

CableOffice™

Commercial Services Annex 1.0 Specification

Superseded

CH-SP-CO-CSA-I02-040806

ISSUED

Notice

This 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.

© Copyright 2003-2004 Cable Television Laboratories, Inc.
All rights reserved.

Document Status Sheet

Document Control Number:	CH-SP-CO-CSA-I02-040806			
Document Title:	Commercial Services Annex 1.0 Specification			
Revision History:	WP01 – Released September 9, 2003 WP02 – Released October 21, 2003 WP03 – Released November 4, 2003 D01 – Released January 5, 2004 I01 – Released March 24, 2004 I02 – Released August 6, 2004			
Date:	August 6, 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.

Contents

1	SCOPE	1
1.1	Introduction and Overview	1
1.2	Key Assumptions	2
1.3	Purpose of document	2
1.4	Organization of document.....	2
1.5	Requirements	3
2	REFERENCES	4
2.1	Normative References	4
2.2	Informative References.....	4
2.3	Reference Acquisition	4
3	TERMS AND DEFINITIONS	5
4	ABBREVIATIONS AND ACRONYMS	7
5	REFERENCE ARCHITECTURE	9
5.1	Reference Architecture.....	9
5.1.1	Address Realms	10
5.2	Commercial Services Functional Reference Model	11
5.3	Example Scenarios	12
5.3.1	Simple Static IP Address Service	12
5.3.2	Static IP Addressing with DHCP service	13
5.3.3	Static IP Addressing with C-NAPT Service	14
5.3.4	Static IP Addressing with C-NAPT and DHCP Service	15
6	MANAGEMENT TOOLS	16
6.1	Wireless LAN Port Control	16
6.1.1	Goals and Design Guidelines	16
6.1.2	System Description.....	16
6.1.3	Requirements	16
6.2	Commercial Services Annex MIB Requirements	17
7	PROVISIONING TOOLS	18
7.1	DHCP Provisioning	18
7.1.1	Goals and Design Guideline.....	18
7.1.2	CSA CDP System Description.....	18
8	PACKET HANDLING AND ADDRESS TRANSLATION	21
8.1	Commercial Services Packet Handling Mode.....	21
8.1.1	Goals and Design Guidelines	21
8.1.2	System Description.....	21
8.1.3	Requirements	23

8.2 Packet Routing	24
8.2.1 Goals and Design Guidelines	24
8.2.2 System Description.....	24
8.2.3 Requirements	26
8.3 Routing Protocol Functionality and Configuration	27
8.3.1 Goals and Design Guidelines	27
8.3.2 System Description.....	27
8.3.3 Routing Protocol Requirements.....	29
9 GENERAL REQUIREMENTS	31
ANNEX A MIB OBJECTS (NORMATIVE)	32
APPENDIX I LAYER 2 TUNNELING FUNCTIONALITY (INFORMATIVE) ..	34
APPENDIX II ACKNOWLEDGEMENTS	35
APPENDIX III REVISION HISTORY	36

Figures

Figure 5-1 Commercial Services Logical Architecture	9
Figure 5-2 Commercial Services Address Realms	10
Figure 5-3 Commercial Services Sub-elements.....	11
Figure 5-4 Static Addressing Scenario.....	12
Figure 5-5 Static and Dynamic Addressing Scenario.....	13
Figure 5-6 Static Addressing with C-NAPT Scenario.....	14
Figure 5-7 Static IP Addressing with C-NAPT and DHCP Service	15
Figure 7-1 CDS Parent Range	18
Figure 8-1 CG with Attached Client Devices from Different LAN Realms	22
Figure 8-2 Network with Multiple Route Types	25
Figure I-1 Use of L2TP-v3 Functionality in CSA	34

Tables

Table 5-1 Commercial Services Functions	11
Table 7-1 CSA DHCP Option 60 Values.....	20
Table 8-1 Possible LAN CPE Client Configurations.....	23
Table 8-2 Network Entries in ipCidrRoute Table.....	26

COPE Superseded

1.1 Introduction and Overview

CableLabs has developed this specification to describe the architecture and operation that enable interoperability for devices compliant with this specification. This specification defines additional requirements to CableHome specifications that support management features and Internet services used in a commercial or business environment. The CableHome 1.0 specification [CH1.0] focuses on the residential gateway device as the single entry point into the home. CableHome 1.1 [CH1.1] expands this scope to specify additional features for the residential gateway and to standardize Quality of Service and LAN messaging features for IP host devices connected to home LANs. The Commercial Services Annex (CSA) specification adds features to the CableHome specifications, 1.0 [CH1.0] or 1.1 [CH1.1], that enable deployment of products with CableHome functionality in a commercial network environment where hosts may or may not be provisioned by the commercial gateway device.

The CSA architecture is based on the CableHome architecture, which 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, the CSA closely aligns its technical specifications with well-known industry standards, as well as other CableLabs projects. The CSA allows efficient use of the cable operators' system infrastructure by providing support for existing and future IP-based services into the commercial environment.

A commercial environment gives rise to a number of situations that are not expected within a residential environment, and which require explicit support. These include:

- The existence of a customer provided DHCP server on the LAN
- Servers residing on the LAN with statically assigned IP addresses
- Various combinations of multiple public IP subnets and a private IP subnet coexisting simultaneously on the LAN
- The need to selectively allow or disallow WAN access for both publicly and privately addressed LAN devices

This Annex defines the capabilities needed to deliver, manage, and support cable services when these types of commercial scenarios arise. The device that inter-connects the commercial LAN and the cable data network is referred to as the Commercial Gateway (CG). The goal of this annex is the creation of a cable operator-configurable CG centric environment that will interact meaningfully with IP based LAN devices (LAN IP Devices).

Following is a summary of the additional capabilities that are defined by the Commercial Services Annex, which are meant to extend the functions of a CableHome 1.0 [CH1.0] or 1.1 [CH1.1] compliant device:

Provisioning and Management

- Cable operator configuration of the Commercial Gateway with routing information
- Additional control of the Commercial Gateway DHCP server, including the ability to enable or disable Commercial Gateway DHCP service
- Enabling and disabling of wireless LAN interfaces
- Ability to enable and disable C-NAPT functionality

Addressing and Packet Handling

- Routing of packets destined to and sourced from the LAN, both with and without network address translation
- Selective WAN forwarding of packets sourced from both publicly and privately addressed LAN devices
- Communication of routing information to the WAN via RIPv2

1.2 Key Assumptions

The following assumptions are being made for the commercial services environment and functionality:

- The CableHome Commercial Gateway is the only connection to the WAN within a particular enterprise
- The CableHome Commercial Gateway DHCP server will serve zero or one LAN subnets
- There is only a single DHCP server active on the LAN
- The CableHome Commercial Gateway is the default gateway for locally attached subnets in the enterprise and may be assigned multiple LAN side addresses (1 for each subnet)
- If routers exist on the enterprise LAN, the commercial gateway will be connected directly to only a single router, and LAN IP devices may reside on the same subnet as that router
- The CableHome Commercial Gateway will not learn or send routing information on the LAN interface via any dynamic routing protocols
- Passthrough packet handling will be supported via the passthrough table
- Functionality is focused on (but not restricted to) a commercial gateway with an embedded cable modem.
- The CableHome C-NAT address translation mode will not be supported in CSA mode

1.3 Purpose of document

The purpose of the CSA 1.0 specification is to define a minimum set of implementation requirements for commercial gateway products that will standardize functionality for management and configuration interfaces. This will allow MSOs to use a single provisioning/management system to more efficiently configure and monitor multiple commercial gateway products from different vendors.

