A CABLE OPERATOR'S GUIDE TO CABLEHOME™ 1.0 FEATURES

Kevin Luehrs, Steve Saunders
CableLabs®
Nancy Davoust
YAS Broadband Ventures

ABSTRACT

CableLabs released the CableHome 1.0 specifications to home networking device vendors and to the general public in April 2002. The specification standardizes a suite of residential gateway functions enabling cable operators to deliver managed broadband services to their high-speed data service subscribers over the subscribers' home networks. This paper introduces the CableHome initiative at CableLabs and the Portal Services (PS) Element as a foundation, and then discusses component functions of the PS Element in terms of setup and configuration, and alternatives for operation. Each cable operator will have the opportunity to configure CableHome-compliant devices in a manner consistent with its business objectives. Although many of the options provided by the CableHome 1.0 specifications are described, specific configuration details are beyond the scope of this paper.

OVERVIEW

Introduction to CableHome

CableHome is an initiative undertaken by CableLabs at the direction of its member cable television companies to develop an infrastructure enabling cable operators to extend high-quality, managed, value-added broadband services to subscribers in their homes in a fashion that is as convenient as possible for the subscribers. The CableHome 1.0 specifications are a set of functional and messaging interface requirements describing cable-industry standard methods for implementing address acquisition, device configuration, device management, network address translation, event reporting, remote diagnostic procedures, secure software download, firewall monitoring and policy file download, as well as other functions in a residential gateway device or element connecting networked devices. These devices are located in a subscriber's home and are connected to the Internet through a DOCSIS cable modem and a cable operator's hybrid-fiber coaxial (HFC) network. Figure 1 illustrates a number of key CableHome network elements and concepts, which are described below. CableHome 1.0 specifications introduce and use concepts of Wide Area Network (WAN) (cable network) and home Local Area Network (LAN) address realms, translated (LAN-Trans) and non-translated (LAN-Pass) address realms within the home LAN, IP addresses intended to be used for management traffic (WAN-Man IP) or for user/application data traffic (WAN-Data IP), and Embedded (with a cable modem) versus stand-alone residential gateway functions. The specifications refer to LAN IP Devices, which are the elements connected to a subscriber's home network communicating using the TCP/IP protocol suite. The specifications also define a Portal Services (PS) Element, which is a collection of functions providing the capabilities listed in the previous paragraph between the WAN and LAN realms, serving networked devices in the translated address realm in the home, and providing management capabilities for monitoring and configuring the various functions of the PS.

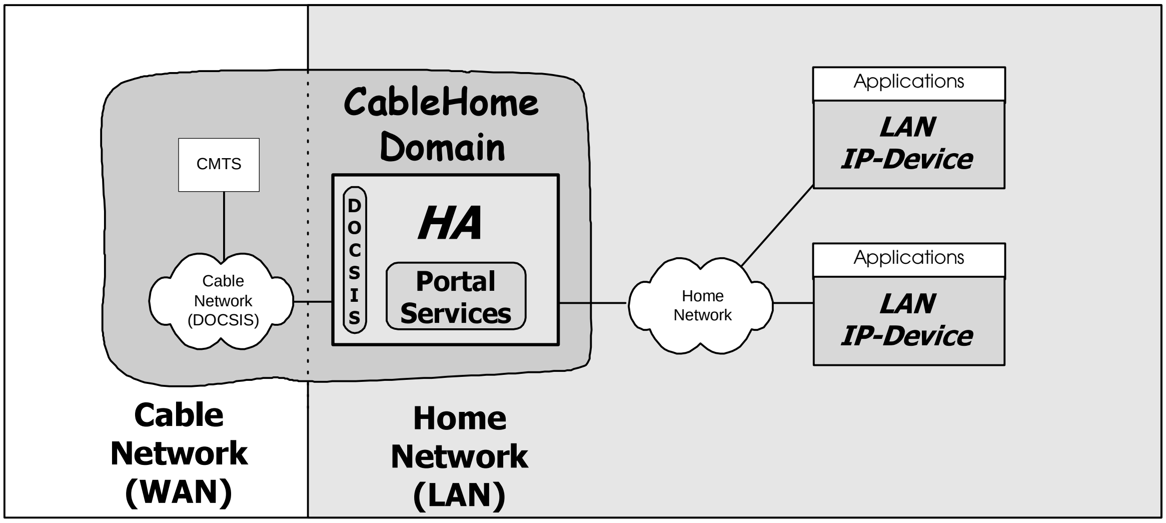

Figure 1: CableHome Network Elements

CableHome functions, in the form of the PS, always operate in conjunction with DOCSIS functionality. The PS functions may reside within the same physical device as the DOCSIS functionality (Embedded PS) or in a separate device (Stand-alone PS). In all cases, CableHome identifies the Home Access (HA) Device as the collection of DOCSIS and CableHome functionality that connects the Cable Network to the Home Network.

The CableHome Domain is the extent of the WAN and LAN networks which carry CableHome messaging and includes devices that implement CableHome functionality. CableHome extends DOCSIS functionality further to the edge of the cable network and provides a set of tools the cable operator can use to better support his or her high-speed data subscribers. In the following sections, the PS Element is described to the next level of detail.

