and PS sends the BP_Init_Response message described in Section VI.1.2 after receiving the BP_Init message sent by BP1. The BP can set any value for DefaultCHPriority tags in a BP_Init message. However, the PS overwrites this value set for DefaultCHPriority in the BP_Init_Response message after consulting with the priority master table. The values for DefaultCHPriority tags are left blank in the following example of a BP_Init message in Section VI.1.1.



QoS Master Table

Application ID	Default CH Priority
400	4
61	7

Application ID	Default CH Priority
400	N/A
61	N/A

Figure VI-1 — Initial LAN Message Exchange

VI.1.1 Initial BP_Init Message

```
POST /DevQoSProfileService HTTP/1.1
HOST: 192.168.0.1
Content-Type: text/xml; charset="utf-8"
Content-Length: 1584
SOAPAction: "/DevQoSProfileService"

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

   <SOAP-ENV:Body>
     <ch:BP_Init xmlns:m="192.168.0.1">
        <ch:BP_IP>
```

[151] Added this new Appendix per ECN CH1.1-N-03068 by GO on 10/31/03.

EXHIBIT A

```
            192.168.0.10
         </ch:BP_IP>
         <ch:DeviceProfile>
            <ch:deviceType>CableHome Host</ch:deviceType>
            <ch:manufacturer>ABC Corporation</ch:manufacturer>
            <ch:manufacturerURL>www.xyz.com</ch:manufacturerURL>
            <ch:hardwareRevision>Second</ch:hardwareRevision>
            <ch:hardwareOptions>802.11 a/b/g</ch:hardwareOptions>
            <ch:serialNumber>CH1234</ch:serialNumber>
            <ch:modelName>ABC IP Camera</ch:modelName>
            <ch:modelNumber>ABC7463</ch:modelNumber>
            <ch:modelURL>www.xyz.com/abcipcamera/</ch:modelURL>
            <ch:modelUPC>3838XZAYS</ch:modelUPC>
            <ch:modelSoftwareOS>VS Works</ch:modelSoftwareOS>
            <ch:modelSoftwareVersion>1.2</ch:modelSoftwareVersion>
            <ch:lanInterfaceType>71</ch:lanInterfaceType>
            <ch:numberMediaAccessPriorities>4</ch:numberMediaAccessPriorities>
            <ch:physicalLocation>Living Room</ch:physicalLocation>
            <ch:physicalAddress>01:02:03:45:67:CD</ch:physicalAddress>
         </ch:DeviceProfile>
         <ch:QoSProfile>
            <ch:QoSApplicationListEntry>
               <ch:BpIpAddress>192.168.0.10</ch:BpIpAddress>
               <ch:ApplicationId>400</ch:ApplicationId>
               <ch:DefaultCHPriority></ch:DefaultCHPriority>
            </ch:QoSApplicationListEntry>
            <ch:QoSApplicationListEntry>
               <ch:BpIpAddress>192.168.0.10</ch:BpIpAddress>
               <ch:ApplicationId>61</ch:ApplicationId>
               <ch:DefaultCHPriority></ch:DefaultCHPriority>
            </ch:QoSApplicationListEntry>
         </ch:QoSProfile>
      </ch:BP_Init>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

VI.1.2 Initial BP_Init Response Message[152]

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/xml; charset="utf-8"
Content-Length: 817

<SOAP-ENV:Envelope
 xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
 SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <ch:BP_Init_Response xmlns:m="192.168.0.1">
      <ch:BPInitConfirmationCode>0</ch:BPInitConfirmationCode >
         <ch:QoSProfile>
         <ch:QoSApplicationListEntry>
            <ch:BpIpAddress>192.168.0.10</ch:BpIpAddress>
            <ch:ApplicationId>400</ch:ApplicationId>
```

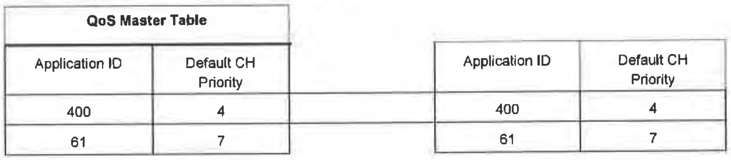
[152] Revised this section per ECN CH1.1-N-03.0087-4 by GO on 12/8/03.

EXHIBIT A

```
            <ch:DefaultCHPriority>4</ch:DefaultCHPriority>
          </ch:QoSApplicationListEntry>
          <ch:QoSApplicationListEntry>
            <ch:BpIpAddress>192.168.0.10</ch:BpIpAddress>
            <ch:ApplicationId>61</ch:ApplicationId>
            <ch:DefaultCHPriority>7</ch:DefaultCHPriority>
          </ch:QoSApplicationListEntry>
        </ch:QoSProfile>
      </ch:BP_Init_Response>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```

VI.2 LAN Message on Session Establishment

This section illustrates BP_Init and BP_Init_Response messages exchanged between a PS and a BP when the BP establishes a session with another host. Figure VI-2 describes the parameters used for the examples of BP_Init and BP_Init_Response messages. In Figure VI-2, BP1 sends the BP_Init message described in Section VI.2.1 after BP1 establishes sessions with BP2 and BP3, and PS sends the BP_Init_Response message described in Section VI.2.2 after receiving the BP_Init message sent by BP1. The BP can set any value for IpPortPriority tags in a BP_Init message. However, the PS overwrites this value set for IpPortPriority in the BP_Init_Response message after consulting with the priority master table. The values for IpPortPriority tags are left blank in the following example of a BP_Init message in Section VI.2.1.



QoS Master Table

Application ID	Default CH Priority
400	4
61	7

Application ID	Default CH Priority
400	4
61	7

EXHIBIT A

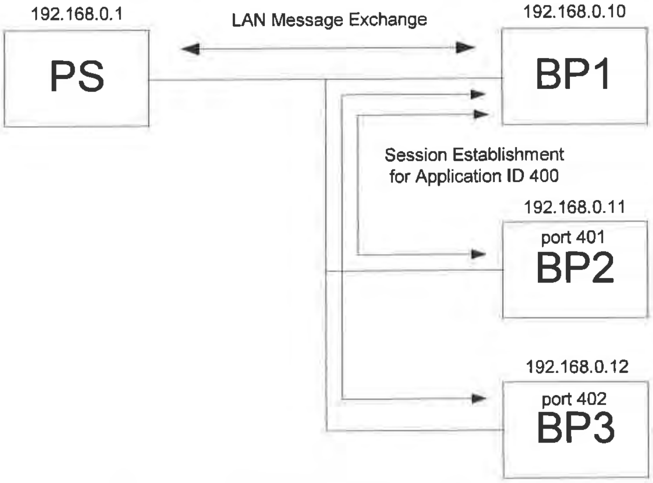


Figure VI-2 — LAN Message Exchange on Session Establishment

VI.2.1 1 BP_Init Message on Session Establishment

```
POST /DevQoSProfileService HTTP/1.1
HOST: 192.168.0.1
Content-Type: text/xml; charset="utf-8"
Content-Length: 1920
SOAPAction: "/DevQoSProfileService"

<SOAP-ENV:Envelope
 xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
 SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
   <SOAP-ENV:Body>
      <ch:BP_Init xmlns:m="192.168.0.1">
         <ch:BP_IP>
            192.168.0.10
              </ch:BP_IP>
              <ch:DeviceProfile>
                <ch:deviceType>CableHome Host</ch:deviceType>
                <ch:manufacturer>ABC Corporation</ch:manufacturer>
                <ch:manufacturerURL>www.xyz.com</ch:manufacturerURL>
                <ch:hardwareRevision>Second</ch:hardwareRevision>
                <ch:hardwareOptions>802.11 a/b/g</ch:hardwareOptions>
                <ch:serialNumber>CH1234</ch:serialNumber>
                <ch:modelName>ABC IP Camera</ch:modelName>
                <ch:modelNumber>ABC7463</ch:modelNumber>
                <ch:modelURL>www.xyz.com/abcipcamera/</ch:modelURL>
                <ch:modelUPC>3838XZAYS</ch:modelUPC>
                <ch:modelSoftwareOS>VS Works</ch:modelSoftwareOS>
                <ch:modelSoftwareVersion>1.2</ch:modelSoftwareVersion>
```

EXHIBIT A

```
            <ch:lanInterfaceType>71</ch:lanInterfaceType>
            <ch:numberMediaAccessPriorities>4</ch:numberMediaAccessPriorities>
            <ch:physicalLocation>Living Room</ch:physicalLocation>
            <ch:physicalAddress>01:02:03:45:67:CD</ch:physicalAddress>
          </ch:DeviceProfile>
          <ch:QoSProfile>
            <ch:QoSApplicationListEntry>
              <ch:BpIpAddress>192.168.0.10</ch:BpIpAddress>
              <ch:ApplicationId>400</ch:ApplicationId>
              <ch:DefaultCHPriority>4</ch:DefaultCHPriority>
              <ch:DestPriorityListEntry>
                <ch:DestIp>192.168.0.11</ch:DestIp>
                <ch:DestPort>401</ch:DestPort>
                <ch:IpPortPriority></ch:IpPortPriority>
              </ch:DestPriorityListEntry>
              <ch:DestPriorityListEntry>
                <ch:DestIp>192.168.0.12</ch:DestIp>
                <ch:DestPort>402</ch:DestPort>
                <ch:IpPortPriority></ch:IpPortPriority>
              </ch:DestPriorityListEntry>
           </ch:QoSApplicationListEntry>
           <ch:QoSApplicationListEntry>
             <ch:BpIpAddress>192.168.0.10</ch:BpIpAddress>
             <ch:ApplicationId>61</ch:ApplicationId>
             <ch:DefaultCHPriority>7</ch:DefaultCHPriority>
          </ch:QoSApplicationListEntry>
        </ch:QoSProfile>
      </ch:BP_Init>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```

VI.2.2 BP_Init_Response message on Session Establishment[153]

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/xml; charset="utf-8"
Content-Length: 1153

<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
    <SOAP-ENV:Body>
      <ch:BP_Init_Response xmlns:m="192.168.0.1">
      <ch:BPInitConfirmationCode>0</ch:BPInitConfirmationCode >
      <ch:QoSProfile>
        <ch:QoSApplicationListEntry>
          <ch:BpIpAddress>192.168.0.10</ch:BpIpAddress>
          <ch:ApplicationId>400</ch:ApplicationId>
          <ch:DefaultCHPriority>4</ch:DefaultCHPriority>
          <ch:DestPriorityListEntry>
            <ch:DestIp>192.168.0.11</ch:DestIp>
            <ch:DestPort>401</ch:DestPort>
            <ch:IpPortPriority>4</ch:IpPortPriority>
```

[153] Revised this section per ECN CH1.1-N-03.0087-4 by GO on 12/8/03.

EXHIBIT A

```
          </ch:DestPriorityListEntry>
          <ch:DestPriorityListEntry>
            <ch:DestIp>192.168.0.12</ch:DestIp>
            <ch:DestPort>402</ch:DestPort>
            <ch:IpPortPriority>4</ch:IpPortPriority>
          </ch:DestPriorityListEntry>
        </ch:QoSApplicationListEntry>
        <ch:QoSApplicationListEntry>
          <ch:BpIpAddress>192.168.0.10</ch:BpIpAddress>
          <ch:ApplicationId>61</ch:ApplicationId>
          <ch:DefaultCHPriority>7</ch:DefaultCHPriority>
        </ch:QoSApplicationListEntry>
      </ch:QoSProfile>
    </ch:BP_Init_Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

EXHIBIT A

Appendix VII Bibliography (informative)

ICSA, "3rd Annual Firewall Buyer's Guide" : http://www.icsalabs.com/html/communities/firewalls/buyers_guide/FWguide99.pdf.

RFC 2979, N. Freed, "Behavior of and Requirements for Internet Firewalls", October 2000.

EXHIBIT A

Appendix VIII Acknowledgements (informative)

This technical report was developed and influenced by numerous individuals representing many different organizations. CableHome hereby wishes to thank everybody who participated directly or indirectly in this effort. In particular, CableHome wishes to recognize the following individuals for their significant involvement and contributions to this technical report.