1.4 Organization of document

Organization of this document is consistent with the organization of the CableHome specifications. The Reference Architecture section covers the main elements and functions of the CSA architecture and how they relate to CableHome. The Management Tools section covers control of the wireless interface and MIB requirements. The Provisioning Tools section covers functionality needed to segment IP addresses and to control the local DHCP server. The Packet Handling and Address Translation section covers packet routing functions, network address translation modes, and communication of route information to the CMTS.

Each section is divided into the design objectives/guidelines, a functional description, and then the actual implementation requirements.

1.5 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. |

2 REFERENCES

2.1 Normative 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.

- [CH1.0] CableHome 1.0 Specification, CH-SP-CH1.0-I05-030801, August 1, 2003, CableLabs, www.cablelabs.com
- [CH1.1] CableHome 1.1 Specification, CH-SP-CH1.1-I05-040806, August 6, 2004, CableLabs, www.cablelabs.com
- [CO1] CableOffice Commercial Services Annex 1.0 MIB Specification, CH-SP-CO-MIB-CSA-I01-040324, March 24, 2004, CableLabs, www.cablelabs.com
- [RFC 791] IETF RFC-791 (STD0005), Internet Protocol, September 1981
- [RFC 1724] IETF RFC-1724, RIP Version 2 MIB Extension, Malkin, G. and Baker, F., November 1994
- [RFC 2082] IETF RFC-2082, RIP-2 MD5 Authentication, Baker, F. and Atkinson, R., January 1997
- [RFC 2096] IETF RFC-2096, IP Forwarding Table MIB, Baker, F., January 1997
- [RFC 2453] IETF RFC-2453 (STD0056), RIP Version 2, Malkin, G., November 1998
- [RFC 2863] IETF RFC-2863, The Interfaces Group MIB, McCloghrie, K. and Kastenholz, F., June 2000

2.2 Informative References

- [RFC 2328] IETF RFC-2328, OSPF Version 2, Moy, J., April 1998

2.3 Reference Acquisition

CableLabs Specifications:

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone 303-661-9100; Fax 303-661-9199; Internet: <http://www.cablelabs.com>

IETF Standards

- IETF Standards, Internet Engineering Task Force (IETF) Secretariat c/o Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100, Reston, VA 20191-5434, Phone 703-620-8990, Fax 703-620-9071, Internet: www.ietf.org

3 TERMS AND DEFINITIONS

This specification uses the following terms:

Address Realms	A network domain in which the network addresses are uniquely assigned to entities such that datagrams can be routed to them.
Authentication	The process of verifying the claimed identity of an entity to another entity.
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.
CableOffice	The CableLabs technology standardization initiative for commercial networks.
Commercial Gateway	A physical device, which contains the Portal Services functional element and provides the interface between the HFC and commercial network.
DHCP Provisioning Mode	DHCP driven PS configuration file download.
Dynamic Host Configuration Protocol (DHCP)	An Internet protocol used for assigning network layer (Internet Protocol) addresses.
Host	A computer or device connected to a network having a unique IP address.
Key	A mathematical value input into the selected cryptographic algorithm.
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.
Local DHCP server	A DHCP server that is installed on the local LAN, as opposed to the CDS which resides in the Commercial Gateway.
Media Access Control (MAC)	It is a sublayer of the Data Link Layer. It normally runs directly over the physical layer.
Multicast	To transmit a single message to a select group of recipients.
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.
Portal Services (PS)	A functional element that provides management and translation functions between the HFC and commercial network.
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 .

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.

Static Pool

A Pool of IP addresses that are used in static or manual assignment by the user.

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

CAP	CableHome Address Portal
CDC	CableHome DHCP Client
CDP	CableHome DHCP Portal
CDS	CableHome DHCP Server
CG	Commercial Gateway
CH	CableHome Host
CM	DOCSIS Cable Modem
CMP	CableHome Management Portal
CMTS	Cable Modem Termination System
C-NAT	CableHome Network Address Translation
C-NAPT	CableHome Network Address and Port Translation
DHCP	Dynamic Host Configuration Protocol
DOCSIS	Data-Over-Cable Service Interface Specification
HFC	Hybrid Fiber Coax
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LAN	Local Area Network
LAN-Pass	Pass-through Local Area Network address
LAN-Trans	Translated Local Area Network address
LAN-Route	Routed Local Area Network address
MAC	Media Access Control
MIB	Management Information Base
MSO	Multiple Systems Operator

NAPT	Network Address and Portal Translation
NAT	Network Address Translation
PS	Portal Services
RFC	Request for Comments
SNMP	Simple Network Management Protocol
USFS	Upstream Selective Forwarding Switch
WAN	Wide Area Network
WAN-Data	Wide Area Network Data Address Realm
WAN-Man	Wide Area Network Management Address Realm

5 REFERENCE ARCHITECTURE

CableHome 1.0/1.1 defines the reference architecture that serves as the basis for the Commercial Services Annex architecture. For detailed coverage of this foundational architecture, please refer to the CableHome 1.0 specification [CH1.0] and the CableHome 1.1 specification [CH1.1]. The discussion that follows focuses on the functional and architectural differences and additions, relative to CableHome 1.0/1.1, required to define commercial services functionality.

5.1 Reference Architecture

The philosophy behind this CableOffice Commercial Services Annex 1.0 architecture is to keep it as similar as possible to the CableHome 1.0/1.1 reference architectures [CH1.0], [CH1.1]. The architectural elements and concepts are exactly the same as those defined in CableHome 1.0/1.1, but a few terms have been changed in order to reflect the fact that we are defining functionality for a commercial environment. The terminology changes include:

- The term “Commercial Gateway” (as opposed to “Residential Gateway”) is being used for the WAN access device
- The term “Commercial Services Domain” (as opposed to “CableHome Domain”) is being used to represent the collection of devices in which Commercial Services functionality resides and the networks over which Commercial Services protocols flow

The Commercial Services reference architecture is illustrated in Figure 5-1, with these modifications applied. Please refer to the CableHome 1.0/1.1 reference architecture sections for a complete description of the various architectural elements and concepts.