Portal Services Element

The CableHome 1.0 PS Element is a collection of eight functions intended for implementation in a residential gateway device with a broadband connection through a DOCSIS cable modem. The PS supports multiple IP clients in the home, and gives them controlled access to the Internet via the cable modem's CPE interface. Most of the PS functions are similar to functions implemented in residential gateway products in the market today, with additional features to enable cable operators to provide quality, managed, value-added service to their high-speed data service subscribers.

Seven of the eight CableHome PS functions are referred to as portals since they link the cable operator's WAN to the subscriber's home LAN. The CableHome Portal functions are listed below:

1) CableHome Dynamic Host Configuration Protocol (DHCP) Portal (CDP):
Provides network address information functions including a server for the networked elements in a subscriber's home.

2) CableHome Address Portal (CAP):
Interconnects the WAN and LAN address realms for application data traffic via network address translation and bridging.

3) CableHome Management Portal (CMP):
Provides an interface between the cable

operator and manageable parameters in the PS through the CableHome-specified Management Information Base (MIB).

4) CableHome Naming Portal (CNP):
Provides a simple DNS service for networked home devices requiring naming services.

5) CableHome Test Portal (CTP):
Provides a means for the cable operator to initiate remote ping and loopback tests.

6) CableHome Security Portal (CSP):
Participates in authentication, and exchanges keying material with the Key Distribution Center (KDC) server for CableHome security functions in the PS.

7) CableHome Quality of Service (QoS) Portal (CQP):
Provides transparent bridging for QoS messaging between PacketCable applications and the PacketCable QoS infrastructure on the cable network.

The eighth PS function is a firewall function that provides protection of the home network from malicious attack.

Relative to residential gateway products currently available through retail, a CableHome 1.0-compliant residential gateway with PS functions will allow the cable operator to better manage subscribers' broadband experiences and minimize subscribers' home network down time. CableHome 1.0 also allows cable operators to provide security and privacy to their high-speed data subscribers.

Compatibility With Existing CableLabs Specifications

An important design goal of the CableHome 1.0 specifications was to be compatible with existing CableLabs and industry specifications to the greatest extent possible. The CableHome specifications were developed for networked elements that will connect to cable operators' HFC network through a CableLabs Certified DOCSIS cable modem. The CableHome PS Element is an extension of the DOCSIS infrastructure, and employs procedures very similar to those required in DOCSIS specifications for management, event reporting, configuration file download, and secure software download.

CableHome 1.0 specifies features compatible with a DOCSIS 1.0 infrastructure, as well as additional features that support advanced capabilities of DOCSIS 1.1 and PacketCable™ infrastructures. CableHome-specified features therefore provide cable operators with a migration path as their facilities evolve over time.

PROVISIONING

CableHome 1.0 specifications define provisioning as the device initialization and initial configuration required to enable the PS Element and networked devices in the home to exchange meaningful information with one another and with elements connected to the cable network and to the Internet. CableHome specifications define a set of provisioning tools to accomplish this so that the cable operator can add value to the process. A goal of the CableHome specification is to define provisioning processes that enable all CableHome functionality without the need for subscriber interaction.

CableHome provisioning tools consist of a DHCP client, a DHCP server, a bulk configuration tool, and a time of day client. These tools have been designed to work on cable networks implementing DOCSIS 1.0 or

DOCSIS 1.1 cable modems (CM) and cable modem termination systems (CMTS), as well as on cable networks where advanced features such as those defined in the PacketCable specifications, are deployed.

Address Assignment

The first step in the device initialization process is the acquisition of a network address. The PS plays a dual role with respect to network address acquisition. The CableHome DHCP Portal (CDP) function is comprised of a CableHome DHCP Client (CDC) to acquire one or more network address(es) from the cable operator, and a CableHome DHCP Server (CDS) to assign private IP address leases to networked elements in the home.

DHCP Options 43, 61, and 177

To fully support addressing capabilities specified by CableHome 1.0, a cable operator’s DHCP server must interpret DHCP Option 61 (client identifier), DHCP Option 43 with sub-options, and DHCP Option 177 with sub-options, plus 18 additional standard DHCP options.

Option 61 allows the PS to uniquely identify itself to the headend DHCP server when requesting multiple WAN-Data IP addresses using a single unique hardware (MAC) address. Support of Option 61 is required when operating the PS in NAT Primary Packet Handling Mode.

Option 43 with sub-options allows the PS to provide more detailed information about its capabilities. For example, CableHome 1.0 defines Option 43 sub-option 2 for the PS to indicate whether it is embedded with a cable modem or is a stand-alone device. Sub-option 11 indicates whether the address the PS is attempting to acquire is for the WAN-Man Interface or for the WAN-Data Interface.

The PS uses Option 177 sub-option 3 to request the location of the cable operator’s SNMP manager, and uses sub-option 11 to request the KDC server’s IP address.