Shekar Annambhotla	Alopa
Michael Walters	Arris Interactive
Rick Chen	Askey
Scott Higgins	Ashley Laurent
Chris Zacker	Broadcom
Jeff Carr	Broadcom
Jim Hinsey	Broadcom
Stephen Palm	Broadcom
Terry Wright	Broadband Home
Amol Bhagwat	CableLabs
Eduardo Cardona	CableLabs
Kevin Luehrs	CableLabs
Oscar Marcia	CableLabs
Michael Mannette	CableLabs
Ralph Brown	CableLabs
Rick Vetter	CableLabs
Roy Spitzer	CableLabs
Steven Saunders	CableLabs
Stuart Hoggan	CableLabs
Joubin Karimi	Cogency
Carlos Pazos	Conexant
Stephen Wasson	Conexant
David Laird	Com21
Wes Peters	DoBox, Inc.
Christian Kurzke	Gatespace
Damon Jones	Gatespace
Dimitrii Loukianov	Intel
Narm Gadiraju	Intel
Randy Dunton	Intel
Raj Bopardikar	Intel
Aidan Shribman	Jungo
Allen Huotari	Linksys
Jed Johnson	Motorola
Kevin Burak	Motorola
Martin Freeman	Philips
Kyung Hee Lee	Samsung
Joe Tzou	SMC/Accton
Jerod Munson	SMC
Gale Moyer	SOHOware
Yong Ho Son	SOHOware
Jason Schnitzer	Stargus
Majid Chelehmal	Terayon
Diego Mazzola	Texas Instruments
Itay Sherman	Texas Instruments
Jeff Mandin	Texas Instruments
David Ryan	Thomson

EXHIBIT A

Mark Mayernick	Thomson
Junichi Takahashi	Toshiba
Paul Ducharme	ViXS
Jack Chen	Xanboo
Doug Jones	YAS Broadband Ventures
John Bevilacqua	YAS Broadband Ventures
Liz Weeks	YAS Broadband Ventures
Nancy Davoust	YAS Broadband Ventures

EXHIBIT A

Appendix IX Revisions (informative)

IX.1 ECNs Incorporated into CH-SP-CH1.1-I02-030801

Table IX-1 – ECNs Incorporated into CH-SP-CH1.1-I02-030801

ECN	Date Accepted	Description
CH1.1-N-03029	5/29/03	Correct reference to Table 7-7 and remove duplicate PICS in Section 7.3.3.2.4
CH1.1-N-03030	5/29/03	Remove DHCP DISCOVER retry description
CH1.1-N-03032	6/5/03	Remove duplicate CVC configuration file requirements
CH1.1-N-03035	7/3/03	This ECR further clarifies how the cabhSec2FwPolicyFileURL mib should be handled when a firewall config file download fails. To support this clarification, the conditions that trigger a firewall config file download were also changed.
CH1.1-N-03039	6/19/03	Update 'Type' field for DHCP Option 177 sub-option 3.
CH1.1-N-03046	7/3/03	Remove PICS duplication in Section 13
CH1.1-N-03048	7/3/03	Clarification on how different DHCP options need to be included in the DHCP DISCOVER and DHCP REQEST messages by the CDC.
CH1.1-N-03051	7/3/03	Addition of two new QoS MIB objects and changes to reflect the new PsDev MIB in the Appendix I.
CH1-N-O2070	1/30/03	Change #3 correctly implemented in this iteration of the specification
CH1.1-N-03059	7/31/03	Update Appendix I MIB list to incorporate changes in CableHome MIBs

IX.2 ECNs Incorporated into CH-SP-CH1.1-I03-040123

Table IX-2 – ECNs Incorporated into CH-SP-CH1.1-I03-040123

ECN	Date Accepted	Description
CH1.1-N-03044	7/10/03	Spec out format and encoding of DHCP option 43 suboptions
CH1.1-N-03056	8/7/03	The string "PSElement" is too long in the PS Element principal name.
CH1.1-N-03060	10/23/03	This ECR defines the transport to be used for the device discovery message exchange.
CH1.1-N-03061	10/2/03	This ECR defines the identifier for an ICMP session.
CH1.1-N-03063	9/25/03	This ECN addresses various editorial changes needed in Section 7 to improve the document.
CH1.1-N-03065	10/2/03	The inclusion of option (50) , Requested Ip Address should not be mandatory to be sent in the CDC DHCP DISCOVER.
CH1.1-N-03068	10/23/03	This ECR adds more clarification on Device Profile and QoS Profile XML schema. Add new Appendix VI, LAN Management Message Example.

EXHIBIT A

ECN	Date Accepted	Description
CH1.1-N-03069	10/23/03	Clarifies specification text for the following items: TLV format; ipNetToMediaTable; Event Priority Table; DHCP Option 43.101 string; Firewall Configuration File download success Event ID; BP DHCP Option 60 string.
CH1.1-N-03071	10/23/03	Inconsistency of encapsulating tag of device profile. Inconsistancy of XML schema sections header.
CH1.1-N-03070	11/13/03	Update references and add requirement for PS to pass all OSI Layer 2 frames that a DOCSIS cable modem is required to pass.
CH1.1-N-03.0074-3	12/4/03	PS Element Certificate and HTTPS Server Certificate modification for TLS.
CH1.1-N-03.0077-4	11/26/03	Clarifies the specification to indicate that the PS must only support a single IP address assigned to its LAN-side TCP/IP stack. Clarifies what is expected to be represented in the PS's ipNetToMediaTable.
CH1.1-N-03078	11/6/03	Correct CableLabs CVC CA certificate references and typographical errors, remove table that duplicates CVC spec text, and clarify CVC structure requirements.
CH1.1-N-03.0087-4	12/4/03	Clarification on the content of BP_Init messages and the use of confirmation codes.
CH1.1-N-03.0089-2	11/26/03	Correct BP_Init and BP_Init_Response message formats.
CH1.1-N-03.0090-2	12/4/03	Clarify usage of vendor specific graphical user interfaces.
CH1.1-N-03.0091-1	12/4/03	Correct incorrect references to Software Download section and remove unused footnote reference.
CH1.1-N-03.0092-4	12/4/03	Adding specification text requiring the PS to create an IP address lease reservation when a DMZ entry (wild-card static port forwarding entry) is created in the CAP table for a dynamically assigned IP address only and clarifying the DMZ functionality text.
CH1.1-N-03.0093-2	12/4/03	Clarification of the format of Vendor-specific TLV information and how the PS handles them.
CH1.1-N-03.0097-5	12/4/03	Modifications to the CableHome Firewall
CH1.1-N-03.0099-3	12/4/03	Correct and clarify Time of Day requirements, remove references to unused Provisioning Timer, clarify PS behavior for IP address lease renewal, clarify conditions for PS configuration file download trigger and for software upgrade trigger, remove redundant TLS Session Teardown requirement, and correct typos.
CH1.1-N-03.0100-1	12/4/03	Clarification on DefaultCHPriority and IpPortPriority elements in a QoS Profile.
CH1.1-N-03.0103-3	12/4/03	Define a new TLV Type for SNMP Sets to be processed before TLV-28.
CH1.1-N-03.0104-2	12/4/03	Clarification to the specification text regarding cabhCdpServerRouter, CabhCdpServerDnsAddress, cabhCdpServerDhcpAddress in various sections due to the changes proposed in the CDP MIB ECR, CH-MIB-R-03076.
CH1.1-N-03.0105-2	12/4/03	Update MIB objects listed in Appendix I

EXHIBIT A

IX.3 ECNs Incorporated into CH-SP-CH1.1-I04-040409

Table IX-3 – ECNs Incorporated into CH-SP-CH1.1-I04-040409

ECN	Date Accepted	Description
CH1.1-N-03.0106-2	12/23/03	Modifications to CTP Ping Tool requirements
CH1.1-N-03.0107-1	12/23/03	Modifications to CTP requirements: Connection Speed Tool
CH1.1-N-03.0109-1	12/18/03	Clarify that the ApplicationId in the QoSProfile can be other than a well-known port number assigned by IANA and related clean-up
CH1.1-N-03.0112-1	1/8/04	Add RFC 3396 to References section
CH1.1-N-04.0115-1	3/11/04	Add parameters to the firewall Type 4 event to specify the reason for failure
CH1.1-N-04.0120-2	3/11/04	Addition of Central CA Option
CH1.1-N-04.0123-2	3/11/04	Misc Firewall Corrections

EXHIBIT A

Home Member Login Broadband Supplier Login Contact Us Site Map

CableLabs®
...Revolutionizing Cable Technology®

Search

About CableLabs | Members' Area | Current Projects | Certification & Qualification | Join CableLabs | News Room | Conferences | CableNET®

Cable Modem/DOCSIS® CableHome® PacketCable™ OpenCable™ Go2Broadband℠ VOD Metadata

CableHome®

News and Events

Click here to go to the CableHome archived press releases.

12/09/04	CableLabs® Certifies Four CableHome® 1.1 Devices
11/29/04	CableLabs® Issues RFP for CableHome® Residential Gateway
08/16/04	CableLabs® Certifies Two CableHome® 1.1 Devices
06/25/04	CableLabs® Certifies Two CableHome™ 1.1 Devices
04/16/04	Milestone CableHome™ 1.1 Certification Issued

Participant Login

- » Project Home
- » Specifications
- » Documents
- » Certification Testing
- » News & Events
- » How to Participate
- » FAQ
- » Glossary
- » Careers
- » Contact CableHome

Copyright | Privacy Policy | Site Map | Contact

EXHIBIT A

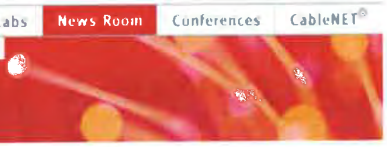
Home Member Login Broadband Supplier Login Contact Us Site Map

CableLabs®
...Revolutionizing Cable Technology®

Search

About CableLabs | Members' Area | Current Projects | Certification & Qualification | Join CableLabs | News Room | Conferences | CableNET®

Press Releases **Who's CableLabs Certified?** **Newsletters**



PRESS RELEASES

Contact:

Mike Schwartz
CableLabs
858 Coal Creek Circle
Louisville, CO 80027-9750
303.661.9100
Contact Mike Schwartz

2004 Press Releases
2003 Press Releases
2002 Press Releases
2001 Press Releases
2000 Press Releases
1999 Press Releases
1998 Press Releases
1997 Press Releases
1996 Press Releases
1995 Press Releases
1994 Press Releases

CableLabs® Issues RFP for CableHome® Residential Gateway

Louisville, Colorado, November 29, 2004 - Key cable operators have teamed with CableLabs® to issue a request for proposal (RFP) that identifies a common set of product requirements for a CableHome®-based residential gateway (integrated cable modem and router/wireless access device). The deadline for responses is January 31, 2005.

CableLabs and its member companies are working to gather information about a residential gateway that will comply with CableHome 1.1 specifications. The gateway will enable the delivery of value-added services for home networking and high-speed data service subscribers, including but not limited to, services requiring quality of service (QoS) guarantees.

By providing a common set of technical requirements for a residential gateway, CableLabs anticipates that enough scale will be provided to enable suppliers to offer this product economically and in a timely manner. Any questions or comments should be directed to Cynthia Metsker in the Broadband Access Department at CableLabs.

Consistent with CableLabs' participation in the Universal Plug and Play (UPnP™) Forum Steering Committee, and with the adoption of UpnP functionality as part of the CableHome 1.1 specification requirements, the RFP includes requirements for residential gateways to implement discovery, prioritized QoS, and Network Address Translation configuration features as defined by UPnP specifications.

"CableHome is one of the ways the cable industry continues to differentiate itself - by enabling seamless connectivity among multiple devices in the home, while also making the experience easy and intuitive for the consumer," said Jeff Austin, Senior Director of New Product Deployments at Comcast Online, the high-speed Internet division of Comcast Cable. "The industry recognizes the importance of CableHome and its key role in positioning cable as the '*platform of choice for the connected home.*' This industry-supported RFP is testament to this and comes at a key moment in the evolution of broadband service delivery," Austin added.

"As cable moves into this new business, having a set of gateways that adhere to our unique requirements will facilitate innovation that will drive a new way of serving the cable consumer in their home," said Mark Bell, Director of Product Development at Cox Communications.

About CableHome
CableLabs and the cable industry have developed the CableHome specification based on consumer research, which identified the need for an interoperable platform that would:

- Enable cable service providers to take care of the technology part of the home networking equation, giving customers the choice to simply focus on enjoying the experience.
- Help speed the development of advanced broadband applications and devices for the home.
- Ensure true seamless integration among these devices.

Founded in 1988 by members of the cable television industry, Cable Television Laboratories is a non-profit research and development consortium that is dedicated to pursuing new cable telecommunications technologies and to helping its cable operator members integrate those advancements into their business objectives. Cable operators from around the world are members. CableLabs maintains web sites at www.cablelabs.com; www.packetcable.com; www.cablemodem.com; www.cablenet.org; and www.opencable.com.

CableLabs®, DOCSIS®, CableHome™, PacketCable™, OpenCable™, OCAP™, CableCARD™, Go2BroadbandSM and CableNET® are marks of Cable Television Laboratories, Inc. All other marks are the property of their respective owners.

UpnP is a certification mark owned and managed by the UpnP Implementers Corp.

EXHIBIT A

Copyright | Privacy Policy | Site Map | Contact

EXHIBIT A

http://web.archive.org/web/20041222135053/http://cablelabs.com/projects/cablehome/downloads/CH_RG_RFP.pdf

EXHIBIT A

CableLabs®

CableHome® Residential Gateway

Request For Proposal

November 24, 2004

Cable Television Laboratories, Inc.
858 Coal Creek Circle
Louisville CO 80027-9750
Phone: (303) 661-9100
Fax: (303) 661-9199
http://www.cablelabs.com

EXHIBIT A

DISCLAIMER

This document is published by Cable Television Laboratories, Inc. ("CableLabs®"). CableLabs® reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various agencies; technological advances; or changes in equipment design, manufacturing techniques or operating procedures described or referred to herein.

CableLabs® makes no representation or warranty, express or implied, with respect to the completeness, accuracy or utility of the report or any information or opinion contained in the report. Any use or reliance on the information or opinion is at the risk of the user, and CableLabs® shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy or utility of any information or opinion contained in the report.

This document is not to be construed to suggest that any manufacturer modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs® or any member to purchase any product whether or not it meets the described characteristics. Nothing contained herein shall be construed to confer any license or right to any intellectual property, whether or not the use of any information herein necessarily utilizes such intellectual property.

This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

November 24, 2004

EXHIBIT A

Request for Proposal

CableHome Residential Gateway

November 24, 2004

1 Overview

CableLabs is working with its members to collect information from you and other manufacturers regarding CableHome® Residential Gateways (hereinafter referred to as a "Residential Gateway") that comply with CableLabs' CableHome specifications as well as the specific requirements listed herein. The purpose of this RFP is to identify Residential Gateways that will enable the delivery of value added services for home networking and high speed data service subscribers, including but not limited to, services requiring quality of service guarantees. The Residential Gateway described in this RFP is expected to meet the current needs of many cable operators. By providing a common set of requirements for Residential Gateways, CableLabs anticipates that this may provide enough scale that it will enable a vendor(s) to economically offer this product in a timely manner. CableLabs and CableLabs' members will review your responses to the technical information requested in Section A below ("Technical Information"). Respondents to this Request for Proposals ("RFP") may be receiving from CableLabs feedback as to the responsiveness of their Technical Information responses as well as any specific technical questions from CableLabs' members. There will be no ranking of responses or an "approved vendor list" resulting from this RFP.