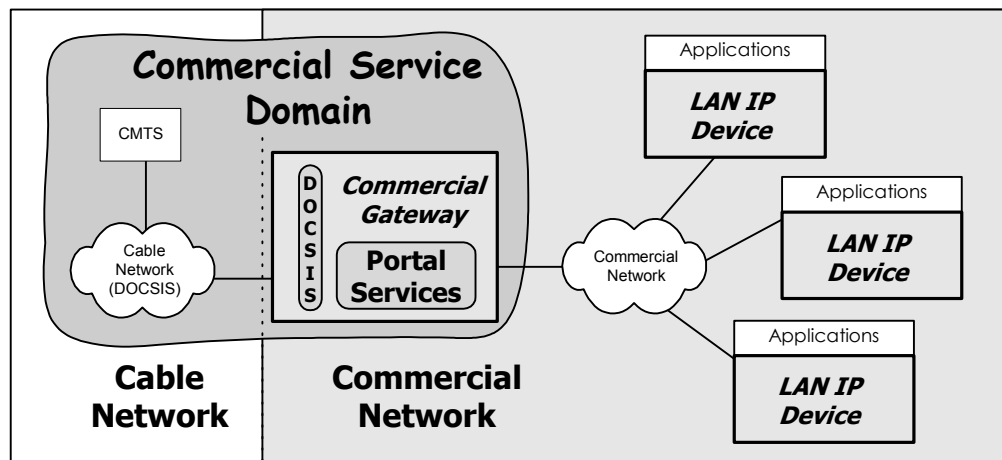


Figure 5-1 Commercial Services Logical Architecture

5.1.1 Address Realms

The concept of address realms is introduced and discussed in the CableHome 1.0/1.1 architectures. The routing support required by a commercial environment gives rise to an additional addressing realm on the LAN, the LAN Routed Address Realm (LAN-Route), as illustrated in Figure 5-2.

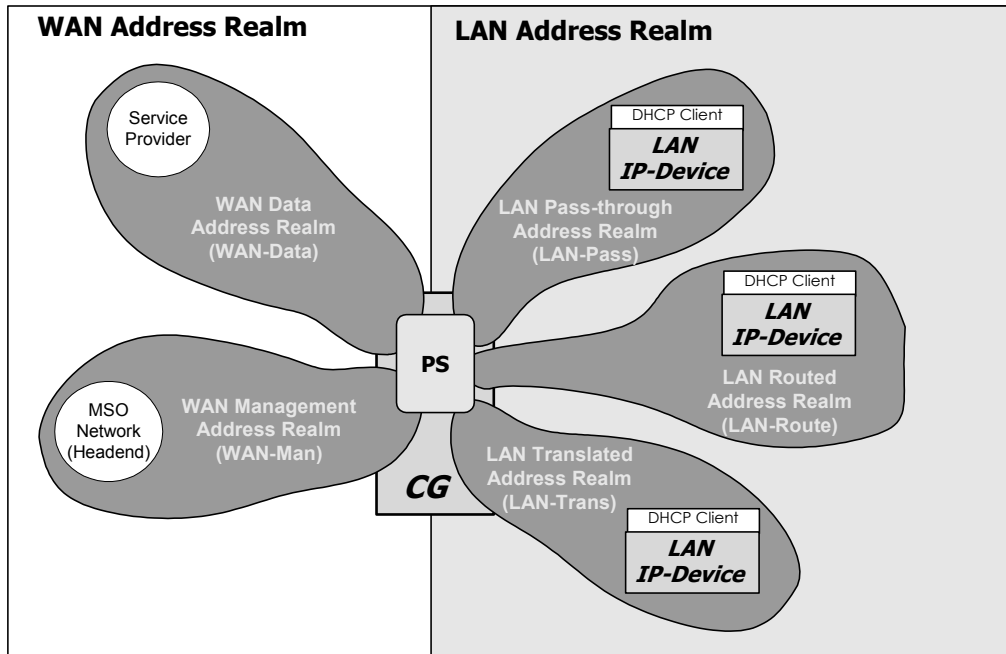


Figure 5-2 Commercial Services Address Realms

For a detailed description of the WAN-Data, WAN-Man, LAN-Pass, and LAN-Trans address realms, please refer to the CableHome 1.0/1.1 architectures. At a high level, the LAN address realms are distinguished by the method in which packets are handled as they pass through the Commercial Gateway, summarized as follows:

- **LAN-Pass:** packets source from or destined to devices within the LAN-Pass realm are bridged, at layer 2, through the Commercial Gateway
- **LAN-Route:** packets source from or destined to devices within the LAN-Route realm are routed, at layer 3, through the Commercial Gateway
- **LAN-Trans:** packets sourced from or destined to devices within the LAN-Trans realm are translated and routed, at layer 3, through the Commercial Gateway¹

¹ Modified per ECN CO-CSA-N-04.0134-2.

5.2 Commercial Services Functional Reference Model

The CableHome 1.0/1.1 architecture defines a number of functional elements which conceptually encapsulate groupings of related functionality, and against which requirements are written. The additional types of functionality required for commercial services support fit well within a subset of these already defined functional elements. Figure 5-3 shows the commercial services functional architecture, which includes the elements in the head-end with which commercial services functionality will interact, and Table 5-1 summarizes the commercial services functionality encapsulated by each of the functional elements. All of the CableHome functional elements are supported for a given product implementation, but for this level of abstraction only those that support CSA functionality are indicated in Figure 5-3 and Table 5-1.

The Portal Services (PS) functional element contains the sub-functions for the CG and provides in-premise and aggregated security, management, provisioning, addressing, routing and QoS services. The term “portal” is used to indicate services that interface the WAN to the LAN. It is possible that CSA compliant CG device could be used in a residential application. In this scenario, CSA functionality can be disabled and the PS sub-functions operate as defined by the CableHome specification.

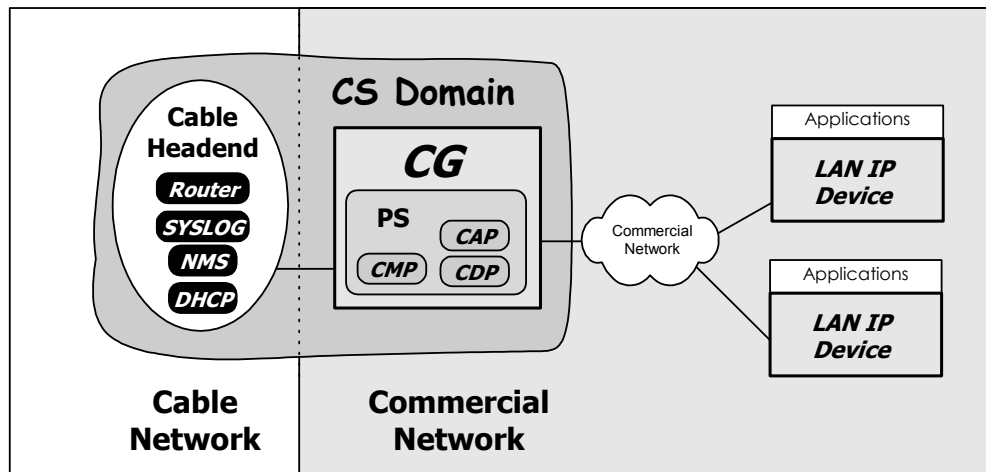


Figure 5-3 Commercial Services Sub-elements

Table 5-1 Commercial Services Functions

CSA Portal Functions	Description
CableHome Management Portal (CMP)	Provides a management interface between the cable network management system and the CSA functionality. Includes the ability to configure the PS with routing information.
CableHome Address Portal (CAP)	Within the PS, the CAP interconnects the WAN and LAN address realms for data traffic. This includes routing, addressing, and bridging functionality, as well as selective packet forwarding to the WAN and communication of routing information to the WAN.
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.

5.3 Example Scenarios

This section describes a number of practical commercial scenarios, providing examples of environments that must be supported by this Annex.