CDC Operation

CableHome 1.0 specifications require the PS to implement two unique hardware (Media Access Controller - MAC) addresses. The WAN-Management (WAN-Man) MAC address allows the PS to uniquely identify itself to the address server (DHCP server) in the headend for acquisition of an IP address to be used for the exchange of management messages between the cable operator's network management system (NMS) and the management entity in the PS. The CDC will always attempt to acquire this WAN-Man IP address. Depending upon which primary packet handling mode the PS is configured to operate (described later in this document), the WAN-Man IP address may be the only IP address the PS acquires. The second hardware address specified by CableHome 1.0 is the WAN-Data MAC address, intended to be used in conjunction with DHCP Option 61 to uniquely identify one or more PS WAN Data Interface(s) for the acquisition of one or more global IP address(es) to map to private IP addresses in the home. The factory default value for the number of WAN-Data IP addresses the PS is required to request is zero. The cable operator must modify a WAN-Data IP Address Count parameter in order to configure the PS to request one or more WAN-Data IP addresses. The cable operator can configure the PS to use the WAN-Man IP address for application data traffic as well as for management traffic. Alternately, the PS can be configured to use one WAN-Data IP address to share among one or more LAN IP Devices when operating in port translation mode, and one or more WAN-Data IP addresses for 1:1 mapping to private LAN IP addresses when operating in address translation mode.

CDS Operation

Unless the cable operator chooses to serve all LAN IP Devices in the home with network addresses directly from the headend DHCP server, he must configure the PS to assign private IP addresses to the subscriber's home LAN elements. This is the function of the CDS. The CDS grants leases for private IP addresses in response to DHCP DISCOVER messages issued by LAN IP Devices, within constraints defined by three cable operator-configurable management parameters: a LAN Address Threshold limit and LAN Address Pool Start and End parameters defining the range of private IP addresses available for assignment.

The CDS supports 18 standard DHCP options. The cable operator can provision values for these options, or allow the PS to assign factory default values defined in the CableHome specifications. The CDS does not "pass through" DHCP options received from the headend DHCP server to LAN IP Devices.

CableHome Provisioning Modes

Two Provisioning Modes are defined in the CableHome 1.0 specifications: DHCP Provisioning Mode and Simple Network Management Protocol (SNMP) Provisioning Mode. The cable operator configures the PS to operate in these modes as described below.

DHCP Provisioning Mode follows closely the provisioning method defined for a cable modem in the DOCSIS 1.0 and DOCSIS 1.1 specifications, and is intended for compatibility with DOCSIS 1.0 and DOCSIS 1.1 systems. Characteristics of DHCP Provisioning Mode are listed below:

- PS configuration file name and location are provided to the PS in the DHCP OFFER
- The PS is required to download a PS configuration file
- The PS will default to using SNMP version 1 and version 2 for management messaging, but can be configured by the cable operator to operate in SNMP version 3 coexistence mode

The cable operator configures the PS to operate in DHCP Provisioning Mode by including the location of the Trivial File Transfer Protocol (TFTP) server containing the appropriate PS configuration file in the *siaddr field* and the name of the PS configuration file the file field of the DHCP OFFER message, AND by not including DHCP Option 177 sub-option 51 (Key Distribution Center (KDC) server location) in the DHCP OFFER. If Option 177 sub-option 51 and either or both of the PS configuration file parameters are not present, or if all three parameters are present in the DHCP OFFER message received from the headend DHCP server, the PS will generate an event indicating an error condition, and re-issue DHCP DISCOVER to try again for a valid combination.

SNMP Provisioning Mode allows the PS to take advantage of advanced features similar to those defined in the PacketCable Multimedia Terminal Adapter (MTA) specifications. Characteristics of PS operation in SNMP Provisioning Mode are as follows:

- The PS will authenticate itself to a Key Distribution Center using the Kerberos protocol, and will exchange security keys with the KDC to use when exchanging management messages with the NMS via SNMP version 3
- PS configuration file download is optional. If no PS configuration file is provided, the PS will operate using factory default settings.

- The PS will default to SNMPv3 Coexistence Mode operation and will use SNMP version 3 for management messaging
- The cable operator may optionally trigger the PS to download a PS configuration file by writing the PS configuration file location and file name in URL format via SNMP version 3

The cable operator configures the PS for SNMP Provisioning Mode by not including PS configuration file information (file name and TFTP server location) and by including DHCP Option 177 sub-option 51 (KDC server location) in the DHCP OFFER message sent to the PS. When configured to operate in SNMP Provisioning Mode, the PS will exchange messages with the KDC server to acquire keying material to authenticate itself with the KDC server. Once authentication has been completed, the PS is capable of exchanging secure SNMP version 3 management messages with the NMS in the headend. When secure management message exchange is enabled, the cable operator has the option of modifying a parameter in the PS via an SNMP message to trigger the download of a PS configuration file. However, since the CableHome specifications define factory default values for all necessary parameters, the PS does not necessarily require a PS configuration file to operate, and could potentially operate indefinitely on the cable network without receiving a configuration file.

<u>PS Configuration File</u>

The PS configuration file provides a means for the cable operator to issue configuration instructions in bulk to a PS Element. It also provides the means for providing the PS with code verification certificates (CVC) used for secure software image download procedures.

CableHome 1.0 specifies TFTP for the transfer of configuration files (PS configuration file and firewall configuration file) from the cable operator's headend to the PS.

Any configuration file downloaded by the PS should be authenticated to ensure that the file is not corrupt. The PS configuration file is authenticated with a hash value, which is a code compared to the result of a calculation performed on the file itself. Correct correlation between the hash value and the calculated value indicates that the file is valid. When the PS is operating in DHCP Provisioning Mode, the hash value is passed to the PS with the configuration file name in the *file* field of the DHCP OFFER message. Download of the PS configuration file to the PS operating in DHCP Provisioning Mode is triggered by the presence of the configuration file name and location in the DHCP OFFER.