In addition to the Technical Information, CableLabs' members would like to receive proposed Residential Gateway sales information, as listed in Section B below ("Sales Information"). **Your responses to the statements in Section B are to be sent only to the CableLabs' members listed in Section B**, who will then make their own, independent business judgments and purchasing decisions. Your responses to the statements in Section B are **not** to be sent to CableLabs. In the event you inadvertently send responses to Section B to CableLabs, CableLabs will not review your responses. All Sales Information sent CableLabs' members shall be considered offers, although CableLabs' members are not bound to accept such offers. The offer containing the Sales Information must remain valid for a period of one hundred and twenty (120) days after January 31, 2005.

CableLabs shall incur no obligation or liability arising from or related to the issuance of this RFP.

CableLabs reserves the right to extend or shorten the time schedule, as necessary, or cancel the RFP completely. The schedule may be altered to take into account any necessary clarification as well as time needed to accomplish the various levels of review. Manufacturers will be notified of any change in the schedule.

Within this RFP, statements that contain "MUST" are requirements, and responses should be in the form of "comply" or "non-comply" with explanation. Statements that contain "SHOULD" are recommended or desired, and responses should be in the form of "comply" or "non-comply" with explanation.

Residential Gateways may be selected for further evaluation and/or for validation testing against the responses to this RFP. It is at CableLabs' discretion to conduct a technical evaluation or to discontinue the technical evaluation of a Residential Gateway. Any technical evaluation of Residential Gateway is to evaluate the Residential Gateway features and is not a substitute for CableLabs certification testing.

2 Confidentiality

CableLabs intends to share your technical responses to this RFP with our member companies. While CableLabs does not intend to share your responses with any other vendor, if your response contains confidential information, CableLabs can offer no assurances that the confidentiality of such will be maintained.

3 Proposal Submission and Timing

The following section provides specific instructions with respect to completing and submitting the proposal response for CableLabs. The completed proposal is due by the close of business on January 31, 2005. A complete proposal includes sending separate pricing information to CableLabs' members.

3.1 Intention to Bid

All prospective Vendors intending to submit a response to the Request for Proposal (RFP) should inform CableLabs in writing by the close of business on December 17, 2004. Notification of intention to bid shall be made by certified mail or by nationally recognized courier such as Federal Express, UPS or Airborne Express to the address listed below. Any Vendor that submits a response to this RFP agrees to provide the technical response and sales information to any CableLabs' member that requests it.

Decisions not to bid will not prejudice the non-bidding company in any way. It is requested that companies electing not to bid inform the CableLabs as soon as possible.

3.2 Proposal Schedule and Delivery

Proposal Schedule	
Activity	Due Date
RFP Sent	November 24, 2004
Intent to Bid Letter	December 17, 2004
Proposal Due	January 31, 2005

CableLabs reserves the right to change the schedule. All response material will be expected by specific dates. No response or additional material will be accepted after the specified dates.

Deliver two (2) paper copies and one (1) electronic copy of your proposal to the following address no later than January 31, 2005. Vendor assumes all risk of loss in the delivery of its proposal. While CableLabs will use best efforts to safeguard proposals in its possession, custody or control, CableLabs assumes no responsibility for lost or misdirected Vendor proposals.

Cynthia Metsker
Cable Television Laboratories, Inc.
858 Coal Creek Circle
Louisville, Colorado 80027-9750
c.metsker@cablelabs.com

3.3 RFP Questions

Questions regarding this RFP should be submitted in writing via hard copy and electronic copy to:

Cynthia Metsker
Cable Television Laboratories, Inc.
858 Coal Creek Circle
Louisville, Colorado 80027-9750
Fax: 303 661 9199
c.metsker@cablelabs.com

Questions received will be answered in writing. Answers to questions from any vendor will be provided to all vendors. No further questions will be accepted after 12 p.m. (Mountain) on January 21, 2005. Please provide the name, address, telephone, e-mail addresses, and fax numbers for the vendor contact that should receive answers to questions.

EXHIBIT A

SECTION A: TECHNICAL REQUIREMENTS (to be sent to CableLabs and to CableLabs' Members listed in Section B)

4 Product Requirements

Each response is required to address the Hardware requirements listed in Section 4.1 and the Software requirements listed in Section 4.2, plus one of the product profiles listed in Section 4.3.

4.1 Hardware

1. MUST have four RJ-45 10/100 auto-sensing Ethernet, full-duplex ports
2. MUST have an embedded DOCSIS 2.0 certified cable modem
3. MUST have a recessed physical Reset to Factory button
4. MUST have a USB 2.0 LAN client interface

4.2 Software

1. MUST be CableHome 1.1 certified
2. MUST be compliant with CableLabs eDOCSIS specification
3. MUST be compliant with CableLabs CableOffice™ Commercial Services Annex (CSA) specification
4. MUST support XML format messaging
5. MUST implement CableHome-UPnP Quality of Service and Internet Gateway Device (IGD) features described the following CableHome 1.1 Engineering Changes:
   - MIB-PSDEV-x-04.0190
   - MIB-CAP-x-04.0191
   - CH1.1-x-04.0193
   - CH1.1-x-04.0194
   - CH1.1-x-04.0195
   - MIB-QOS-x-04.0196
   - CH1.1-x-04.0197
6. MUST implement a cable operator-branded Graphical User Interface accessible via HTTP with configurable parameters specified in the RFP (specifics TBD)
7. MUST support backup/restore of local settings. Specify how backup is done.
8. MUST support at least 16 DOCSIS Service Identifiers (SIDs)
9. SHOULD support URL filtering, domain name filtering, and keyword filtering parental control features.
10. SHOULD support VPN endpoint and VPN pass-through technologies. Describe VPN endpoint and VPN pass-through support.

11. MUST support multicast pass-through with MIBs to enable and disable the multicast pass-through feature. Describe multicast pass-through support.
12. MUST support Simple Traversal of UDP through NAT (STUN) for SIP [IETF RFC 3489]
13. Describe any additional software features not covered above.

4.2.1 Firmware Upgrade

The vendor may optionally provide functionality that permits upgrade of enhanced endpoints via the Residential Gateway. The process must be transparent to the end-user and must require minimal configuration from the WAN. If the upgrade process from the Residential Gateway is not possible the hardware manufacturer must provide an alternative such as an upgrade option via a software utility.

4.3 Product Profiles

Responses are required to include features from one of the three product profiles listed below, in addition to Hardware requirements listed in Section 4.1 and Software requirements listed in Section 4.2.

4.3.1 Wi-Fi Profile

4.3.1.1 Wi-Fi Profile Hardware Requirements

1. MUST have one embedded IEEE 802.11g interface with one fixed antenna

4.3.1.2 Wi-Fi Profile Software Requirements

1. MUST implement IEEE 802.11 *dot11* and CableHome *cabhPsDev802dot11* MIB objects as specified in the current CableHome 1.1 specification.
2. MUST support WPA, WEP, 64-bit encryption, and 128-bit encryption

4.3.2 HomePlug Profile

4.3.2.1 HomePlug Profile Hardware Requirements

1. MUST have one HomePlug 1.0 certified interface that establishes connectivity via the Residential Gateway power supply.
2. MUST have two LED indicators for displaying the status of the HomePlug network. Required HomePlug LED Indicator Behavior is described below.
3. SHOULD have sufficient memory to support upgrade to HomePlug 2.0 specifications
4. MUST be capable of supporting a minimum of sixteen (16) endpoints simultaneously however, only eleven (11) enhanced access point endpoints must be simultaneously supported in order to avoid 802.11b/g frequency overlap.

HomePlug LED Indicator Behavior

The Residential Gateway must have a single LED indicator reserved for the HomePlug interface. The LED must indicate the status of the HomePlug interface as indicated in Table 1.

Table 1. HomePlug LED Indicator

Value	LED Behavior
Residential Gateway HomePlug Interface Offline	Offline
Residential Gateway HomePlug Interface Initializing	Flashing State
Residential Gateway HomePlug Interface Initialized	Solid State

4.3.2.2 HomePlug Profile Software Requirements

1. MUST implement the HomePlug Management Information Base (MIB) described in Appendix I of this RFP.
2. MUST implement the HomePlug Functional Processes described in Appendix II of this RFP.

The gateway must be interoperable with all HomePlug 1.0 device types (enhanced and legacy). Specifically, the gateway must support setting the network password to any HomePlug 1.0 endpoints[1] and support XML format messaging to configure wireless security settings on Access Point type endpoints.

The XML messaging and schema will be distributed at a later date upon finalizing the requirements.

4.3.3 Wi-Fi and HomePlug Profile

Implement Wi-Fi Hardware and Software features listed in Section 4.3.1 and HomePlug Hardware and Software features listed in Section 4.3.2.

The RFP response should include a description of how the CableHome compliant residential gateway implementing a Wi-Fi interface will simultaneously satisfy the objectives listed below. The preferred solution will require no user intervention:

- Prevent interference between the residential gateway Wi-Fi interface and endpoints' Wi-Fi interfaces, such as might occur if the residential gateway's Wi-Fi interface and the endpoint's Wi-Fi interface are using the same channel (frequency) and SSID.
- Enable Wi-Fi mobile station handoffs between endpoints and between an endpoint and a residential gateway in a subscriber's premise.

[1] Reference section 3.9.4 Network Encryption Key Management of the HomePlug 1.0.1 specification

- Prevent unauthorized access to the subscriber's wireless LAN

5 Product Availability

1. Specify when Hardware with`Lab evaluation quality Software can be made available to cable operators.
2. Specify when Production Hardware with commercially available software can be made available to cable operators.

6 Documentation, Training and Customer Service Support

Please provide the following information related to documentation, training and support. Documents should be available in paper and electronic format. Submit quotation for documentation, training and customer service support independent of product quotation.

1. Vendor MUST provide a self-install CD with product. Describe features of the self-install CD in the response.
2. Vendor MUST provide an installation and configuration guide
3. Vendor MUST provide a software operations guide.
4. Vendor MUST provide a reference guide for the visible state indicators on the Residential Gateway
5. Vendor MUST provide a software operations guide including a reference guide for LED indicators
6. Vendor MUST provide onsite installation, operations and troubleshooting training for Field Service Representatives
7. Vendor MUST provide 24/7 technical support for cable operator customer service representatives
8. Describe support options available, i.e. telephone, web based, onsite engineer, etc.

7 Specification Compliance and Certification

7.1 Compliance

Describe the Residential Gateway's compliance with the following CableLabs specifications:

1. CableHome 1.1 certification wave (CW) 32 functionality including all CW mandated ECNs
2. DOCSIS 2.0 CW 32 functionality including all CW mandated ECNs

7.2 Certification

1. Proof of UL certification must be provided in the RFP response.

EXHIBIT A

SECTION B. SALES INFORMATION: Terms and Conditions, Warranty and Pricing

8 Sending Responses

Responses to the following are to be sent to these CableLabs' members at the following addresses:

1. Brian Martone
   Senior Manager
   Comcast Cable Communications, LLC
   1500 Market Street, 9th Floor West Tower
   Philadelphia, PA 19102

2. Malcolm Stanley
   Senior Director Product Development
   Rogers Cable Communications
   333 Bloor Street East
   Toronto, ON M4W 1G9

3. Mark Bell
   Product Development Manager
   Cox Communications
   1400 Lake Hearn Drive NE
   Atlanta, GA 30319

4. Fred Pappalardo
   VP Corporate Development
   Finance
   Time Warner Cable
   290 Harbor Drive
   Stamford, CT 06902-6732

5. Ron Vought
   Manager – IP Broadband Engineering & Operations
   Adelphia Communications
   512 Bank Street
   Coudersport, PA 16915

6. Michael Giobbi
   VP Engineering & Technology

Armstrong Holdings, Inc.
One Armstrong Place
Butler, PA 16001

7. Andrej Copic
Systems Engineer
Cogeco Cable, Inc.
PO Box 5076 Station Main
Burlington, ON L7R 4S6

8. Bob King
Director Broadband Projects
Charter Communications
6th Floor, Fiddlers Green Center
6399 South Fiddlers Green Circle
Greenwood Village, CO 80111

9 Terms and Conditions

1. All pricing, fees, taxes and other charges included in contract
2. Volume discounts based on volume usage
3. Services offered as a bundle and independent of each other
4. Contract with option for No Term Agreement and No Volume Commitment
5. Executed Service Level Agreements including specified penalties

9.1 Warranty

1. State the parameters of your warranty and detail the warranty period for the Residential Gateway.
2. State your return policy for the Residential Gateway.

9.2 Unit Pricing

1. Provide the Residential Gateway unit price. If there are different versions of the Residential Gateway, provide a unit price for each version.
2. Discount Pricing
3. Provide a discount schedule based on quantity of units purchased.

Appendix I
HomePlug Management Information Base

The Residential Gateway must implement the HomePlug Management Information Base (MIB) objects listed in this appendix to support cable operator management of the HomePlug network.