5.3.1 Simple Static IP Address Service

The Commercial Gateway device is configured to route traffic for any CPE with a host address within a configured IP address range. The Commercial Gateway device is assigned a public IP address of the network and a netmask which together represent the commercial LAN. The commercial customer is responsible for assigning IP addresses from this pool of public IP addresses either statically or via the customer's own DHCP server. Refer to Figure 5-4.

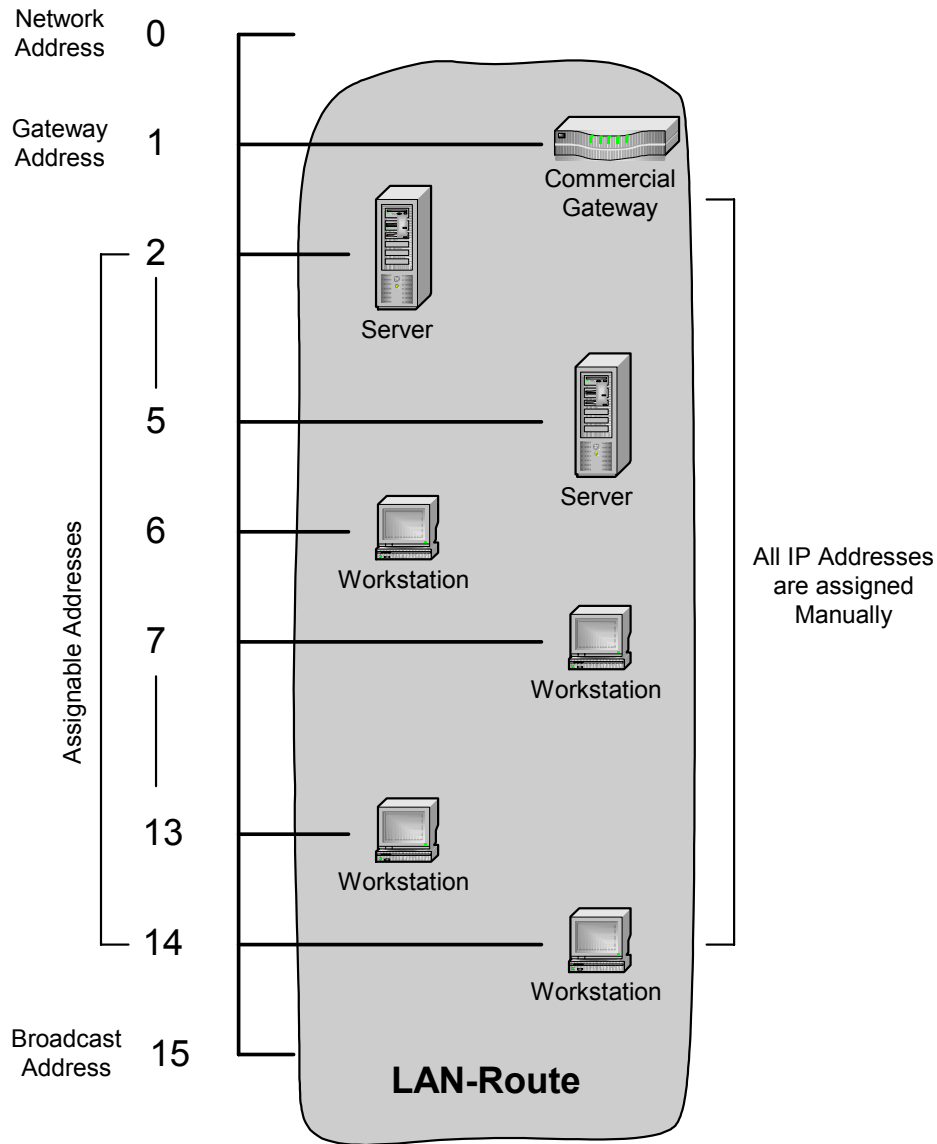


Figure 5-4 Static Addressing Scenario

5.3.2 Static IP Addressing with DHCP service

The Commercial Gateway device is configured to route traffic from any CPE with a host address within a configured IP address range. The Commercial Gateway device provides the DHCP service that serves the publicly routable IP addresses to the CPE devices. The size of the dynamically assigned address pool is adjustable, where the remaining IP addresses are to be statically assigned. The statically assigned IP addresses are taken from the beginning of the network pool, the dynamic addresses make up the remainder. Refer to Figure 5-5.