When the PS operates in SNMP Provisioning Mode, the cable operator must provision the hash value in the PS by writing it to the PS via SNMP, before the configuration file download is triggered by a second SNMP message writing the configuration file name and address to the PS.

Once triggered to download the PS configuration file, the PS will continue trying to download the file until it successfully downloads and processes the file. If the PS encounters an error when processing the PS configuration file, it will report the failure as an event and try again to download the file.

The cable operator is responsible for correctly sequencing configuration parameters in the PS configuration file, for not creating conflicts between configuration file-set parameters and SNMP-set parameters, for providing the correct PS configuration file name and location to the PS, for providing the correct hash value to the PS, and for correctly triggering the file download.

MANAGEMENT

CableHome 1.0 specifications describe several features allowing the cable operator to monitor and configure PS parameters, format event reporting, and initiate remote testing for diagnosing problems on the home LAN. The CableHome Management Portal (CMP) function of the PS is the entity that responds to SNMP management messages from the cable operator's NMS. Access to the CMP is through the PS WAN-Man Interface, which is bound to the WAN-Man IP address.

The PS is capable of operating in two Management Modes. The cable operator can configure the PS to operate in NmAccess mode for DOCSIS 1.0 compatibility, or to operate in SNMP v3 Coexistence Mode, which is supported by DOCSIS 1.1 and PacketCable specifications.

Management Mode

A PS operating in DHCP Provisioning Mode defaults to operating in NmAccess Mode, and to using SNMP v1/v2. In this mode the cable operator can control access to management parameters by writing to the NmAccess Table of the DOCSIS Device MIB [RFC 2669]. The cable operator can also put the PS into SNMPv3 Coexistence Mode by writing the appropriate parameters to the snmpCommunityTable [RFC 2576] through the PS configuration file or via direct SNMP messaging. Once in Coexistence Mode, the PS will respond to SNMP v1, v2, or v3 messages.

When the PS is operating in SNMP Provisioning Mode, it defaults to operation in SNMP v3 Coexistence Mode for management messaging. All three versions of SNMP are supported but by default version 1 and version 2 are disabled. The cable operator can enable them by writing appropriate parameters to the snmpCommunityMIB [RFC 2576].

When operating in SNMPv3 Coexistence Mode, access to manageable parameters is controlled by View-based Access Control Model (VACM) Views [RFC 2575] and User-based Security Model (USM) [RFC 2574] Users. CableHome 1.0 defines one User, CHAdministrator, and one View (read and write access to all parameters), which are assigned to the cable operator. With the rights afforded to the CHAdministrator User, the cable operator can create additional Users and Views. In this way, the cable operator can allow access on an object-by-object basis to the subscriber or other parties.

Event Reporting

CableHome 1.0 specifies over 50 defined events for asynchronous reporting of errors and pass and fail conditions for several processes. Most of these are events also defined in the DOCSIS specifications, and some are CableHome-specific events. The cable operator can control how the events are reported, and can throttle individual events by writing to appropriate objects of the DOCSIS Device MIB, support for which is required in the CableHome 1.0 specifications. Events can be reported as local (to the PS) log entries, system log entries, or traps. The cable operator can retrieve local log entries by accessing the appropriate MIB objects using SNMP.

CableHome Test Portal

The CableHome Test Portal (CTP) consists of two remote diagnostic testing functions: CTP Connection Speed Tool and CTP Ping Tool. The cable operator initiates these tests by issuing appropriate SNMP commands to the CMP.

The Connection Speed Tool is a form of loopback test in which the CTP sends packets, the length, number, and frequency of which are specified by the cable operator, to a privately-addressed element connected to the home LAN. If the loopback function is supported in the home network device, it will echo the packet(s) back to the CTP, which will log statistics such as round trip time, packets sent, and packets received for the cable operator to retrieve from a set of MIB objects. The Connection Speed Tool enables the cable operator to gain some performance statistics about the link between the PS and any connected device with an IP address that supports the loopback function.

The Ping Tool allows the operator to ping a privately-addressed device in the home to verify connectivity between the PS and the device. The cable operator configures the destination IP address, number of packets, packet size, frequency, and timeout parameters, and retrieves test results by accessing MIB objects using SNMP.

CableHome-Defined Parameters

Access to PS parameters is one of the values CableHome provides by enabling the cable operator to provide managed service to high-speed data subscribers.

CableHome defines five MIBs for this purpose: PS Device (PSDEV) MIB, CDP MIB, CAP MIB, CTP MIB, and Security (SEC) MIB. MIB objects are accessible through the CMP, via the PS WAN-Man Interface.

The PS DEV MIB provides access to device information such as serial number, hardware version, and MAC addresses; device reset control; provisioning mode control; configuration file parameters; provisioning state information; notification (trap) objects; and software image download parameters.

CDP MIB objects include information about home LAN elements (IP addresses, client identifiers, lease times, host names, and DHCP options); server addresses; LAN address control parameters (address limits and address pool range); and a table of client identifiers associated with the WAN-Data Interface. The cable operator has visibility on privately-addressed home LAN elements through this MIB.