1. List of Objects

Objects	Syntax	MaxAccess	XML Tag
hmPlgMgmtMib			
hmPlgMgmtObjects			
hmPlgMgmtBase			
hmPlgMgmtXmlSchemaVer	INTEGER	read-only	TBD
hmPlgMgmtPsEk	OCTET STRING	read-only	-
hmPlgLogicalNetworkTable		not-accessible	-
hmPlgLogicalNetworkEntry		not-accessible	-
hmPlgLogicalNetworkIndex	INTEGER	not-accessible	-
hmPlgLogicalNetworkPwd	OCTET STRING	read-create	TBD
hmPlgLogicalNetworkPwdControl	INTEGER	read-create	-
hmPlgLogicalNetworkStatus	RowStatus	read-create	-
hmPlgDevBase			
hmPlgDevTable		not-accessible	
hmPlgDevEntry		not-accessible	
hmPlgDevIndex	INTEGER	read-only	-
hmPlgDevMacAddr	PhysAddress	read-create	-
hmPlgDevLocation	INTEGER	read-create	-
hmPlgDevAssumedType	DisplayString	read-create	-
hmPlgDevType	INTEGER	read-only	-
hmPlgDevXmlSchemaVer	INTEGER	read-only	TBD
hmPlgDevEK	INTEGER	read-create	TBD
hmPlgDevDesiredPwd	RowPointer	read-create	TBD
hmPlgDevMethod	INTEGER	read-only	-
hmPlgDevAuthState	BITS	read-only	-
hmPlgDevCommit	INTEGER	read-create	-
hmPlgDevCommitStatus	INTEGER	read-only	-
hmPlgDevRowStatus	RowStatus	read-create	-
hmPlgApTable			
hmPlgApEntry			
hmPlgApIndex	INTEGER	not-accessible	
hmPlgApMacAddr	PhysAddress	read-only	TBD
hmPlgAp802dot11MacAddr	PhysAddress	read-only	TBD
hmPlgApCurrSsid	OCTET STRING	read-only	TBD
hmPlgApDesiredSsid	OCTET STRING	read-create	TBD
hmPlgApCurrSsidAdvertisement	TruthValue	read-only	TBD

EXHIBIT A

Objects	Syntax	MaxAccess	XML Tag
hmPlgApDesiredSsidAdvertisement	TruthValue	read-create	TBD
hmPlgApCurrTxChannel	INTEGER	read-only	TBD
hmPlgApDesiredTxChannel	INTEGER	read-create	TBD
hmPlgApSecCapabilities	BITS	read-only	TBD
hmPlgApCurrSecOperMode	BITS	read-only	TBD
hmPlgApDesiredSecOperMode	BITS	read-create	TBD
hmPlgApCurrWEPPassphrase	OCTET STRING	read-only	TBD
hmPlgApCurrWEPEncryptKey	OCTET STRING	read-only	TBD
hmPlgApCurrWPAPassphrase	OCTET STRING	read-only	TBD
hmPlgApCurrWPAPreShareKey	OCTET STRING	read-only	TBD
hmPlgApCurrCpeFilterStatus	INTEGER	read-only	TBD
hmPlgApDesiredCpeFilterStatus	INTEGER	read-create	TBD
hmPlgApRowStatus	RowStatus	read-create	-
hmPlgApSecTable			
hmPlgApSecEntry		not-accessible	
hmPlgApSecIndex	INTEGER	read-create	
hmPlgApSecMacAddr	PhysAddress	read-create	TBD
hmPlgApSecWEPPassphrase	OCTET STRING	read-create	TBD
hmPlgApSecWPAPskPassphrase	OCTET STRING	read-create	TBD
hmPlgApSecWEPKeyIndex	INTEGER	read-create	TBD
hmPlgApSecWEPKey1	OCTET STRING	read-create	TBD
hmPlgApSecWEPKey2	OCTET STRING	read-create	TBD
hmPlgApSecWEPKey3	OCTET STRING	read-create	TBD
hmPlgApSecWEPKey4	OCTET STRING	read-create	TBD
hmPlgApSecWPAPreShareKey	OCTET STRING	read-create	TBD
hmPlgApSecWPARekeyTime	Unsigned32	read-create	TBD
hmPlgApSecRowStatus	RowStatus	read-create	
hmPlgApCpeFilterTable			
hmPlgApCpeFilterEntry		not-accessible	
hmPlgApCpeFilterIndex	INTEGER	not-accessible	
hmPlgApCpeFilterMacAddr	PhysAddress	read-create	TBD
hmPlgApCpeFilterMapping	INTEGER	read-create	-
hmPlgApCpeFilterApMacAddr	RowPointer	read-create	-
hmPlgApCpeFilterLogicalNetwork	RowPointer	read-create	-
hmPlgApCpeFilterRowStatus	RowStatus	read-create	-
hmPlgApCurrCpeFilterTable			
hmPlgApCurrCpeFilterEntry			
hmPlgApCurrCpeFilterApMacAddr	PhysAddress	read-only	TBD
hmPlgApCurrCpeFilterMacAddr	PhysAddress	read-only	TBD
hmPlgCpeDevTable			
hmPlgCpeDevEntry			
hmPlgCpeDevMacAddr	PhysAddress	read-only	
hmPlgCpeDevEndpointMacAddr	PhysAddress	read-only	

EXHIBIT A

2. Object Definitions

```
-- Comcast Cable Communications, LLC. Intellectual Property
-- Confidential & Proprietary.  Copyright 2004

COMCAST-HOMEPLUG-MANAGEMENT-MIB DEFINITIONS ::= BEGIN

IMPORTS
MODULE-IDENTITY,
      OBJECT-TYPE,
      Enterprises,
      Unsigned32,
      NOTIFICATION-TYPE              FROM SNMPv2-SMI
      DisplayString,
      PhysAddress,
      RowPointer,
      RowStatus,
      TruthValue,
      TEXTUAL-CONVENTION             FROM SNMPv2-TC
      OBJECT-GROUP,
      MODULE-COMPLIANCE,
      NOTIFICATION-GROUP             FROM SNMPv2-CONF
      comcastResidentialServices     FROM COMCAST-RESIDENTIAL-SERVICES-MIB;

hmPlgMgmtMib       MODULE-IDENTITY
LAST-UPDATED       "200411080000Z" -- November 08, 2004
ORGANIZATION       "Comcast Cable Communications, LLC."

    CONTACT-INFO
                   "                 Nirmal Mody
                   [Email]     Nirmal_Mody@cable.comcast.com
                   [Address]   Comcast Cable Communications, LLC.
                                     1500 Market Street
                                     9th Floor West Tower
                                     Philadelphia, PA 19102
                   [Telephone] 215-981-8530                        "

      DESCRIPTION
            "This MIB is for the management of Enhanced HomePlug EndPoints
             via a CableHome Residential Gateway Embedded with a HomePlug
             Interface. REFERENCE Comcast Request for Development:
             HomePlug Embedded CableHome Residential Gateway v1.2."


      ::= { comcastResidentialServices 1 }

-------------------------------------------------------------------------------
-----

hmPlgMgmtObjects        OBJECT IDENTIFIER ::= { hmPlgMgmtMib 1 }
hmPlgMgmtBase           OBJECT IDENTIFIER ::= { hmPlgMgmtObjects 1 }
hmPlgDevBase            OBJECT IDENTIFIER ::= { hmPlgMgmtObjects 2 }
--
--
--

hmPlgMgmtXmlSchemaVer   OBJECT-TYPE
      SYNTAX       INTEGER {
                         v1 (1)
```

```
                    -- v2(2),
                    }
      MAX-ACCESS  read-only
      STATUS      current
      DESCRIPTION
            "Supported XML Schema version by the gateway."
      DEFVAL { v1 }
      ::= { hmPlgMgmtBase 2 }

hmPlgMgmtPsEk      OBJECT-TYPE
      SYNTAX      OCTET STRING
      MAX-ACCESS read-only
      STATUS      current
      DESCRIPTION
            "The factory default Encryption Key of the embedded HomePlug
             interface on the gateway."
      ::= { hmPlgMgmtBase 3 }

hmPlgLogicalNetworkTable      OBJECT-TYPE
      SYNTAX      SEQUENCE OF HmPlgLogicalNetworkEntry
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
            "This table contains the passwords for one or more of the
             logical networks supported by the gateway. The gateway must
             support at least 1 logical network."
      ::= { hmPlgMgmtBase 4 }

hmPlgLogicalNetworkEntry      OBJECT-TYPE
      SYNTAX      HmPlgLogicalNetworkEntry
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
            "Entry for the HomePlug Logical Networks Table."
      INDEX { hmPlgLogicalNetworkIndex }
      ::= { hmPlgLogicalNetworkTable 1 }

      HmPlgLogicalNetworkEntry ::= SEQUENCE {
      hmPlgLogicalNetworkIndex            INTEGER,
      hmPlgLogicalNetworkPwd              OCTET STRING,
      hmPlgLogicalNetworkPwdControl       INTEGER,
      hmPlgLogicalNetworkStatus           INTEGER
      }

      hmPlgLogicalNetworkIndex      OBJECT-TYPE
            SYNTAX      INTEGER
            MAX-ACCESS  not-accessible
            STATUS      current
            DESCRIPTION
                  "Index."
            ::= { hmPlgLogicalNetworkEntry 1 }

      hmPlgLogicalNetworkPwd  OBJECT-TYPE
            SYNTAX      OCTET STRING (SIZE (4..16))
            MAX-ACCESS  read-create
            STATUS      current
            DESCRIPTION
                  "The gateway must support at least one Logical Network and
                   the default password of this first network must be
                   'HomePlug'.  If the gateway  supports multiple logical
                    networks, then the entries must automatically be created
```

EXHIBIT A

```
                    in the table with passwords HomePlug2, HomePlug3 etc.
                  The gateway must derive the encryption key from the network
                  password as per the HomePlug specification for
                  encrypting/decryption all messages to and from the endpoints
                  belonging to a particular network."
            ::= { hmPlgLogicalNetworkEntry 2 }

      hmPlgLogicalNetworkPwdControl OBJECT-TYPE
            SYNTAX      TruthValue
            MAX-ACCESS  read-create
            STATUS      current
            DESCRIPTION
                  "Setting this value to 'true(1)' will trigger a Password
                   update process from the gateway to the endpoints listed in
                  the hmPlgDevTable that are part of referenced Logical
                  Network.  Reading the value must always report false(2)."
            ::= { hmPlgLogicalNetworkEntry 3 }

      hmPlgLogicalNetworkStatus     OBJECT-TYPE
            SYNTAX      INTEGER     {
                              enabled (1),
                              disabled (2)
                              }
            MAX-ACCESS  read-create
            STATUS      current
            DESCRIPTION
                  "Setting this object to enabled (1) will activate the
                   logical network.
                  Setting this object to disabled (2) will deactivate the use
                  of the logical network."
            ::= { hmPlgLogicalNetworkEntry 4 }

--
--
--

hmPlgDevTable     OBJECT-TYPE
      SYNTAX      SEQUENCE OF HmPlgDevEntry
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
            "HomePlug Devices Table."
      ::= { hmPlgDevBase 1 }

hmPlgDevEntry     OBJECT-TYPE
      SYNTAX      HmPlgDevEntry
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
            "HomePlug Devices Table Entry"
      INDEX { hmPlgDevIndex }
      ::= { hmPlgDevTable 1 }

      HmPlgDevEntry ::= SEQUENCE {
      hmPlgDevIndex             INTEGER,
      hmPlgDevMacAddr           PhysAddress,
      hmPlgDevLocation          OCTET STRING,
      hmPlgDevAssumedType       INTEGER,
      hmPlgDevType              INTEGER,
      hmPlgDevXmlSchemaVer      INTEGER,
      hmPlgDevEK                INTEGER,
```

EXHIBIT A

```
hmPlgDevDesiredPwd       RowPointer,
hmPlgDevCreationMethod   INTEGER,
hmPlgDevAuthState        BITS,
hmPlgDevCommit           INTEGER,
hmPlgDevCommitStatus     INTEGER,
hmPlgDevRowStatus        RowStatus
}

hmPlgDevIndex      OBJECT-TYPE
      SYNTAX       INTEGER
      MAX-ACCESS   not-accessible
      STATUS       current
      DESCRIPTION
            "Index"
      ::= { hmPlgDevEntry 1 }

hmPlgDevMacAddr    OBJECT-TYPE
      SYNTAX       PhysAddress
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "MAC Address of the endpoint."
      ::= { hmPlgDevEntry 2 }

hmPlgDevLocation   OBJECT-TYPE
      SYNTAX       OCTET STRING (SIZE(0..80))
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "General description the end-user may use to associate the
             location within the home where the endpoint will be plugged
             in. For example  'kitchen' or 'right corner of the master
             bedroom'"
      ::= { hmPlgDevEntry 3 }

hmPlgDevAssumedType OBJECT-TYPE
      SYNTAX       INTEGER {
                         accessPoint (1),
                         ethernet (2),
                         usb (3),
                               }
      MAX-ACCESS         read-create
      STATUS             current
      DESCRIPTION
      "The assumed type of the device.  This object is only used
       temporarily during endpoint configuration."
      ::= { hmPlgDevEntry 4 }

hmPlgDevType OBJECT-TYPE
      SYNTAX       INTEGER {
                         accessPoint (1),
                         ethernet (2),
                         usb (3),
                         enhancedAccessPoint (4),
                         nonEnhancedOther (5)
                         }
      MAX-ACCESS   read-only
      STATUS       current
      DESCRIPTION
            "Endpoint Type."
      ::= { hmPlgDevEntry 5 }
      hmPlgDevXmlSchemaVer    OBJECT-TYPE
            SYNTAX      INTEGER {
                              notSupported (1),
                              v1 (2)
                              }
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                  "Supported XML Schema version by the Enchanced Endpoint.
                   Reading this object for a Standard HomePlug devices will
                   always return 'notSupported(1)"
            ::= { hmPlgDevEntry 6  }

      hmPlgDevEK  OBJECT-TYPE
            SYNTAX      INTEGER (4..32)
            MAX-ACCESS  read-create
            STATUS      current
            DESCRIPTION
                  "The Factory default unique non-vol HomePlug Device
Encryption Key."
            ::= { hmPlgDevEntry 7 }

      hmPlgDevDesiredPwd      OBJECT-TYPE
            SYNTAX      RowPointer
            MAX-ACCESS  read-create
            STATUS      current
            DESCRIPTION
                  "Row Pointer to the hmPlgLogicalNetworkTable to denote which
                   network the endpoint is to associated to."
            ::= { hmPlgDevEntry 8 }

      hmPlgDevCreationMethod  OBJECT-TYPE
            SYNTAX      INTEGER {
                              staticReservation (1),
                              manual (2)
                              }
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                  "staticReservation(1) denotes that the endpoint was pre-
                   configured or authorized via the UI.  manail (2) denotes
                   that the endpoint was configured utilizing the endpoint's
                   vendor software utility."
            ::= { hmPlgDevEntry 9 }

      hmPlgDevAuthState OBJECT-TYPE
            SYNTAX      BITS {
                              apConfigInvalid (0),
                              apConfigPending (1),
                              authorizationPending (2),
                              authorized (3),
                              deletionPending (4),
                              networkPwdUpdateFailed (5),
                              networkPwdUpdatePending (6)
                              }

            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                  "When an Access Point device rejects the Wireless Encryption
```

```
                values set from the gateway must set BIT apConfigInvalid
                (0) to '1'.

               When an Access Point type endpoint has finished the
               authentication process but has not been configured with the
               wireless encryption parameters the gateway must set BIT to
               apConfigPending (1) to '1'.  This applies to situations were
               the AP's Wi-Fi configuration is done via a software
               utililty or directly via a local web interface.

               When the endpoint is pre-configured via the Static
               Reservation process however, has not initialized the gateway
               must set the BIT authorizationPending (2) to '1'.

               When the endpoint accepts authorization and/or configuration
               parameters and joins the network the gateway must set
               authorized (3) to '1'.

               When an entry is queued for deletion, however the endpoint
               is offline, the gateway must set deletionPending (4) to '1'.
               The gateway must delete all references of the endpoint when
               it re-initializes.  The gateway must queue the message
               indefinitely unless until the row is deleted.

               When the logical network password is changed but the
               endpoint does not accept the change the gateway must set
               networkPwdUpdateFailed (5) to '1'.

               If the password change message is sent but the gateway does
               not receive an acceptance or decline message it is to assume
               that the endpoint is offline and must set the
               networkPwdUpdatePending (6) bit to '1'. When the endpoint
               initializes the gateway must push the password update
               message to the endpoint."
         ::= { hmPlgDevEntry 10 }

hmPlgDevCommit     OBJECT-TYPE
    SYNTAX         INTEGER {
                           apConfigProfile  (1),
                           apEncryptProfile (2),
                           authStaticReservation (3),
                           setToFactory (4),
                           epCurrProfileQuery (5),
                           idle (6)
                           }

         MAX-ACCESS  read-create
         STATUS           current
         DESCRIPTION
               "When set to apConfigProfile (1) the gateway will send an
                APConfigProfile message to the endpoint. When set to
                apEncryptProfile (2) the gateway will send an
                APEncryptProfile message to the endpoint. When set to
                authStaticReservation(3) the gateway will send an
                AuthenticateStaticReservation message to the endpoint. When
                set to setToFactory (4) the gateway must send an
                EpSetToFactory message to the endpoint. When set to
                endpointCurrProfileQuery (5) the gateway must
                send an CurrProfileQuery request to the endpoint. This
                object must return to 'idle (6) once the query message is
                initiated."
```