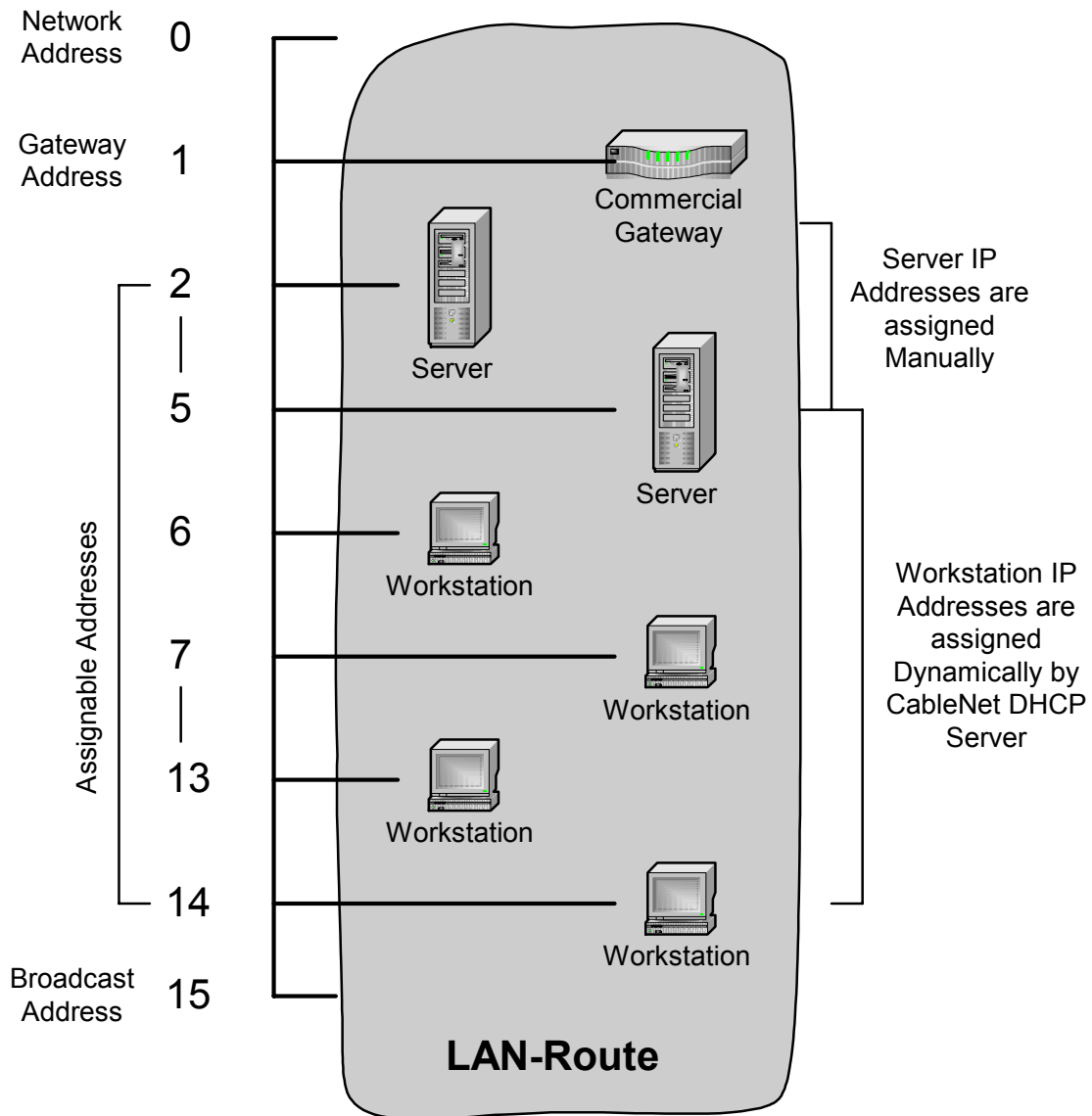


Figure 5-5 Static and Dynamic Addressing Scenario

5.3.3 Static IP Addressing with C-NAPT Service

The Commercial Gateway device is configured with two IP Networks, one public network and one private network. The public network is routed as per Section 5.3.1. The Commercial Gateway device uses C-NAPT to route traffic to and from the private network CPE. The commercial customer is responsible for assigning IP addresses for both the public and private networks and the Commercial Gateway device does not provide DHCP service. Refer Figure 5-6.

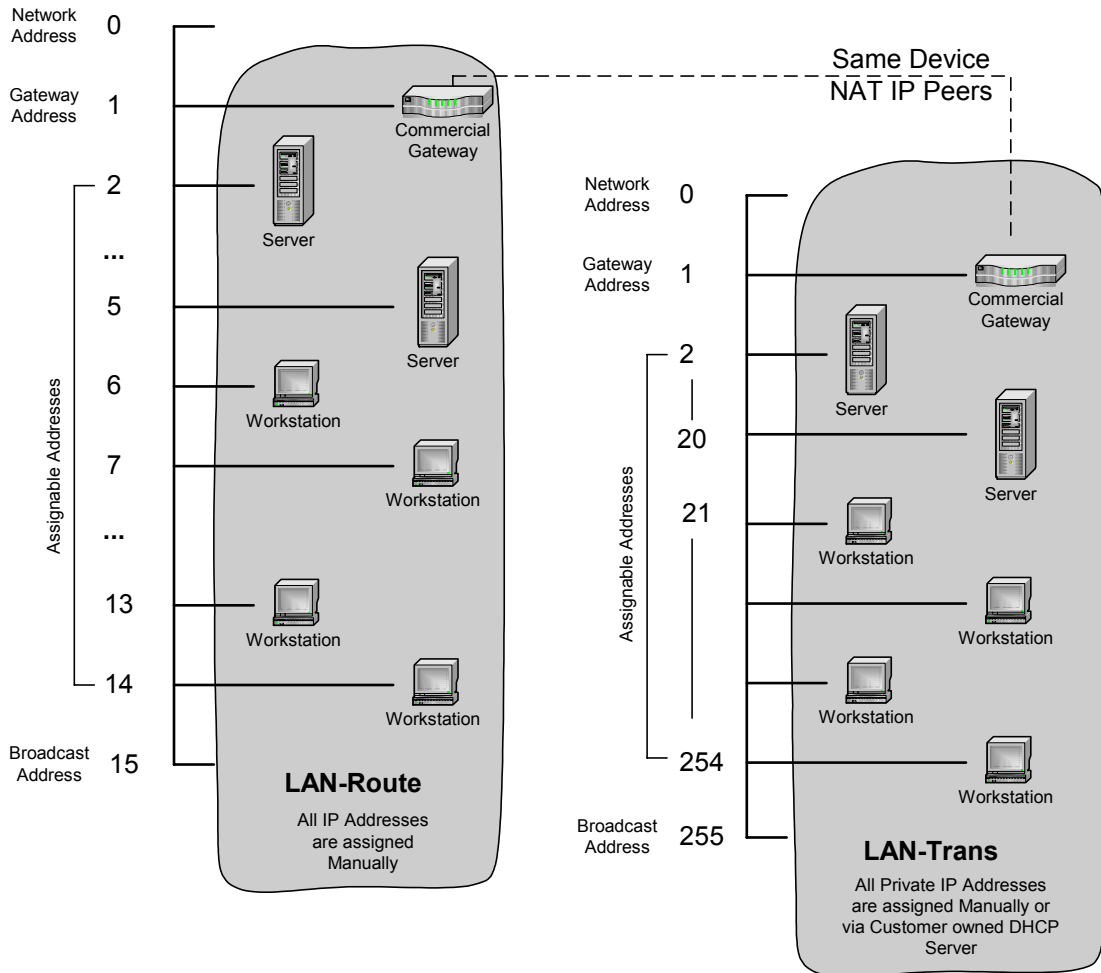


Figure 5-6 Static Addressing with C-NAPT Scenario

5.3.4 Static IP Addressing with C-NAPT and DHCP Service

The Commercial Gateway device is configured with two IP Networks, one public network and one private network. The public network is per Section 5.3.1. The Commercial Gateway device uses C-NAPT to route traffic to and from the private network CPE. The commercial customer is responsible for assigning IP addresses for the public network. The Commercial Gateway device provides the DHCP service that serves the Privately routable IP addresses to the CPE devices. The size of the dynamically assigned address pool is adjustable, where the remaining IP addresses are to be statically assigned. The statically assigned IP addresses are taken from the beginning of the network pool, the dynamic addresses make up the remainder. Refer to Figure 5-7.