WAN-to-LAN IP address mappings stored in the PS are accessible through the CAP MIB. This MIB also provides access to timeout parameters for the mappings, a table of hardware addresses of LAN elements assigned address leases directly from the headend DHCP server, and the primary packet handling mode control parameter. The cable operator can provision WAN-to-LAN IP address mappings by writing to the appropriate parameters in the CAP MIB.

The CTP MIB contains parameters that control and configure the Connection Speed and Ping Tools, and provides access to the results of those tests.

Firewall parameters including the firewall policy file name and location, hash value, and enable/disable control are accessible through the Security MIB. This MIB also provides control over firewall-related events that allows the cable operator to be notified about various types of attacks.

PACKET HANDLING

A collection of functions within the CableHome Address Portal (CAP) provide packet handling capabilities that enable IP packet flow from the WAN to the LAN, and vice versa (the NAT, NAPT, and Passthrough functions described below). In addition, the CAP provides a function that protects the HFC network from intra-home traffic (the USFS function described below).

The packet handling functions that are applied will be dependent upon whether public, private, or mixed addressing is desired for LAN IP Devices. If the cable operator has chosen to address LAN IP Devices privately, then network address translation (NAT) functions must be employed in order to enable packet flow between the LAN and WAN. If public addressing has been chosen for LAN IP Devices, then the CAP must ensure that all traffic (including DHCP messaging) is transparently bridged between the LAN and WAN. In addition, packet handling for mixed public and private addressing of LAN IP Devices is supported.

In order to control which packet handling functions are active, the cable operator can configure the PS to operate in one of four primary packet-handling modes, which are listed below:

- Passthrough Bridging Mode
- CableHome Network Address Port Translation (C-NAPT) Transparent Routing Mode
- CableHome Network Address Translation (C-NAT) Transparent Routing Mode
- Mixed Bridging/Routing Mode

These modes determine the mapping functions applied between WAN-Data IP addresses and the addresses of devices connected to the subscriber's home LAN.

The cable operator configures the PS to operate in one of these modes by modifying the CAP Primary Mode parameter passed as a PS configuration file parameter or via an SNMP set message. The factory default value of the CAP Primary Mode is C-NAPT Transparent Routing Mode.

The cable operator will configure the PS to operate in Passthrough Bridging Mode when one or more of the following considerations are relevant:

- Public addressing is desired for all IP devices in a home (in anticipation that applications will be running in the home that are C-NAT/C-NAPT intolerant)
- It is important to preserve existing home device address assignment models (i.e. public addresses served directly to CPE by cable network DHCP servers)

It should be noted that, when in Passthrough mode, addresses supplied to a home might reside on different logical IP subnets.

In Passthrough mode, the CAP acts as a transparent bridge for packets flowing between the LAN and WAN. Forwarding decisions are made primarily at OSI Layer 2 (data link layer) and C-NAT/C-NAPT Transparent Routing functions are not applied. Like all other traffic between WAN and LAN elements in this mode, DHCP messaging is bridged, resulting in direct address acquisition communications between home devices and cable network DHCP servers. As a result, all LAN IP Devices will receive public IP addresses, and no address translation will be required.

The cable operator will configure the PS to operate in C-NAPT Transparent Routing Mode if one or more of the following considerations are relevant:

- Conservation of public IP addresses is important
- Same-subnet addressing for devices on the home LAN is important

C-NAPT address translation is a one-to-many mapping function. A single public WAN IP address is mapped to multiple private LAN addresses via port multiplexing. In C-NAPT Mode the CDC acquires one WAN-Data IP address and uses this address for each of one or more WAN address - private LAN address tuple(s). The single WAN-Data IP address can be shared between two or more networked elements connected to the home LAN. C-NAPT address mappings can be created dynamically or the cable operator can provision them.

Dynamic C-NAPT address mappings are created when a privately addressed element in the home network sources a packet destined for an IP address outside the private address space in the home. When the packet reaches the PS, the CAP will determine whether a mapping exists for the source address and, finding none, will create the mapping, replace the packet's source address with the WAN-Data IP address, and forward the packet to the PS Element's default gateway.

If the cable operator creates a C-NAPT mapping, the CAP will find the mapping when an "outbound" packet arrives from the home LAN, replace the packet's private source IP address with the corresponding WAN-Data IP address, and forward the packet to the upstream router in the cable operator's network. C-NAPT mapping creates a 1-to-many association between the WAN-Data IP address and the private IP addresses bound to elements connected to the home LAN.

The cable operator will configure the PS to operate in C-NAT Transparent Routing Mode if one or more of the following considerations are relevant

- Same subnet addressing for devices on the home LAN is important
- Applications that cannot tolerate C-NAPT Routing will be running in the home.
- Source based routing within the cable network will be employed in conjunction with network address translation

It is possible that a set of public IP addresses provided to a home may not reside on the same subnet. C-NAT address translation is a one-to-one mapping function. The PS will own all of the public address supplied to the home, and they will be uniquely mapped to the same-subnet private addresses that have been assigned by the CDS to LAN IP Devices. This one-to-one mapping function enables a privately addressed home device to be uniquely associated with a public WAN IP address, and thus source based routing techniques used in the cable network will not be compromised.