EXHIBIT A

```
            ::= { hmPlgDevEntry 11 }

      hmPlgDevCommitStatus    OBJECT-TYPE
            SYNTAX      INTEGER {
                              failed (1),
                              inProgress (2),
                              successful (3)
                              }
            MAX-ACCESS read-only
            STATUS      current
            DESCRIPTION
                  "This object returns the status of the query set in the
                   hmPlgDevCommit object."
            ::= { hmPlgDevEntry 12 }

      hmPlgDevRowStatus OBJECT-TYPE
            SYNTAX                  RowStatus
            MAX-ACCESS              read-create
            STATUS                  current
            DESCRIPTION
                  " active (1) -- Set to active when the endpoint is online
                    notInService (2) -- Set to notInService when the endpoint
                                        is offline
                    notReady (3)
                    createAndGo (4)
                    createAndWait (5)
                    destroy (6) "
            ::= { hmPlgDevEntry 13 }

--
--
-- HomePlug Access Point Table
--

hmPlgApTable      OBJECT-TYPE
      SYNTAX            SEQUENCE OF HmPlgApEntry
      MAX-ACCESS  not-accessible
      STATUS            current
      DESCRIPTION
            "hmPlg Devices Table."
      ::= { hmPlgDevBase 2 }

hmPlgApEntry      OBJECT-TYPE
      SYNTAX            HmPlgApEntry
      MAX-ACCESS  not-accessible
      STATUS            current
      DESCRIPTION
            "HomePlug Access Point Devices Table Object entry"
      INDEX { hmPlgApIndex, hmPlgApDesiredTxChannel }
      ::= { hmPlgApTable 1 }

      HmPlgApEntry ::= SEQUENCE {
            hmPlgApIndex                        INTEGER,
            hmPlgApMacAddr                      PhysAddress,
            hmPlgAp802dot11MacAddr              PhysAddress,
            hmPlgApCurrSsid                     OCTET STRING,
            hmPlgApDesiredSsid                  OCTET STRING,
            hmPlgApCurrSsidAdvertisement        TruthValue,
            hmPlgApDesiredSsidAdvertisement     TruthValue,
            hmPlgApCurrTxChannel                INTEGER,
            hmPlgApDesiredTxChannel             INTEGER,
      hmPlgApSecCapabilities             BITS,
      hmPlgApCurrSecOperMode             BITS,
      hmPlgApDesiredSecOperMode          BITS,
      hmPlgApCurrWEPPassphrase           OCTET STRING,
      hmPlgApCurrWEPEncryptKey           OCTET STRING,
      hmPlgApCurrWPAPassphrase           OCTET STRING,
      hmPlgApCurrWPAPreShareKey          OCTET STRING,
      hmPlgApCurrCpeFilterStatus         INTEGER,
      hmPlgApDesiredCpeFilterStatus      INTEGER,
      hmPlgApRowStatus                   RowStatus
      }

hmPlgApIndex            OBJECT-TYPE
      SYNTAX                  INTEGER
      MAX-ACCESS        not-accessible
      STATUS                  current
      DESCRIPTION
            "Index"
::= { hmPlgApEntry 1 }

hmPlgApMacAddr          OBJECT-TYPE
      SYNTAX                  PhysAddress
      MAX-ACCESS        read-create
      STATUS                  current
      DESCRIPTION
            "MAC Address of the Access Point."
::= { hmPlgApEntry 2 }

hmPlgAp802dot11MacAddr  OBJECT-TYPE
      SYNTAX            PhysAddress
      MAX-ACCESS        read-create
      STATUS            current
      DESCRIPTION
            "MAC Address of the 802.11 interface of the Access Point."
      ::= { hmPlgApEntry 3 }

hmPlgApCurrSsid         OBJECT-TYPE
      SYNTAX                  OCTET STRING (SIZE(0..32))
      MAX-ACCESS  read-only
      STATUS                  current
      DESCRIPTION
            "The Current SSID value on the AP."
      ::= { hmPlgApEntry 4 }

hmPlgApDesiredSsid      OBJECT-TYPE
      SYNTAX            OCTET STRING (SIZE(0..32))
      MAX-ACCESS        read-create
      STATUS            current
      DESCRIPTION
            "The Desired SSID value on the AP."
      ::= { hmPlgApEntry 5 }

hmPlgApCurrSsidAdvertisement            OBJECT-TYPE
      SYNTAX            TruthValue
      MAX-ACCESS        read-only
      STATUS            current
      DESCRIPTION
            "Value (1) 'true' denotes the Access Point SSID is
            advertised.
            Value (2) 'false' denotes the AP does not advertise its
            SSID."
```

```
          ::= { hmPlgApEntry 6 }

    hmPlgApDesiredSsidAdvertisement           OBJECT-TYPE
          SYNTAX              TruthValue
          MAX-ACCESS          read-create
          STATUS              current
          DESCRIPTION
                " Reference: cabhPsDev802dot11BaseAdvertiseSSID
                When set to false(2) the AP does not advertise the BSS SSID
                in a proprietary manner.  To avoid interoperability problems
                and service disruption it is RECOMMENDED to set this object
                always to true.  This feature does not provide any security,
                and does not prevent Wireless Stations to obtain the SSID by
                sniffing frames from other stations in the ESS. If the
                device does not support the feature of turning on/off
                the SSID advertisement, this object always reports 'true(1)'
                and reports the error 'wrongValue' when set to 'false(2)."
          DEFVAL { true }
          ::= { hmPlgApEntry 7 }

    hmPlgApCurrTxChannel     OBJECT-TYPE
          SYNTAX INTEGER {
                      one (1),
                      two (2),
                      three (3),
                      four (4),
                      five (5),
                      six (6),
                      seven (7),
                      eight (8),
                      nine (9),
                      ten (10),
                      eleven (11)
--                    twelve (12),
--                    thirteen (13),
--                    fourteen (14)
                      }
          MAX-ACCESS          read-only
          STATUS              current
          DESCRIPTION
                "The current Transmit Channel Value on the Access Point."
      ::= { hmPlgApEntry 8 }

    hmPlgApDesiredTxChannel        OBJECT-TYPE
          SYNTAX INTEGER {
                      one (1),
                      two (2),
                      three (3),
                      four (4),
                      five (5),
                      six (6),
                      seven (7),
                      eight (8),
                      nine (9),
                      ten (10),
                      eleven (11)
                      }
          MAX-ACCESS          read-create
          STATUS              current
          DESCRIPTION
                "The desired Transmit (TX) Channel to be utilized by the AP.
```

```
             The gateway must not permit the assignment of a TX Channel
             that is already assigned."
        ::= { hmPlgApEntry 9 }

    hmPlgApSecCapabilities  OBJECT-TYPE
        SYNTAX  BITS {
                      wep64(0),
                      wep128(1),
                      wpaPSK(2)
                      --wpa2PSK(3)
                      }
        MAX-ACCESS          read-only
        STATUS              current
        DESCRIPTION
             "Reference:  cabhPsDev802dot11SecCapabilities
             The AP capabilities for Authentication and encryption used
             to  authenticate 802.11 clients."
        ::= { hmPlgApEntry 10 }

    hmPlgApCurrSecOperMode          OBJECT-TYPE
        SYNTAX BITS {
                      wep64(0),
                      wep128(1),
                      wpaPSK(2)
                      --wpa2PSK(3)
                      }
        MAX-ACCESS          read-only
        STATUS              current
        DESCRIPTION
             "The utilized encryption mechanism(s) on the AP."
        ::= { hmPlgApEntry 11 }


    hmPlgApDesiredSecOperMode       OBJECT-TYPE
        SYNTAX  BITS {
                      wep64(0),
                      wep128(1),
                      wpaPSK(2)
                      --    wpa2PSK(3)
                      }
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION
             "Reference:  cabhPsDev802dot11SecOperMode
             Indicates the Authentication and encryption mechanism to be
             enabled for the users and advertised in Beacon messages.
             Bits set to this object and not supported by the AP in
             hmPlgApSecCapabilities are set to '0'
             without failing the SNMP set.  Setting two bit that the
             gateway does not support in combination returns an error
             'wrongValue'. In particular:

             # Setting to '1' both wep64(0)and wep128(1) bits returns an
               error 'wrongValue'.
             # Setting a combination of WEP bits (wep64(0) or wep128(1))
               and wpaPSK bit returns is not a mandatory requirement,
               therefore an error 'wrongValue' may be reported.
             # Setting the wpaPSK(2) bit to '1' indicates the usage of
               WPA-PSK TKIP.
             # Setting all bits to '0' indicates no security mechanism is
               to be used."
```

```
      ::= { hmPlgApEntry 12 }

hmPlgApCurrWEPPassphrase      OBJECT-TYPE
      SYNTAX      OCTET STRING (SIZE(0|5..63))
      MAX-ACCESS  read-only
      STATUS      current
      DESCRIPTION
            "The current WEP Passphrase value in non-HEX format on the
             AP Endpoint."
      ::= { hmPlgApEntry 13 }

hmPlgApCurrWEPEncryptKey      OBJECT-TYPE
      SYNTAX      OCTET STRING (SIZE(0|5..13))
      MAX-ACCESS  read-only
      STATUS      current
      DESCRIPTION
            "The Current WEP Key configured on the AP."
      ::= { hmPlgApEntry 14 }

hmPlgApCurrWPAPassphrase      OBJECT-TYPE
            SYNTAX            OCTET STRING (SIZE(0|5..63))
            MAX-ACCESS        read-only
            STATUS            current
            DESCRIPTION
                  "The current WPA-PSK Passphrase value in non-HEX
                   format configured on the AP."
            ::= { hmPlgApEntry 15 }

hmPlgApCurrWPAPreShareKey     OBJECT-TYPE
      SYNTAX      OCTET STRING (SIZE(0|32))
      MAX-ACCESS        read-only
      STATUS            current
      DESCRIPTION
            "The current WPA PreShare Key configured on the AP."
      ::= { hmPlgApEntry 16 }

hmPlgApCurrCpeFilterStatus    OBJECT-TYPE
      SYNTAX      INTEGER {
                        enabled (1),
                        disabled (2)
                        }
      MAX-ACCESS  read-only
      STATUS      current
      DESCRIPTION
            "The current 802.11 MAC filtering status on the endpoint.
             When this object reports enabled, the endpoint only permits
             the MAC Addresses listed in the hmPlgApCpeFilterTable to
             connect wirelessly to its 802.11 interface."
      ::= { hmPlgApEntry 17 }

hmPlgApDesiredCpeFilterStatus OBJECT-TYPE
      SYNTAX INTEGER {
                  enabled (1),
                  disabled (2)
                  }
      MAX-ACCESS read-create
      STATUS      current
      DESCRIPTION
            "Setting this object to enabled (1) will turn on 802.11 MAC
             Address Filtering.  Setting the object to disabled (2) will
             turn if off."
```