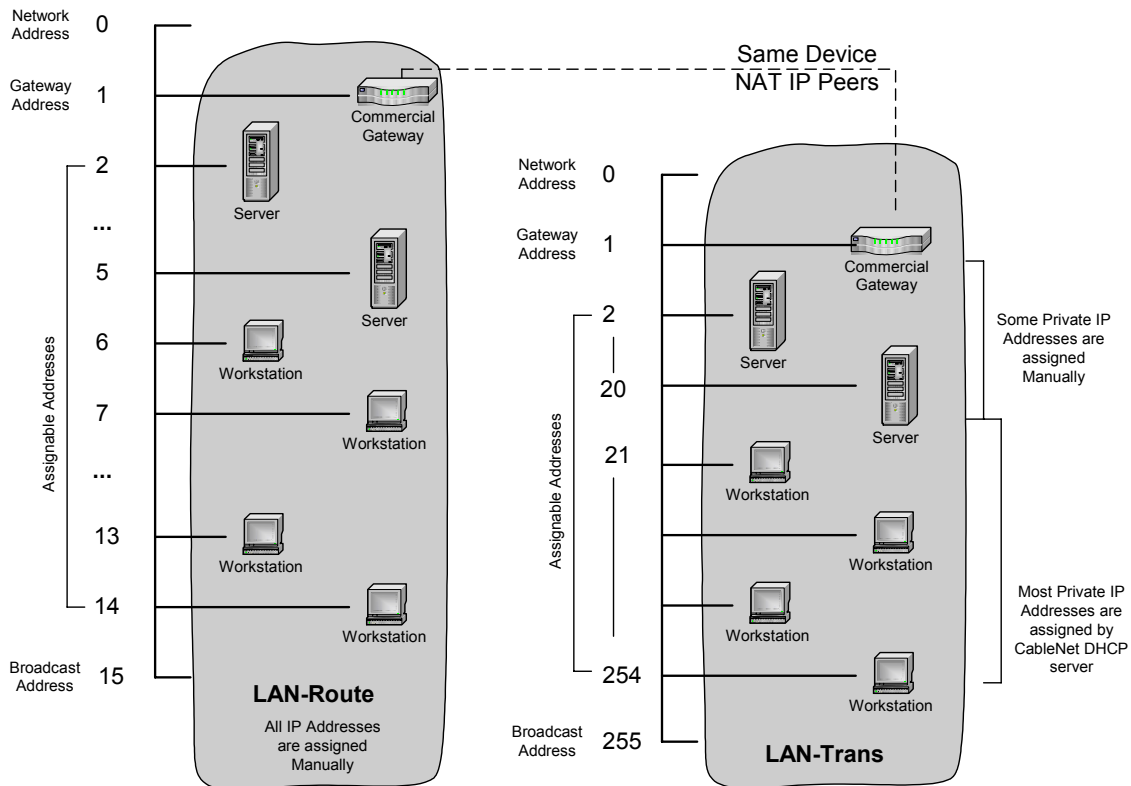


Figure 5-7 Static IP Addressing with C-NAPT and DHCP Service

6 MANAGEMENT TOOLS

6.1 Wireless LAN Port Control

For commercial gateway (CG) devices that have one or more wireless LAN interfaces, this section specifies requirements for a standard method to enable and disable the wireless LAN interface(s). CG devices are not required to have a wireless LAN interface, but if one is implemented, the PS element must adhere to the requirements specified in this section.

6.1.1 Goals and Design Guidelines

The goals and design guidelines for the wireless LAN port control functionality are:

- Provide a standard method to enable and disable the wireless LAN interface(s)
- Make use of the standard interface control mechanisms already defined by CableHome [CH1.0], [CH1.1]
- Provide a single control to enable/disable all wireless interfaces on the CG

6.1.2 System Description

As specified by CableHome, the IF-MIB [RFC 2863] must be implemented by a compliant CG device. The ifTable contains a row entry for each interface supported by the device and also a row entry that represents the aggregate of all LAN interfaces, per the CableHome specifications [CH1.0] and [CH1.1]. Through the ifAdminStatus columnar object, any interface on the PS, as identified by the ifIndex number, can be enabled and disabled, including any wireless interface.

While the mechanism exists to enable and disable a wireless interface, the ifIndex numbers of these interfaces are not specified. Therefore, they may vary from vendor to vendor. This is operationally problematic since it is likely that the ifIndex number for the wireless interface will differ between vendor products.

This specification extends upon CableHome to provide a standard method to enable and disable the wireless interface(s) on a CG device. Specifically, if a CG device has one or more wireless interfaces, it must support the following:

1. An additional row entry in the ifTable that represents the “*Aggregated Wireless LAN Interface*” interface. This enables a single control to enable and disable all wireless interfaces on a CG device. This row entry would be applicable even if the CG device only has a single wireless interface.
2. The ifIndex of the “*Aggregated Wireless LAN Interface*” interface must be 254. This enables the operator to enable/disable the wireless interface(s) using a common interface number across all CG devices, independent of the device manufacturer.

6.1.3 Requirements

If one or more wireless LAN interfaces exist, the PS MUST create an instance of ifEntry for the “*Aggregated Wireless LAN Interface*” interface, which is identified by the ifIndex value of 254 and ifDescr of “*Aggregated Wireless LAN Interface*”.

The PS MUST assign the value ‘other(1)’ to ifTable [RFC 2863] ifType entries corresponding to ifIndex 254.

The PS MUST set the ifTable ifPhyAddress value corresponding to ifIndex 254 to a zero-length octet string.

The PS MAY implement the ifTable counters for ifIndex value 254.

6.2 Commercial Services Annex MIB Requirements

In addition to the CableHome 1.0 [CH1.0] or CableHome 1.1 [CH1.1] MIB object requirements, the PS MUST implement each MIB object listed in Annex A. If the Persistent column for a MIB object listed in Annex A 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.

The additional required MIB objects for the Commercial Services Annex can be found in the following MIB documents:

- IP Forwarding Table MIB [RFC 2096]
- RIP Version 2 MIB Extension [RFC 1724]
- Commercial Services Annex MIB [CO1]

7 PROVISIONING TOOLS

7.1 DHCP Provisioning

The CSA DHCP provisioning functions extend those defined in the CableHome specifications [CH1.0] and [CH1.1]. The extensions accommodate the PS's enhanced router capabilities and the possible use of local DHCP servers that may exist in a commercial environment.

7.1.1 Goals and Design Guideline

The goals and design guidelines for CSA provisioning functionality are:

- Provide a method to indicate to an MSO's provisioning system that a PS has CSA capabilities.
- Provide a method to enable/disable the DHCP server in the PS.
- Support static and dynamic segmentation of a configured public or private IP address range.

7.1.2 CSA CDP System Description

The CSA CDP element builds on CableHome's CDP functionality. The CDP is a sub-element of the PS and contains the address functions to act as the DHCP server in the LAN and a DHCP client in the WAN. These addressing functions are supported by the CDS for DHCP server functions and the CDC for WAN client functions.

7.1.2.1 CSA CDS System Description

The CSA CDS functionality extends the CableHome CDS functions. Like CableHome, the CSA CDS is configured with one IP address range and uses this address range for dynamic address assignments. The CSA CDS extensions to the CableHome CDS are described in this section.

A PS may be configured with multiple routed IP ranges (see Section 8.2). Among these IP ranges, 0 or more are publicly routed IP addresses in LAN-Route address realm and 0 or 1 are translated IP addresses in the LAN-Trans address realm. The CDS can be configured to serve a portion or the whole of only one of these ranges. The term CDS Range refers to the routed address range that the CDS is configured with. The CDS range is delineated by the MIB objects `cabhCdpLanPoolStart` and `cabhCdpLanPoolEnd`. The routed address range that contains the CDS range is called the CDS Parent Range (see Figure 7-1).

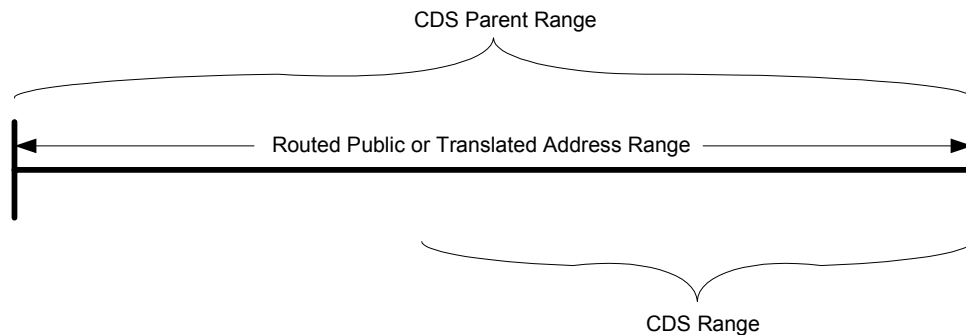


Figure 7-1 CDS Parent Range

When the CDS is activated to serve an address segment, the configured CDS range is the PS's dynamic address pool. If the CDS is not configured to serve addresses of the entire Parent Range, the remaining

addresses are considered the static pool, which the customer uses for static or manual address assignment. Static assignments are not reserved in the CDS, nor does the CDS record whether or not an address in the static pool is assigned.