Dynamic C-NAT address mappings are created when a privately addressed element in the home network sources a packet destined for an IP address outside the private address space in the home. When the packet reaches the PS, the CAP will determine whether a mapping exists for the source address and, finding none, will create the mapping, replace the packet's source address with the WAN-Data IP address, and forward the packet to the PS Element's default gateway. If there is not a WAN-Data IP address available against which to create the C-NAT mapping, an event will be generated.

If the cable operator creates a C-NAT mapping, the CAP will find the mapping when an "outbound" packet arrives from the home LAN, will replace the packet's private source IP address with the corresponding WAN-Data

IP address, and will forward the packet to the upstream router in the cable operator's network. C-NAT mapping creates a one-to-one association between the WAN-Data IP address and the private IP addresses bound to elements connected to the home LAN.

The cable operator will configure the PS to operate in Mixed Bridging/Routing Mode if the cable operator wishes to use private addressing for some of the devices in the home (thus requiring C-NAT/C-NAPT Routing functionality) while concurrently using public addressing for other devices (thus requiring the Passthrough Bridging function).

To operate in this mode, the cable operator sets the primary mode to C-NAT or C-NAPT Transparent Routing. In addition, one or more MAC addresses, belonging only to those LAN IP Devices whose traffic is to be bridged, are written into what is known as the Passthrough Table.

When in this mode, the CAP 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 Passthrough Table, 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 Passthrough Table, the frame is transparently bridged to the appropriate LAN interface. If the MAC address does not exist in the Passthrough Table, the packet is processed by higher layer functions, including the C-NAT/C-NAPT Transparent Routing functions.

The Upstream Selective Forwarding Switch (USFS) function prevents intra-home communications from affecting the HFC network and is in place primarily for the case in which devices in the home are publicly addressed and reside on different logical IP subnets.

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 ipNetToMediaTable [RFC-2011], which contains a list of MAC Addresses, their corresponding IP Addresses, and PS Interface Index numbers of the physical interfaces with which these addresses are associated. 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 DHCP table entries.

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 out the proper PS LAN interface. 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).

NAME RESOLUTION

CableHome 1.0 specifications define a basic name resolution service for devices connected to the subscriber's home LAN. This function, embodied in the CableHome Naming Portal (CNP), establishes a table of host names, client identifiers, and private IP addresses for home LAN elements. This feature allows the home user to refer to networked devices in the home by a human-readable name rather than by an IP address.

The CNP obtains host name and associated private IP address information for LAN IP Devices from the CDP LAN Address Table in the CDP MIB. The CDP LAN Address Table is populated when devices in the home are served by the CDS with private address leases.

When a DNS query is issued to the PS Element's DNS server IP address from a privately-addressed element in the home, the CNP refers to its table and if the requested host name is found, the CNP replies with the appropriate IP address. If the CNP does not locate the requested host name in its table, it replies to the querying device on the home LAN with the globally-routable IP address of the cable operator's DNS server. It is then the responsibility of the home LAN device to direct its query directly to the cable operator's DNS server for host name resolution.

Queries from devices in the passthrough realm, i.e., those devices served directly from the cable operator's headend DHCP and DNS servers, will be addressed directly to the cable operator's headend DNS server and will not be served by the CNP.

CableHome 1.0 requires compliance with standard DNS message formats described in [RFC 1034] and [RFC 1035].

SECURITY

The security in CableHome can vary widely depending upon which system the cable operator deploys and how the operator configures options for each system. The security considerations discussed here are intended to give the operator some insight into what security configuration settings exists for each system. Security settings will be discussed for

- Items that need to be configured in the back office prior to network operation
- PS Element security configuration during the provisioning process
- PS Element security configuration via SNMP
- Firewall configuration
- Secure Software Download

The first step to understanding the security considerations is for the operator to decide which network environment CableHome will be deployed upon. The CableHome specification was created to operate in three environments. These three environments are referred to as DOCSIS 1.0 system, DOCSIS 1.1 system, and CableHome Enhanced environment. A DOCSIS 1.0 system is a PS configured to operate in DHCP Provisioning Mode and NMAccess management mode. A DOCSIS 1.1 system is a PS configured to operate in DHCP Provisioning Mode and SNMPv3 Coexistence Mode for management messaging.

This discussion will point out security for each of these options and explain the relevant security setting for each.

Back Office Security Configurations

In the back office the cable operator will need to set up and configure the CableHome network, prior to running the CableHome system. There are several security considerations and configurations needed.

Configuration for secure software download is required in the DOCSIS 1.0 system for the stand-alone PS Element and for either the embedded or stand-alone PS Element in the DOCSIS 1.1 system. The operator must insert one or more CVCs into the PS configuration file to enable the secure software download. The operator may choose to apply for a service provider CVC with CableLabs, and must keep secret the private key associated with the CVC. The cable operator may then optionally insert their CVC in the configuration file to give the operator control over all software download images that will be accepted by the PS Element. The options for control of software download are discussed in more detail in the software download section. Secure software download provides the same security and uses the same method for all three systems.

The CableHome Enhanced environment requires security configuration for secure software, mutual authentication and secure management messages. For CableHome, secure software download requirements are the same as for DOCSIS 1.0 or 1.1 systems. To meet the requirement for mutual authentication, CableHome uses X.509 certificates and the Kerberos protocol with the PKINIT extension.