EXHIBIT A

```
            ::= { hmPlgApEntry 18 }

      hmPlgApRowStatus  OBJECT-TYPE
            SYNTAX      RowStatus
            MAX-ACCESS  read-create
            STATUS      current
            DESCRIPTION
                  "Row Status"
            ::= { hmPlgApEntry 19 }

--
--
-- Wireless Encryption Table
--
hmPlgApSecTable         OBJECT-TYPE
      SYNTAX      SEQUENCE OF HmPlgApSecEntry
      MAX-ACCESS        not-accessible
      STATUS            current
      DESCRIPTION
            "WEP / WPA-PSK Security Table."
      ::= { hmPlgDevBase 3}

hmPlgApSecEntry   OBJECT-TYPE
      SYNTAX                  HmPlgApSecEntry
      MAX-ACCESS  not-accessible
      STATUS            current
      DESCRIPTION
            "WEP / WPA-PSK Security entry."
      INDEX { hmPlgApSecIndex }
      ::= { hmPlgApSecTable 1 }

HmPlgApSecEntry ::= SEQUENCE {
      hmPlgApSecIndex               INTEGER,
      hmPlgApSecMacAddr             PhysAddress,
      hmPlgApSecWEPPassphrase       OCTET STRING,
      hmPlgApSecWPAPskPassphrase    OCTET STRING,
      hmPlgApSecWEPKeyIndex         INTEGER,
      hmPlgApSecWEPKey1             OCTET STRING,
      hmPlgApSecWEPKey2             OCTET STRING,
      hmPlgApSecWEPKey3             OCTET STRING,
      hmPlgApSecWEPKey4             OCTET STRING,
      hmPlgApSecWPAPreShareKey      OCTET STRING,
      hmPlgApSecWPARekeyTime        Unsigned32,
      hmPlgApSecRowStatus           RowStatus
      }

      hmPlgApSecIndex   OBJECT-TYPE
            SYNTAX      INTEGER
            MAX-ACCESS  not-accessible
            STATUS      current
            DESCRIPTION
                  "Index"
            ::= { hmPlgApSecEntry 1 }

      hmPlgApSecMacAddr OBJECT-TYPE
            SYNTAX      PhysAddress
            MAX-ACCESS  read-create
            STATUS      current
            DESCRIPTION
                  "MAC Address of the endpoint"
            ::= { hmPlgApSecEntry 2 }
```

EXHIBIT A

```
hmPlgApSecWEPPassphrase OBJECT-TYPE
      SYNTAX      OCTET STRING (SIZE(0|5..63))
      MAX-ACCESS  read-create
      STATUS      current
      DESCRIPTION
            "WEP Passphrase used to derive the WEP Encryption Key.
             Reference cabhPsDev802dot11SecPassPhraseToWEPKey object for
             algorithm requirements.  For WEP 128 write key to
             hmPlgApSecWEPKey1 object. For WEP 64 generate four keys and
             write to objects hmPlgApSecWEPKey1 through
             hmPlgApSecWEPKey4."
      ::= { hmPlgApSecEntry 3 }

hmPlgApSecWPAPskPassphrase    OBJECT-TYPE
      SYNTAX      OCTET STRING (SIZE(8..63))
      MAX-ACCESS  read-create
      STATUS      current
      DESCRIPTION
            "Passphrase used to derive the WPA PreShare Key.  Reference:
            cabhPsDev802dot11SecPSKPassPhraseToKey
            For wpaPSK: The value of hmPlgApSecWPAPreShareKey is updated
            with the Password Base Key Derivation Function from the
            Password-based Cryptographic Specification PKCS #5 v2.0 RFC
            2898 (PBKDF2) with the following specific parameters:
            PSK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256)
            PassPhrase is the value of this object ssid is the gateway
            SSID value used as the function salt ssidLength is the
            number of octets of ssid the iterations count is 4096 and
            the key generation length is 256 bits (32 octets).  This
            object value is normally read by issuing SNMP request PDUs.
            This object can be cleared with an SNMP SET to an empty
            string Value and the gateway MUST not update the type of
            keys being set to '1' in hmPlgApDesiredSecOperMode.
            Vector examples for wpaPSK: for wpaPSK:
            passphrase: 'ABCD4321' ( hex code 0x41.42.43.44.34.33.32.31)
            SSID: 'ABCD4321' ( hex code 0x41.42.43.44.34.33.32.31 )
            256 bit PBKDF2('ABCD4321', 'ABCD4321', 8, 4096, 32)
            hmPlgApSecWPAPreSharedKey =
            0x7C199CF2FEF9AF206C8EE0E9703920C23517068B3F96B011E0F975C913
            1BDB58"
      ::= { hmPlgApSecEntry 4 }

hmPlgApSecWEPKeyIndex   OBJECT-TYPE
      SYNTAX      INTEGER {
                        key1 (1),
                        key2 (2),
                        key3 (3),
                        key4 (4)
                        }
      MAX-ACCESS  read-create
      STATUS      current
      DESCRIPTION
            "This object is used to determine which WEP 64 Key is to be
             utilized.

            For WEP 128 default to KEY 1.  The default key for WEP 64 is
            key1 (1)"
      ::= { hmPlgApSecEntry 5 }

hmPlgApSecWEPKey1 OBJECT-TYPE
```

```
    SYNTAX      OCTET STRING (SIZE (0|5..13))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The 10 (WEP 64) or 26 (WEP 128) Hexadecimal character WEP
        Key. This  object can be set directly or derived from the
        Passphrase set if the value of this object is the zero-
        length string, the gateway must not activate the WEP
        security mechanism."
       ::= { hmPlgApSecEntry 6 }

 hmPlgApSecWEPKey2 OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0|5))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The 10 Hexadecimal character WEP 64 Key.  This object can
        be set directly or derived from the Passphrase."
    ::= { hmPlgApSecEntry 7 }

 hmPlgApSecWEPKey3 OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0|5))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The 10 Hexadecimal character WEP 64 Key.  This object can
        be set directly or derived from the Passphrase."
    ::= { hmPlgApSecEntry 8 }

hmPlgApSecWEPKey4   OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (0|5))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The 10 Hexadecimal character WEP 64 Key.  This object can
        be set directly or derived from the Passphrase."
       ::= { hmPlgApSecEntry 9 }

 hmPlgApSecWPAPreShareKey      OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0|32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The Pre-shared key used for the AP when the bit 'wpaPSK'.
        This object can be set directly or derived from the
        Passphrase set if the value of this object is the zero-
        length string, the gateway must not activate the PSK
        security mechanism."
    ::= { hmPlgApSecEntry 10 }

 hmPlgApSecWPARekeyTime  OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    UNITS       "seconds"
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Reference:  cabhPsDev802dot11SecWPARekeyTime
       Time interval to initiate WPA Group Keys (GTK) updates."
    DEFVAL { 86400 }
    ::= { hmPlgApSecEntry 11 }
```

```
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------

hmPlgApCpeFilterTable   OBJECT-TYPE
      SYNTAX      SEQUENCE OF HmPlgApCpeFilterEntry
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
            "This table lists the MAC Addresses of CPE devices that the 802.11
             filtering is to be applied to when hmPlgApCpeFilterDesiredStatus
             for an AP is 'enabled (1)'."
      ::= { hmPlgDevBase 4 }

hmPlgApCpeFilterEntry OBJECT-TYPE
      SYNTAX      HmPlgApCpeFilterEntry
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
            "hmPlgCurrCpeFilterTable entry."
      INDEX { hmPlgApCpeFilterIndex }
      ::= { hmPlgApCpeFilterTable 1 }

HmPlgApCpeFilterEntry ::= SEQUENCE {
      hmPlgApCpeFilterIndex               INTEGER,
      hmPlgApCpeFilterMacAddr             PhysAddress,
      hmPlgApCpeFilterMapping             INTEGER,
      hmPlgApCpeFilterApMacAddr           RowPointer,
      hmPlgApCpeFilterLogicalNetwork  RowPointer,
      hmPlgApCpeFilterRowStatus           RowStatus
      }

      hmPlgApCpeFilterIndex   OBJECT-TYPE
            SYNTAX      INTEGER
            MAX-ACCESS  not-accessible
            STATUS      current
            DESCRIPTION
                  "Index"
            ::= { hmPlgApCpeFilterEntry 1 }

      hmPlgApCpeFilterMacAddr OBJECT-TYPE
            SYNTAX      PhysAddress
            MAX-ACCESS  read-create
            STATUS      current
            DESCRIPTION
                  "The MAC Address of the CPE device which is permitted to
                   connect to the endpoint when MAC Address filtering is
                   enabled."
            ::= { hmPlgApCpeFilterEntry 2 }

      hmPlgApCpeFilterMapping OBJECT-TYPE
            SYNTAX      INTEGER {
                              allAccessPoints (1),
                              accessPointSpecific (2),
                              logicalNetworkSpecific (3)
                              }
            MAX-ACCESS  read-create
            STATUS      current
            DESCRIPTION
                  "When this object is set to 'allAccessPoints (1)' the MAC
                  Address of the CPE will be included in the AP Profile
```

EXHIBIT A

```
                message to all endpoints that have CPE Filtering enabled.
                When set to 'accessPointSpecific (2)'the CPE MAC Address
                must be only be sent to a specific endpoint.  When set to
                'logicalNetworkSpecific (3)' the CPE MAC Address will be
                included in the AP Profile message to AP's belonging to a
                specific logical network."
          DEFVAL { allAccessPoints }
          ::= { hmPlgApCpeFilterEntry 3 }

    hmPlgApCpeFilterApMacAddr      OBJECT-TYPE
          SYNTAX       RowPointer
          MAX-ACCESS   read-create
          STATUS       current
          DESCRIPTION
                "When the hmPlgApCpeFilterMapping is set to '2', the gateway
                will send include the CPE MAC Address in the AP Profile
                 Message to the specified enpdoint.  This has no purpose
                 when hmPlgApCpeFilterMapping is set to either 1 or 3. This
                 object references an entry the entry object
                 'hmPlgDevMacAddr' in the hmPlgDevTable."
          ::= { hmPlgApCpeFilterEntry 4 }

    hmPlgApCpeFilterLogicalNetwork      OBJECT-TYPE
          SYNTAX       RowPointer
          MAX-ACCESS   read-create
          STATUS       current
          DESCRIPTION
                "When the hmPlgApCpeFilterMapping is set to '3', the gateway
                 will send include the CPE MAC Address in the AP Profile
                 Message to all enpdoints part of this logical network.
                 This has no purpose when hmPlgApCpeFilterMapping is set to
                 either 1 or 2. This object references an entry object
                 'hmPlgLogicalNetworkPwd' in the hmPlgLogicalNetworkTable."
          ::= { hmPlgApCpeFilterEntry 5 }

    hmPlgApCpeFilterRowStatus      OBJECT-TYPE
          SYNTAX       RowStatus
          MAX-ACCESS   read-create
          STATUS       current
          DESCRIPTION
                "Row Status for the table."
          ::= { hmPlgApCpeFilterEntry 6 }


-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------


hmPlgApCurrCpeFilterTable      OBJECT-TYPE
      SYNTAX       SEQUENCE OF HmPlgApCurrCpeFilterEntry
      MAX-ACCESS   not-accessible
      STATUS       current
      DESCRIPTION
            "This table lists the MAC Addresses of LAN IP devices that are
             permitted to connect to the Access Point."
      ::= { hmPlgDevBase 5 }

hmPlgApCurrCpeFilterEntry OBJECT-TYPE
      SYNTAX       HmPlgApCurrCpeFilterEntry
      MAX-ACCESS   not-accessible
      STATUS       current
      DESCRIPTION
            "hmPlgCurrCpeFilterTable entry."
      INDEX { hmPlgApCurrCpeFilterApMacAddr }
      ::= { hmPlgApCurrCpeFilterTable 1 }

HmPlgApCurrCpeFilterEntry ::= SEQUENCE {
      hmPlgApCurrCpeFilterApMacAddr PhysAddress,
      hmPlgApCurrCpeFilterMacAddr         PhysAddress
      }

      hmPlgApCurrCpeFilterApMacAddr OBJECT-TYPE
            SYNTAX      PhysAddress
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                  "The MAC Address of the AP endpoint."
            ::= { hmPlgApCurrCpeFilterEntry 1 }

      hmPlgApCurrCpeFilterMacAddr   OBJECT-TYPE
            SYNTAX      PhysAddress
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                  "The MAC Address of the CPE permitted to connect to the
                   endpoint when 802.11 MAC Address filtering is enabled."
            ::= { hmPlgApCurrCpeFilterEntry 2 }

---------------------------------------------------------------------------
---------------------------------------------------------------------------
---------------------------------------------------------------------------

hmPlgCpeDevTable  OBJECT-TYPE
      SYNTAX      SEQUENCE OF HmPlgCpeDevEntry
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
            "This table lists the MAC Addresses of LAN IP devices that are
            online and connected to the gateway via a HomePlug endpoint."
      ::= { hmPlgDevBase 6 }

hmPlgCpeDevEntry OBJECT-TYPE
      SYNTAX      HmPlgCpeDevEntry
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
            "hmPlgCpeDevTable entry."
      INDEX { hmPlgCpeDevMacAddr }
      ::= { hmPlgCpeDevTable 1 }

HmPlgCpeDevEntry ::= SEQUENCE {
      hmPlgCpeDevMacAddr            PhysAddress,
      hmPlgCpeDevEndpointMacAddr    PhysAddress
      }

      hmPlgCpeDevMacAddr      OBJECT-TYPE
            SYNTAX      PhysAddress
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                  "The MAC Address of the CPE device."
            ::= { hmPlgCpeDevEntry 1 }
      hmPlgCpeDevEndpointMacAddr    OBJECT-TYPE
            SYNTAX      PhysAddress
            MAX-ACCESS  read-only
            STATUS      current
            DESCRIPTION
                  "The MAC Address HomePlug endpoint via which the CPe is
                  connected."
            ::= { hmPlgCpeDevEntry 2 }

END
```

EXHIBIT A

```
COMCAST-RESIDENTIAL-SERVICES-MIB  DEFINITIONS ::= BEGIN

IMPORTS
      MODULE-IDENTITY,
      enterprises             FROM SNMPv2-SMI;

comcast     OBJECT IDENTIFIER ::= { enterprises 17270 }

comcastResidentialServices    MODULE-IDENTITY
      LAST-UPDATED      "200410050000Z" -- October 5, 2004
      ORGANIZATION      "Comcast Corporation"
    CONTACT-INFO
            "                           Nirmal Mody
                  [Email]         Nirmal_Mody@cable.comcast.com
                  [Organization]  Comcast Cable Communications
                  [Address]         1500 Market Street
                                    9th Floor West Tower
                                    Philadelphia, PA 19102
                  [Telephone]       215-981-8530

                                    Aaron Settles
                  [Email]         Aaron_Settles@cable.comcast.com
                  [Organization]  Comcast Cable Communications
                  [Address]         30B Coachman Square
                                    Clifton Park, NY 12065
                  [Telephone]       (720) 490-0137

           "

      DESCRIPTION
            "This is the root MIB for all Comcast High-Speed Data Residential
            Services."

      ::= { comcast 3 }

hmPlgMgmtMib                  OBJECT IDENTIFIER ::= {
comcastResidentialServices  1 }
comcastUiFeaturesMib    OBJECT IDENTIFIER ::= { comcastResidentialServices  2
}

END
```

Appendix II
Desired HomePlug Functional Process

All CableLabs Residential Gateway HomePlug endpoints will be managed via the gateway. As such all the functional processes are defined with the gateway as the central management device. No proposals will be considered that involve installation of a software utility on LAN IP devices such as a personal computer or utilizing a PC to configure 802.11 settings of HomePlug endpoints. A cable operator may provide a User Interface resident on the gateway to centralize the management of all HomePlug devices.