When the CDS hands out an IP lease from the dynamic pool, DHCP Option 1 and 3 of the lease should be configured using the values from the cabhCdpServer mib. These values can be configured using the cabhCdpServerSubnetMask MIB object for DHCP option 1 and the cabhCdpServerRouter MIB object for DHCP option 3, respectively.²

A routed address range may be for a local or remote network (see Section 8.2). The CDS is not required to serve addresses to a remote network located behind another router on the LAN.

In a CSA deployment, the following 3 options regarding dynamic address assignment may be selected:

1. Use the CDS DHCP server;
2. Use a local DHCP server;
3. No dynamic address assignment.

It is expected that there is only one active DHCP server in the LAN. In other words, if a customer uses a local DHCP server on the commercial LAN, then the CDS should be disabled. CSA uses the MIB object cabhCdpCsaServerEnable to control whether the CDS is enabled or disabled.

When the CDS is disabled, it must not respond to DHCP client messages under any conditions. On the other hand, when the CDS is enabled, it must function as defined by the implemented CableHome specification, CableHome 1.0 [CH1.0] or CableHome 1.1 [CH1.1].

7.1.2.2 CSA CDS Requirements

If the MIB object cabhCdpCsaServerEnable is set to true (1), then the PS MUST enable its CDS functions and operate as defined by the version of CableHome specification, CableHome 1.0 [CH1.0], or CableHome 1.1 [CH1.1], implemented in the CG device.

If the MIB object cabhCdpCsaServerEnable is set to false (2), then the PS MUST disable its CDS functions and not respond to DHCP client messages.

The process of disabling or enabling of the CDS using the cabhCdpCsaServerEnable MIB object MUST NOT alter existing CDS configurations (i.e., the value of the cabhCdpServer MIB object).

7.1.2.3 CSA CDC System Description

The CSA CDC functionality extends the CableHome CDC functions. Like CableHome, the CSA CDC element is responsible for acquiring WAN addresses and provisioning mode selection. It also sends information regarding the capabilities of the PS to the WAN provisioning system via DHCP options.

A PS that is CSA compliant will use DHCP Option 60 to communicate its CSA capabilities by appending the string “:CSA1.0” to the CableHome DHCP Option 60 values.

7.1.2.4 CSA CDC Requirements

The CDC MUST append the string “:CSA1.0” to the base DHCP Option 60 value corresponding to the CableHome version that CSA is built on, as specified in Table 7-1.

² Modified per ECN CO-CSA-N-04.0134-2.

Table 7-1 CSA DHCP Option 60 Values

Base CableHome CableHome Version	CSA DHCP Option 60 Value
CableHome1.0	“CableHome1.0:CSA1.0”
CableHome1.1	“CableHome1.1:CSA1.0”

8 PACKET HANDLING AND ADDRESS TRANSLATION

8.1 Commercial Services Packet Handling Mode

Since CSA functions are an extension to CableHome functions, CG devices that are CSA compliant may also be used for residential applications, which only require the CableHome functionality. Therefore, a method to disable or enable the CSA requirements defined in this specification is needed. It is also important that when CSA functions are enabled that they integrate and operate smoothly with CableHome functionality.

8.1.1 Goals and Design Guidelines

The goals of the Commercial Services annex to the CableHome packet handling modes include:

- Ability to enable or disable CSA specific functions
- Ability to simultaneously support clients in the LAN-Route, LAN-Trans and LAN-Pass realms
- Ability to route packets between the WAN and the LAN side clients

8.1.2 System Description

The CableHome specification defines three primary packet handling modes of operation. Using the `cabhCapPrimaryMode` MIB object, the PS can be configured to Passthrough, NAPT, or NAT modes of operation.

To operate as a CSA Commercial Gateway, the `cabhCapPrimaryMode` object is extended with a new value to indicate the PS is operating in CSA Mode. CSA Mode is enabled when the `cabhCapPrimaryMode` object is set to a value of “`csa(10)`”. While operating in this mode, the PS will function as described by the CSA specification and simultaneously support clients in the LAN-Pass, LAN-Trans and LAN-Route realms. When not in the CSA Mode, the PS will perform as described in the CableHome specification.

CSA Mode is similar to the CableHome C-NAPT mode of operation with the additional ability to support devices in the LAN-Route realm. Traffic originating from and destined to devices in the LAN-Route domain should not be translated and should be routed according to the route entries in the `ipCidrRouteTable` MIB object (see Section 8.2) and as defined per [RFC 791].

Packets from or to LAN-Pass devices are bridged, at layer 2, through the Commercial Gateway as defined by the Mixed Bridging Mode functionality in the CableHome specification. Devices can be configured for the LAN-Pass realm by programming their MAC addresses in the `cabhCapPassthroughTable` MIB object.

The CableHome specification defines the CAP Mapping Table used to store information required to perform C-NAT and C-NAPT transparent routing functions. For devices in the LAN-Route realm, the CAP Mapping Table is not utilized.

In CSA Mode, the CableHome C-NAT packet handling mode is not supported and must be disabled. In this case, the `cabhCdpWanDataIpAddrCount` MIB object is expected to be set to a value of zero or one. If the `cabhCdpWanDataIpAddrCount` MIB object is set to a value greater than one, the PS will ignore it and not acquire more than one WAN-Data IP address.

In CSA Mode, the PS element (CDS) may be configured to provision addresses for devices only in the LAN-Route or the LAN-Trans realms. Broadcast DHCP messages originating from devices in the LAN-

Route or LAN-Trans realms must not be forwarded to the WAN. Additionally, broadcast DHCP messages originating from devices in the LAN-Pass realm should be bridged to the WAN.

The CableHome specification defines Multicast packet handling for clients in the LAN-Pass and the LAN-Trans domains. For clients in the LAN-Route realm, the PS will transparently bridge downstream IGMP messaging and downstream IP Multicast packets. For LAN-Route and LAN-Trans originated IGMP messaging and IP Multicast packets, the CG must route this traffic to the WAN unless the source IP address of the LAN device is not defined in the ipCidrRouteTable as specified in Section 8.2.

The Upstream Selective Forwarding Switch (USFS) as defined in the CableHome specification prevents traffic between LAN IP devices from traversing the HFC network. This functionality is also applicable to devices residing in the LAN-Route realm. In other words, traffic between devices in the LAN-Pass, LAN-Trans, and LAN-Route realms will be handled by the USFS function and should not be forwarded to the HFC network.