The cable operator must set up the KDC for Kerberos functionality. The KDC must have a KDC certificate issued by the Service Provider CA certificate, which means the cable operator must apply for a CableLabs Service Provider CA certificate. The KDC must also be provisioned with the CableLabs Manufacturer Root CA certificate and the Local System CA certificate if one exists. If the cable operator is planning on using the same KDC for PacketCable then the KDC will need the MTA Root CA Certificate as well. With the CA certificate comes the responsibility of running a public key infrastructure (PKI), and the cable operator will need to implement the appropriate security policies and procedures.

The Kerberos set up involves more than just provisioning the box with certificates. It involves planning for the Kerberos infrastructure, configuration of the infrastructure (multiple KDCs) and configuration of CableHome management message security for SNMPv3.

To create a Kerberos infrastructure several key issues need to be resolved. The Kerberos protocol has a master and slave relationship within for its server hierarchy. The cable operator will need to decide how many Kerberos realms are needed, the name of each realm, how many slave KDCs are needed and where they should be located, hostnames for each KDC and how to map the hostnames into the Kerberos realms. The operator will also need to set up and manage the Kerberos database.

The KDCs are then configured for the infrastructure settings along with the Kerberos message settings and the CableHome specific settings. For the KDC messages, encryption with DES3 and authentication with MD5 is required and may need to be configured. The CableHome Kerberos configurations include various message parameter options. For example the operator will need configuration for the desired Kerberos ticket duration.

The KDC supplies the PS Element with the initial information used to set up the SNMPv3 keys, one key for authentication and one key for privacy (encryption). For this reason, the KDC needs to be provisioned with the correct encryption and authentication algorithms for the KDC to negotiate with the PS Element within the Kerberos message exchanges on behalf of the SNMP manager in the NMS. SNMPv3 authentication is required, and must use a default value for the MD5 hash algorithm. The operator may support other hash algorithms and can add those to the list of acceptable or preferred hash algorithms. Encryption on management messages is currently optional and the operator will either need to list the null algorithm, if no encryption is desired, or the DES algorithm if encryption is needed. DES is currently the only SNMPv3 supported encryption algorithm. Both the KDC and the NMS will need to be configured to choose the appropriate hash and encryption algorithm for the NMS and PS Element to communicate securely.

PS Element Security Configuration During the CableHome Provisioning Process

Security within the PS Element provisioning process includes security on the information provided in the message exchanges, establishment of security configuration settings as a result of the information extracted from the messages, and completion of the mutual authentication process. Security for the message exchanges was set up in the back office configuration and the KDC and NMS were also appropriately provisioned with the security configuration settings needed to communicate with the PS Elements. The cable operator should not need to configure anything during the provisioning process itself.

On DOCSIS 1.0 and 1.1 systems within CableHome mutual authentication is not available. Security on management messages is possible in SNMPv3 Coexistence Mode if the operator uses SNMPv3. The cable operator will set up security for the PS Element the same way it is described in DOCSIS 1.1 specifications for the cable modem. The PS Element will receive its initial keying material for SNMPv3 from the Diffie-Hellman kick start. To provide the Diffie-Hellman kick start with all the appropriate parameters, the CableHome Administrator calculates the values for security name and public number and populates the usmDHKickstartTable with these values.

In SNMP provisioning mode, the PS Element completes mutual authentication with the KDC, key management for SNMPv3, configuration file settings, and configuration file security. There are three parts to authentication: the identity credential, the checking of the identity credential for validity and the common means to communicate the identity information. CableHome specifies an industry standard identification credential, X.509 certificates, in conjunction with RFC 2459 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 AS Reply messages. 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.

If an operator wishes to enable secure software download, the trigger is a CVC and must be sent in the PS configuration file. The operator has five choices for which CVCs to place in the configuration file. These are discussed in the secure software download section. The CVCs placed in the PS configuration file must match the CVCs sent in the code image download. Prior to placing any CVCs in the PS configuration file, the CVCs must be verified and validated as part of the back office security procedures.

The configuration file requires a SHA-1 hash to protect it from being changed in transit. The NMS will add the hash to the configuration file prior to placing it on the TFTP server for download. The PS element will check the hash prior to processing the configuration file.

SNMP PS Element Security Configuration

Some security information may be updated via SNMP. This allows the operator flexibility in managing the network and does not require the PS Element to get a new configuration file each time these items need to be updated. The operator may initiate and monitor secure software downloads, update CVC certificate information, and monitor firewall events via SNMP MIB variables.

Firewall Configuration

Firewall configuration follows the same method as specified for PS Element configuration. In DHCP provisioning mode, the cable operator provides information to trigger a firewall configuration in the PS configuration file. If the IP address of the firewall configuration file TFTP server, the firewall configuration file filename, the hash of the firewall configuration file, and the encryption key (if the firewall configuration file is encrypted) are included in the PS configuration file then the PS Element will request the firewall configuration 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. If encrypted, the file is decrypted. The file is then processed. In SNMP provisioning mode, the cable operator may trigger a firewall configuration by passing firewall configuration file information in either the PS configuration file or via SNMP, but the rest of the process is the same.