This document references the utilization of a Transaction ID for each message generated and/or received by the gateway for the AP configuration. The requirements for generating the unique ID are open to vendor's suggestion.

3. Configuring the Global Network Password

The gateway must support the configuration of the Logical Network Password via the UI and via SNMP. This password is the desired password for a logical network used for authenticating endpoints with the gateway. The gateway must support at least one (1) logical network and its default value must be 'HomePlug'. Once the password is updated the value must be stored in the hmPlgLogicalNetworkPwd object in the hmPlgLogicalNetworkTable.

4. HomePlug Endpoint Configuration

4.1. Use Case

Use Case: Endpoint Configuration
Actor: Installer (End-User or Technician)
Purpose: Configure endpoint via Static Reservation Configuration Process
Objective: This Use Case summarizes the steps needed to configure an endpoint through the
Type: Primary and Essential
Cross Reference: None

Actor Action	System Response
1. Installer clicks on "Add HomePlug device to my Network" tab via the UI.	1a. Gateway prompts for the device type and its encryption key
2.1. Installer selects the type of device being added to the network: Ethernet, USB, or AP 2.2. Installer enters Device Encryption Key	2a. Gateway stores value into MIB database. Gateway sets Status to 'authorizationPending'.

3. If the device type is Ethernet or USB, configuration is complete. If the device type is AP, the installer enters the Wireless Security Settings for the endpoint.	3a. Gateway stores settings for the Wireless Security settings into MIB database.
4. Installer plugs endpoint into power-outlet or the endpoint is already plugged in prior the configuration.	4a. Gateway detects a HomePlug device on the power line network 4b. Gateway utilizes the EK to encrypt and transmit the Global Network Password and Device Encryption Key Select identifier to the HomePlug device 4c. The HomePlug device returns a Confirm Network Encryption Key MAC management entry (Network Password) to the gateway 4d. Gateway updates status for Ethernet and USB type devices to 'authorized' and RowStatus to 'active' 4e. If set type is AP, Gateway queries endpoint for the current profile 4f. AP endpoint responds with its current profile 4g. Gateway sends wireless AP configuration message 4h. Endpoint responds with an accept message 4i. Gateway changes endpoint status to 'authorized' and RowSatus to 'active'

4.2. Configuration Process through the Gateway

The end-user must have the option to configure the endpoints, via the UI, prior to or after plugging it into the power outlet. The gateway must create an entry in the HomePlug Devices Table (hmPlgDevTable) table based on user input.

MIB Objects to Populate	Value
hmPlgDevRowStatus	'createAndWait'
hmPlgDevAssumedType	Assumed endpoint type
hmPlgDevEk	Device Encryption Key of the endpoint
hmPlgDevDesiredPwd	Row Pointer to 'hmPlgLogicaltNetworkPwd'
hmPlgDevMethod	'staticReservation'
hmPlgDevAuthState	'authorizationPending'

If the Assumed Device Type (hmPlgDevAssumedType) value is 'accessPoint', the gateway must also provide the end-user option to configure the Wireless Encryption settings for the endpoint. The gateway must create an entry in the HomePlug AP Devices Table (hmPlgApTable) and populate the objects below from user input.

Objects to Populate	Value
hmPlgApRowStatus	'createAndWait'
hmPlgApDesiredSsid	Desired SSID
hmPlgApDesiredSsidAdvertisement	Enable or Disable

hmPlgApDesiredTxChannel	Desired Transmit Channel
hmPlgApDesiredSecOperMode	Encryption Mode
hmPlgApDesiredFilterStatus	Enable/Disable CPE Filtering (Optional)

If the value of the Desired Encryption Mode (hmPlgApDesiredSecOperMode) is set to anything other than 'none' the gateway must automatically create an entry in the AP Security Table (hmPlgApSecTable) with the MAC Address of the endpoint.

Objects to Populate	Value
hmPlgApSecMacAddr	MAC Address of the HomePlug Endpoint
hmPlgApSecWEPPassphrase	WEP Passphrase
hmPlgApSecWPAPskPassphrase	WPA PSK Passphrase
hmPlgApSecWEPKeyIndex	WEP Key Index (Default to '1' for 128-BIT WEP).
hmPlgApSecWEPKey1	WEP Key derived from Passphrase or set directly
hmPlgApSecWEPKey2	WEP Key derived from Passphrase or set directly
hmPlgApSecWEPKey3	WEP Key derived from Passphrase or set directly
hmPlgApSecWEPKey4	WEP Key derived from Passphrase or set directly
hmPlgApSecWPAPreShareKey	WPA Key derived from Passphrase or set directly
hmPlgApSecWPARekeyTime	WPA PSK re-key interval

The gateway must support the creation of encryption keys through a Passphrase entry for 64-Bit and 128-Bit WEP. The requirements on the Passphrase to Key algorithm are detailed in the CableHome 1.1 specification, specifically in description of the cabhPsDev802dot11SecPassPhraseToWEPKey MIB object. The Passphrase value will be inputted by the end-user via the UI. The gateway must create four (4) keys of length ten (10) hexadecimal character each for 64-Bit WEP. The end-user may only select one (1) key which must be determined by the Key Index (hmPlgApSecWepKeyIndex). For 128-Bit WEP, only one (1) key of length twenty-six (26) hexadecimal characters must be created.

For WPA-PSK the Passphrase to key derivation requirements are also detailed in CableHome 1.1 specification: Reference description of the cabhPsDev802dot11SecPSKPassPhraseToKey MIB object. The end-user must enter a passphrase that is between eight (8) to sixty-three (63) characters in length. The end-user must also select the ReKey interval (hmPlgApSecWPARekeyTime). If no ReKey interval is specified it must default to 86400 seconds.

Alternatively, the end-user may enter the encryption keys for WEP and-or WPA-PSK directly via the UI. As such, Passphrase value must be null.

Once all the necessary encryption objects in the entry are populated, the gateway must change the RowStatus in the HomePlug Devices (hmPlgDevTable), HomePlug AP Table (hmPlgApTable), and HomePlug AP Security (hmPlgApSecTable) tables to 'notInService' to indicate that the device is not active.

Assuming that an endpoint with factory settings is plugged into the outlet after it was configured in the gateway: The gateway must be capable of sensing its presence on the power-line network. Upon detecting a new endpoint the gateway must set the hmPlgDevCommit object to 'authStaticReservation' for each entry in the hmPlgDevTable with hmPlgDevAuthState value is 'authorizationPending'.

If an endpoint is detected during its configuration through the gateway, the gateway must wait for the configuration to be completed prior to triggering the hmPlgDevCommit to 'authStaticReservation'. So in the case where the assumed type is set to Ethernet or USB the gateway must proceed once the endpoint encryption key is entered. However, if the assumed type is set to Access Point then the gateway must wait for the wireless settings to be entered.

The gateway must encrypt the key derived from referenced hmPlgDevDesiredPwd value with the Device Encryption key and transmit it to the endpoint once the commit is triggered. As per HomePlug specification if the endpoint is successful in decrypting the message with its default key, it will update the key it utilizes for encryption. The endpoint will also transmit back to the gateway an update successful message detailed in the HomePlug specification. Reference: HomePlug 1.0.1 specification for the encryption algorithm.

However, if the user has configured multiple endpoints (by entered multiple encryption keys) and the gateway senses multiple endpoints on the network that are not part of its logical network, the gateway must sequentially loop through all entries part in the hmPlgDevTable with status 'authorizationPending'.

Once the endpoint replies with a commit successful message the gateway must set the hmPlgDevAuthState to 'authorized' and the hmPlgDevRowStatus to 'active'. The gateway must attempt to retrieve the endpoint's MAC Address and if possible its type (USB, Ethernet or AP).

If the endpoint's device type cannot be determined the gateway must always query to retrieve the endpoint's wireless settings by sending a Current Profile Query (CurrProfileQuery) message. The message must be initiated by setting the hmPlgDevCommit object to 'epCurrProfileQuery'. If the endpoint does not respond to the message, the gateway must attempt to retransmit the query message twice more with a wait period of 3 seconds in between. If all query attempts fail the gateway must set the hmPlgDevType to 'nonEnhancedOther' and the hmPlgAuthState bit to 'authorized' and the hmPlgDevRowStatus to 'active'. If the endpoint does respond the gateway must update the hmPlgDevType object accordingly, set the hmPlgAuthState object to 'authorized' and the hmPlgDevRowStatus to 'active'.

If the endpoint's type is determined to be Ethernet or USB but the assumed type was set to Access Point, the gateway must not transmit with the Current Profile Query message. The hmPlgAuthState must be set to 'authorized' the hmPlgDevType object to 'nonEnhancedOther' and hmPlgDevRowStatus to 'active'. If the endpoint is determined to be an Access Point, but the assumed type was set to Ethernet or USB the gateway must proceed with a query message but set the hmPlgAuthState to 'apConfigPending'. The assumption is that the endpoint will operate with factory default wireless settings or be will be configured by the end-user directly.

If the type is determined to be an Access Point and the assumed type was set to "accessPoint", the gateway must push the pre-configured Wireless Encryption parameters by setting the hmPlgDevCommit value to 'apEncryptProfile'. The gateway must send the AP Encryption Profile (ApEncryptionProfile) message to the endpoint.

CurrProfileQuery Message

Atrib. Name	Value	Description
TBD	CurrProfileQuery	Message Name
TBD		Transaction ID
TBD	hmPlgMgmtXmlSchemaVer	Supported XML Schema Version

Access Point Current Profile Query Response Message

Attrib. Name	MIB Objects to Populate	Description
TBD	-	Message Name: EpCurrProfile
TBD	-	Transaction ID of the CurrProfileQuery
TBD	hmPlgDevXmlSchemaVer (do not repopulate)	Supported XML Schema Version
TBD	hmPlgDevMacAddr (do not repopulate)	Endpoint MAC Address
TBD	hmPlgDevDescr	Endpoint Description
TBD	hmPlgDevType (do not repopulate)	Endpoint Type
TBD	hmPlgAp802dot11MacAddr	AP 802.11 Interface MAC Address
TBD	hmPlgApCurrSsid	AP Current SSID
TBD	hmPlgApCurrSsidAdvertisement	AP Current SSID Broadcast State
TBD	hmPlgApCurrTxChannel	AP Current Transmit Channel
TBD	hmPlgApSecCapabilities	AP Supported Encryption Schemes
TBD	hmPlgApCurrSecOperMode	AP Current Encryption Mode
TBD	hmPlgApCurrWEPPassphrase	AP Current WEP Passphrase
TBD	hmPlgApCurrWPAPassphrase	AP Current WPA-PSK Passphrase
TBD	hmPlgApCurrWEPEncryptKey	AP Current WEP Encryption Key
TBD	hmPlgApCurrWPAPreShareKey	AP Current WPA PreShare Key
TBD	hmPlgApCurrCpeFilterStatus	AP MAC Address Filtering Status
TBD	hmPlgApCurrCpeFilterMacAddr	List of permitted MAC Addresses

ApConfigProfile Message

Atrib. Name	Value	Description
TBD	ApConfigProfile	Message Name: ApConfigProfile
TBD		Transaction ID
TBD	hmPlgMgmtXmlSchemaVer	Supported XML Schema Version by the PS
TBD	hmPlgApDesiredSsid	SSID
TBD	hmPlgApDesiredSsidAdvertisement	Enabled or Disabled
TBD	hmPlgApDesiredTxChannel	Desired Transmit Channel
TBD	hmPlgApDesiredSecOperMode	None or WEP and or WPA-PSK
TBD	hmPlgApDesiredFilterStatus	Enabled or Disabled
TBD	hmPlgApCpeFilterCpeMacAddr	List of permitted MAC Addresses (if Enabled)

(Based on the hmPlgApDesiredSecOperMode value selection the ApConfigProfile message must also include values configured in the hmPlgApSecTable)

Atrib. Name	Value	Description
TBD	hmPlgApSecWEPPassphrase	WEP Passphrase
TBD	hmPlgApSecWPAPskPassphrase	WPA PSK Passphrase
TBD	hmPlgApSecWEPKeyIndex	WEP Key Index (Default to '1' for 128-BIT WEP).
TBD	hmPlgApSecWEPKey	WEP Key derived from Passphrase or set directly
TBD	hmPlgApSecWPAPreShareKey	WPA Key derived from Passphrase or set directly
TBD	hmPlgApSecWPARekeyTime	WPA PSK re-key interval

The AP will respond with an accept (ApConfigProfileAccepted) or decline message (ApConfigProfileDecline). If the message is ApConfigProfileDecline the gateway must set the Authorization State to 'apConfigInvalid' and prompt for re-entry of the Wireless Configuration parameters. If an accept message is received the gateway must change the Authorization State to 'authorized' and set the hmPlgDevRowStatus to 'active'.

ApConfigProfileAccept Message

Atrib. Name	Value	Description
TBD	ApConfigProfileAccept	Message Name
TBD		Transaction ID
TBD		Supported XML Schema Version by the Endpoint

ApConfigProfileDecline Message

Atrib. Name	Value	Description
TBD	ApConfigProfileDecline	Message Name
TBD		Transaction ID
TBD		Supported XML Schema Version by the Endpoint

4.3. Adding Pre-Configured Endpoints to the Network

The gateway must permit the addition of endpoints to the logical network configured through other means. For example, the end-user may utilize a vendor specific software utility to configure the network password on the endpoints. The gateway must attempt to identify the endpoint's MAC Address and possibly its device type. The gateway must create an entry in the hmPlgDevTable for the device and set the values to following:

MIB Objects to Populate	Value
hmPlgDevRowStatus	'active'
hmPlgDevMacAddr	MAC Address of the endpoint
hmPlgDevType	Endpoint type
hmPlgDevDesiredPwd	Row Pointer to 'hmPlgLogicaltNetworkPwd'
hmPlgDevMethod	'manual'
hmPlgDevAuthState	'authorized'

The gateway must query to find out the endpoint's type and if it is determined to be an Access Point, the gateway must automatically send a Current Profile Query (CurrProfileQuery) message

EXHIBIT A

by setting the hmPlgDevCommit object to 'epCurrProfileQuery'to retrieve the AP's configured settings. If the endpoint's device type cannot be determined the gateway must query to retrieve the endpoint's wireless settings regardless by sending the CurrProfileQuery message.

If the endpoint does not respond to the message, the gateway must retransmit the query twice more with a wait period of 3 seconds in between. If all query attempts fail the gateway must set the hmPlgDevType to 'nonEnhancedOther' and the hmPlgAuthState object to 'authorized' and the hmPlgDevRowStatus to 'active'. If the endpoint does respond the gateway must set the hmPlgAuthState to 'apConfigPending' and the hmPlgDevRowStatus to 'active'.

If the endpoint's type is determined to be Ethernet or USB the gateway must not transmit with the Current Profile Query message. The hmPlg'State must be set to 'authorized', the hmPlgDevType to 'nonEnhancedOther' and hmPlgDevRowStatus to 'active'.

CurrProfileQuery Message

Atrib. Name	Value	Description
TBD	CurrProfileQuery	Message Name
TBD		Transaction ID
TBD	hmPlgMgmtXmlSchemaVer	Supported XML Schema Version

Access Point Current Profile Query Response Message

Attrib. Name	MIB Objects to Populate	Description
TBD	-	Message Name: EpCurrProfile
TBD	-	Transaction ID of the CurrProfileQuery
TBD	hmPlgDevXmlSchemaVer (do not repopulate)	Supported XML Schema Version
TBD	hmPlgDevMacAddr (do not repopulate)	Endpoint MAC Address
TBD	hmPlgDevDescr	Endpoint Description
TBD	hmPlgDevType (do not repopulate)	Endpoint Type
TBD	hmPlgCurrPassword	Endpoint Current Password
TBD	hmPlgAp802dot11MacAddr	AP 802.11 Interface MAC Address
TBD	hmPlgApCurrSsid	AP Current SSID
TBD	hmPlgApCurrSsidAdvertisement	AP Current SSID Broadcast State
TBD	hmPlgApCurrTxChannel	AP Current Transmit Channel
TBD	hmPlgApSecCapabilities	AP Supported Encryption Schemes
TBD	hmPlgApCurrSecOperMode	AP Current Encryption Mode
TBD	hmPlgApCurrWEPPassphrase	AP Current WEP Passphrase
TBD	hmPlgApCurrWPAPassphrase	AP Current WPA-PSK Passphrase
TBD	hmPlgApCurrWEPEncryptKey	AP Current WEP Encryption Key
TBD	hmPlgApCurrWPAPreShareKey	AP Current WPA PreShare Key
TBD	hmPlgApCurrCpeFilterStatus	AP MAC Address Filtering Status
TBD	hmPlgApCurrCpeFilterMacAddr	List of permitted MAC Addresses

If the hmPlgApCurrCpeFilterStatus is determined to be 'enabled', however the hmPlgApDesiredCpeFilterStatus object will be set to 'disabled' by default. In this situation the gateway must send an AP Configuration Profile (ApConfigProfile) message to disable the MAC Address filter. The gateway must also add the CPE MAC Addresses identified on the AP to the hmPlgApCurrCpeFilterTable with the hmPlgApCpeFilterMapping object set to 'accessPointSpecific (2)'.

ApConfigProfile Message

Atrib. Name	Value	Description
TBD	ApConfigProfile	Message Name: ApConfigProfile
TBD		Transaction ID
TBD	hmPlgMgmtXmlSchemaVer	Supported XML Schema Version by the PS
TBD	hmPlgApDesiredCpeFilterStatus	Disabled

5. Gateway Initialization Process

When the gateway initializes it must attempt to automatically reestablish connectivity with all endpoints part of its Logical Network(s). The gateway must set the status of the hmPlgDevAuthState to 'authorized' and hmPlgDevRowStatus to 'active' for each endpoint that is active. The gateway must automatically send a CurrProfileQuery message by setting the hmPlgDevCommit object to 'epCurrProfileQuery' to each endpoint determined to be an access point in the hmPlgApDevTable.

All enhanced endpoints will respond with a current profile (EpCurrProfile) message utilizing its current password value for encryption. The gateway must translate the message and verify if the values received in the profile message match configuration values in the MIB database. The profile message will contain the following values:

Access Point Current Profile Query Response Message

Attrib. Name	MIB Objects to Populate	Description
TBD	-	Message Name: EpCurrProfile
TBD	-	Transaction ID of the CurrProfileQuery
TBD	hmPlgDevXmlSchemaVer (do not repopulate)	Supported XML Schema Version
TBD	hmPlgDevMacAddr (do not repopulate)	Endpoint MAC Address
TBD	hmPlgDevDescr	Endpoint Description
TBD	hmPlgDevType (do not repopulate)	Endpoint Type
TBD	hmPlgCurrPassword	Endpoint Current Password
TBD	hmPlgAp802dot11MacAddr	AP 802.11 Interface MAC Address
TBD	hmPlgApCurrSsid	AP Current SSID
TBD	hmPlgApCurrSsidAdvertisement	AP Current SSID Broadcast State
TBD	hmPlgApCurrTxChannel	AP Current Transmit Channel
TBD	hmPlgApSecCapabilities	AP Supported Encryption Schemes
TBD	hmPlgApCurrSecOperMode	AP Current Encryption Mode
TBD	hmPlgApCurrWEPPassphrase	AP Current WEP Passphrase
TBD	hmPlgApCurrWPAPassphrase	AP Current WPA-PSK Passphrase
TBD	hmPlgApCurrWEPEncryptKey	AP Current WEP Encryption Key
TBD	hmPlgApCurrWPAPreShareKey	AP Current WPA PreShare Key
TBD	hmPlgApCurrCpeFilterStatus	AP MAC Address Filtering Status
TBD	hmPlgApCurrCpeFilterMacAddr	List of permitted MAC Addresses

If in the case where the gateway is offline and the end-user re-configures an Access Point's wireless settings manually, when the gateway is turned back on it must over-ride the AP settings by reverting to the values set in the gateway.

In situations where the gateway initializes from a Reset to Factory Default all authentication with configured endpoints may be lost. The Logical Network Password will be restored to "HomePlug". So in this case the end-user will have to re-enter the device encryption keys for all endpoints to reestablish the network.

6. Endpoint Initialization

When a configured endpoint initializes the gateway must set the status of the hmPlgDevRowStatus object to 'active'. If the endpoint type is known to be an AP the gateway must automatically send a CurrProfileQuery message by setting the hmPlgDevCommit object to 'epCurrProfileQuery'.

7. HomePlug IP Device Table

The gateway must maintain an entry for all LAN IP devices that are connected via a HomePlug endpoint. The values must be stored in the hmPlgCpeDevTable.

8. Changing Access Point Configuration

The end-user may change the Access Point settings via the gateway UI which must be updated on the endpoint. Upon setting the hmPlgDevCommit to 'apConfigProfile', the gateway must send an AP Configuration Profile (ApConfigProfile) message to the endpoint.

ApConfigProfile Message

Atrib. Name	Value	Description
TBD	ApConfigProfile	Message Name: ApConfigProfile
TBD		Transaction ID
TBD	hmPlgMgmtXmlSchemaVer	Supported XML Schema Version by the PS
TBD	hmPlgApDesiredSsid	SSID
TBD	hmPlgApDesiredSsidAdvertisement	Enabled or Disabled
TBD	hmPlgApDesiredTxChannel	Desired Transmit Channel
TBD	hmPlgApDesiredSecOperMode	None or WEP and or WPA-PSK
TBD	hmPlgApCurrCpeFilterStatus	AP MAC Address Filtering Status
TBD	hmPlgApCpeFilterMacAddr	List of permitted MAC Addresses

(Based on the hmPlgApDesiredSecOperMode value selection the ApConfigProfile message must also include values configured in the hmPlgApSecTable)

Atrib. Name	Value	Description
TBD	hmPlgApSecWEPPassphrase	WEP Passphrase
TBD	hmPlgApSecWPAPskPassphrase	WPA PSK Passphrase
TBD	hmPlgApSecWEPKeyIndex	WEP Key Index (Default to '1' for 128-BIT WEP).
TBD	hmPlgApSecWEPKey	WEP Key derived from Passphrase or set directly
TBD	hmPlgApSecWPAPreShareKey	WPA Key derived from Passphrase or set directly
TBD	hmPlgApSecWPARekeyTime	WPA PSK re-key interval

The AP will respond with an accept (ApConfigProfileAccepted) or decline message (ApConfigProfileDecline). If the message is ApConfigProfileDecline the gateway must set the Authorization State to 'apConfigInvalid' and prompt for re-entry of the Wireless Configuration parameters. If an accept message is received the gateway must change the Authorization State to 'authorized' and set the hmPlgDevRowStatus to 'active'.

9. Changing Network Password

The end-user may change the Network Password for one or more of the supported Logical Networks on the gateway. As such the gateway must inform the endpoints part of the Logical Network(s) about the password update. The gateway must be capable of utilizing the each endpoint's unique encryption key to encrypt the new encryption key derived from the Logical Network password and transmitting it to each endpoint. The gateway must set the 'hmPlgLogicalNetworkPwdControl' to 'true' for the row corresponding to the logical network(s) whose password is being changed to trigger the update.

If the endpoint is online it will respond with a confirmation message and proceed with updating its network password to the new logical network password.

If the endpoint is offline the gateway must queue the message indefinitely from the point of the commit and set the hmPlgDevAuthState to 'networkPwdUpdatePending'. So when an endpoint is detected on the power-line network, the gateway must attempt to inform the endpoint of the network password change.

In the case where one or more of the endpoints were added to the logical network via means outside the Static Reservation method, the gateway will not contain the endpoints factory default unique encryption key and will fail to update that endpoint. To avoid this scenario, the UI will be designed to prompt the end-user to add the DEK of such devices prior to committing the logical password network update change.

10. Deleting Endpoint Entry

When an entry is deleted for an enhanced endpoint the gateway must send an Endpoint Set to Factory (EpSetToFactory) message to the endpoint by setting the hmPlgDevCommit to 'setToFactory'. The commit must trigger an EpSetToFactory message to the endpoint which is to be deleted. The gateway must then wait for the endpoint to respond with an acknowledgement message prior to deleting the entry. The endpoint, if registered, will respond with an Endpoint Set to Factory Acknowledge (EpSetToFactoryAck) message. Upon receiving this message the gateway must delete all references for the endpoint from the hmPlgDevTable, hmPlgApTable and the hmPlgApSecTable by setting the Row Status to 'destroy' for each entry corresponding to the endpoint's MAC Address.

EpSetToFactory message

Atrib. Name	Value	Description
TBD	EpSetToFactory	Message Name: EpSetToFactory
TBD		Transaction ID
TBD	hmPlgMgmtXmlSchemaVer	Supported XML Schema Version by the PS
TBD	hmPlgMgmtPsMacAddr	MAC Address of the PS's HomePlug interface

EpSetToFactoryAck message

Atrib. Name	Value	Description
TBD	EpSetToFactoryAck	Message Name: EpSetToFactoryAck
TBD	Value from the EpSetToFactory	Transaction ID sent in the EpSetToFactory Message
TBD	hmPlgMgmtXmlSchemaVer	Supported XML Schema Version by the PS
TBD		MAC Address of the End Point

If no confirmation is received, the gateway must set the authorization state (hmPlgDevAuthState) for the entry to 'deletionPending' and set the Row Status to 'notInService'. Once the endpoint initializes the gateway must complete the queued delete process.

If the device type is non-enhanced, the gateway must reset the endpoints default password back to "HomePlug" and remove the entry from the hmPlgDevTable. This is to be done by utilizing the factory encryption key of the endpoint to encrypt "HomePlug" as the password.