Firewall attack events are monitored via SNMP MIBs. The cable operator must configure the firewall attack time limit and maximum number of events allowed within that time limit. An event is logged if more than the maximum number of attacks occurs. The operator security policy and procedures manual should instruct the administrator with an appropriate response to attacks.

Firewall rule sets are not defined in CableHome. A variable is defined to track the rule set version and an additional variable allows the operator to enable or disable the security policy for the firewall.

Secure Software Download Configuration

The DOCSIS CM controls embedded downloads. If the PS Element is embedded with a DOCSIS cable modem, then the software image must be a single image and the download will be controlled by the cable modem according to the DOCSIS specifications. If the PS Element is not embedded with the cable modem, then the PS Element has its own code image and is responsible for the secure software download process as specified in CableHome.

Inclusion of CVC(s) in the configuration file to match the CVC(s) in the code image enable secure operator controlled downloads. The cable operator will enable secure software download to the PS Element by placing the location of the file, the filename and the CVC(s) in the PS configuration file. Once secure software download is enabled, the operator can trigger a software download by sending the location of the file and the filename from the NMS. The download will only be triggered if the filename does not match the name of the current code image in the PS Element. In the configuration file the operator will choose between the five possible CVC combinations to provide authorization for specific images according to their security policy.

- Option 1: Send the manufacturer's CVC
- Option 2: Send the manufacturer's CVC and CableLabs CVC.
- Option 3: Send CableLabs CVC
- Option 4: Send the manufacturer's CVC and the service provider's CVC
- Option 5: Send the service provider's CVC

The manufacturer's CVC and corresponding signature ensure the code has not been altered since it left the manufacturer's facility. The signature can legally bind the manufacturer to any claims made about this particular code image. The CableLabs signature means that the code has been through the certification testing program and was passed by the certification board. The CableLabs certified sticker on the outside of the box is now accompanied by the CableLabs digital signature over the certified code image for certified product. The operator's signature will bind the signed code image according to the operator's security policy. Code images will only be downloaded into the PS Elements according to the operator's security policy, and it is up to the operator to define if the manufacturer, CableLabs, or operator approved code is appropriate for the PS Elements on their network.

Back office CVC validation is necessary. Prior to providing images for secure software download the operator must 1) validate and verify the CVC(s) and signature(s)on the code image, 2) validate and verify the CVC(s) prior to placement in the configuration file, 3) make sure the CVC(s) to be placed in the configuration file match those in the code image, 4) insert the CVC(s) into the configuration file, and if using the service provider CVC, then 5) attach the service provider CVC to the code image and sign the code image. The configuration file and code file is then ready to be placed on the TFTP server for the provisioning process to start. It is imperative for the PS to check the software image CVC(s) and signatures prior to use to make sure the code file has not been tampered with and to ensure the code has come from a trusted source.

The operator can either upgrade the PS Element to the next authorized version of the code or revert to a previous version of the authorized code at any time using the same process. To revert to a previous version of code, the manufacturer signing time on the code must either be equivalent to or later than the current version of the code installed in the PS Element. Logistically this means the cable operator will need to track signing times on all the valid code images for compliance to the security policy.

If secure software download fails for any reason, an event will be sent to the NMS and the cable operator will need to decide on the appropriate course of action.

There are many other aspects of security for CableHome that are not discussed in this paper. The goal was to address from a high level some of the items the cable operator will need to configure in order to deploy and maintain a secure CableHome network. It is critical for the cable operator to create and use a security policy and procedures manual for all aspects of its network access, information storage, technical configuration, security breaches, security auditing and reviews as well as the daily maintenance of security technology.

REFERENCES

CableHome 1.0 Specification, CH-SP-D01-020131, Cable Television Laboratories, Inc., January 31, 2002

PacketCable Security Specification, PKT-SP-SEC-I05-020116, Cable Television Laboratories, Inc., January 16, 2002, http://www.PacketCable.com./

Kerberos V5 Installation Guide, Release 1.2, Document Edition 1.1, Massachusetts Institute of Technology, January 9, 2002, http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.3/doc/install.html#SEC7

CableHome PSDEV MIB Specification, CH-SP-MIB-PSDEV-D02-020131, Cable Television Laboratories, Inc., January 31, 2002

CableHome CAP MIB Specification, CH-SP-MIB-CAP-D02-020131, Cable Television Laboratories, Inc., January 31, 2002

CableHome CDP MIB Specification, CH-SP-MIB-CDP-D02-020131, Cable Television Laboratories, Inc., January 31, 2002

CableHome CTP MIB Specification, CH-SP-MIB-CTP-D02-020131, Cable Television Laboratories, Inc., January 31, 2002

CableHome Security MIB Specification, CH-SP-MIB-SEC-D02-020131, Cable Television Laboratories, Inc., January 31, 2002

RFC 1034, IETF, Domain Names - Concepts and Facilities, November 1987.

RFC 1035, IETF, Domain Names - Implementation and Specification. November 1987.

RFC 2011, IETF, SNMPv2 Management Information Base for the Internet Protocol Using SMIv2, November 1996.

RFC 2459, IETF, Internet X.509 Public Key Infrastructure Certificate and CRL Profile. January 1999.

RFC 2574, IETF, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP), April 1999.

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

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

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