In order to populate the ipNetToMediaTable, the CableHome USFS functionality also requires that the PS learn all IP and MAC addresses with their associated physical interface in the LAN-Trans and LAN-Pass address realms. This functionality is also applicable to the LAN-Route realm. IP/Mac address learning can occur by a variety of methods and is left to vendor implementation

Below is a graphical example of a CG with attached client devices belonging to different LAN realms:

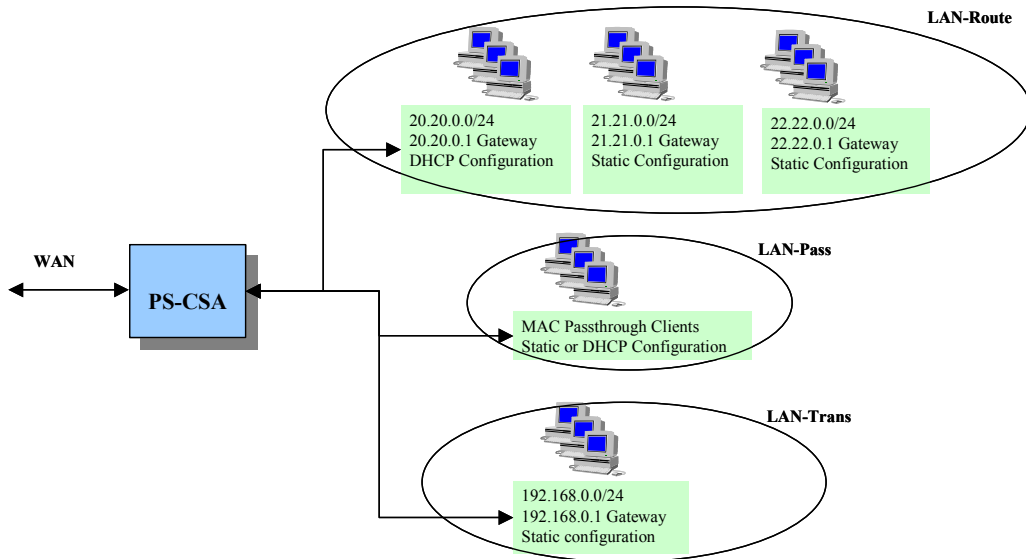


Figure 8-1 CG with Attached Client Devices from Different LAN Realms.

The following table shows how to setup each of the four CSA configuration examples as described in Section 5.3 of this document. For each example, the table illustrates all of the possible LAN CPE client configurations which are allowed:

Table 8-1 Possible LAN CPE Client Configurations

CSA Ex.	CH Primary Mode (cabhCapPrimaryMode)	CSA LAN Network (ipCidrRouteTable)	CDP Server (cabhCdpServerEnable)	Possible LAN-side Client Configurations
1	csa(10)	Public route is defined	False	1. Public routed subnet clients (Static) 2. MAC passthrough clients (Static and/or WAN-side DHCP)
2	csa(10)	Public route is defined	True	1. Public routed subnet clients (Static and CDS DHCP) 2. MAC passthrough clients (Static and/or WAN-side DHCP)
3	csa(10)	Public route is defined Private route is defined	False	1. Public routed subnet clients (Static) 2. Private IP clients (Static) 3. MAC passthrough clients (Static and/or WAN-side DHCP)
4	csa(10)	Public route is defined Private route is defined	True	1. Public routed subnet clients (Static) 2. Private IP clients (Static and/or CDS DHCP) 3. MAC passthrough clients (Static and/or WAN-side DHCP)

8.1.3 Requirements

In addition to the cabhCapPrimaryMode MIB object values defined by the CableHome specification, the PS MUST also support a value of “csa(10)”.

If the cabhCapPrimaryMode MIB object is set to a value of “csa(10)”, the PS MUST operate as defined by the CSA specification. If the cabhCapPrimaryMode MIB object is not set to a value of “csa(10)”, the PS MUST operate as defined by the CableHome specification.

The PS MUST disable CableHome C-NAT packet handling mode functionality.

The PS MUST support a network configuration with simultaneous existence of LAN clients in the LAN-Trans, LAN-Pass, and LAN-Route realms.

The PS MUST NOT forward DHCP messages from LAN-IP devices to the WAN unless their MAC address is in the cabhCapPassthroughTable MIB object.

If the cabhCdpWanDataIpAddrCount MIB object is set to a value greater than one, the PS MUST ignore it and not acquire more than one WAN-Data IP address. The PS will never return a value greater than one when the cabhCdpWanDataIpAddrCount MIB is queried.³

The PS MUST not forward LAN broadcast traffic to the WAN unless it originates from a LAN-IP device with its MAC address in the cabhCapPassthroughTable MIB object.

The PS MUST transparently bridge WAN-to-LAN IGMP messaging and IP Multicast packets.

³ Modified per ECN CO-CSA-N-04.0134-2.

In addition to devices in the LAN-Pass and LAN-Trans realms, the PS MUST learn all IP and MAC addresses with their associated physical interface in the LAN-Route realm.

Traffic between devices in the LAN-Pass, LAN-Trans, and LAN-Route realms MUST be handled by the USFS function and MUST NOT be forwarded to the HFC network.

8.2 Packet Routing

Routing packets between the WAN and the LAN is a key feature of the CSA specification. This section describes the required configuration and forwarding functions for routing packets.

8.2.1 Goals and Design Guidelines

The packet routing goals of the Commercial Services Annex include:

- Ability to remotely configure and view route information at the Commercial Gateway
- Ability to configure one or more LAN-Route public network range(s) that are allowed access to the WAN
- Ability to configure a single LAN-Trans private network that is allowed access to the WAN

8.2.2 System Description

The CSA Commercial Gateway will allow configuration of the following types of routes:

- A route for each public LAN IP address range assigned to the Commercial Gateway
- A route representing a single private LAN IP address range
- A route representing a remote LAN side network behind a router that is connected directly to the Commercial Gateway

8.2.2.1 Route Table MIB Objects

A routing table is used to configure network routing information in the PS. A route entry can describe a LAN-Route public network address or a LAN-Trans private network address. Either of these entries may be local or remote. A local network implies that the CG is directly connected to that network and a remote network corresponds to a network located behind a router. While the routing table can support multiple entries, the PS is only required to support at least three entries. This will enable a possible configuration of a LAN-Route, a LAN-Trans, and a default entry.

The ipCidrRouteTable MIB object, as defined in [RFC 2096], describes a method by which routes can be remotely managed at the CG. Each route is described by a set of objects within the ipCidrRouteEntry MIB object. Objects that are not relevant to the configuration of a route as described in this section can be ignored or set to their default values. The following set of MIB objects within the ipCidrRouteEntry MIB object are used to support CSA routing functions:

- The ipCidrRouteDest and ipCidrRouteMask correspond to the IP Network Address and IP Subnet Mask respectively.
- The ipCidrRouteNextHop object is the address of the next network upstream for a remote route. The CSA specification additionally requires that for a local route, the ipCidrRouteNextHop object represents the Gateway IP address for the route represented by the ipCidrRouteDest and ipCidrRouteMask objects.
- The ipCidrRouteIfIndex describes the interface used to reach the next hop. The PS only permits the configuration of ranges associated to the Aggregated LAN Interface and rejects the configuration of

routes associated to particular physical LAN interfaces. In other words, the PS will accept the configuration of LAN side route entries only if the corresponding `ipCidrRouteIfIndex` value is 255.

- The `ipCidrRouteType` is significant in the sense that it is used to indicate the type of the route being configured. There may be more than one LAN network address configured at the PS. Each route entry will describe a network that will be serviced by the PS:
 - A value of “local” indicates that the route is for a network that is directly connected to the interface defined by the `ipCidrRouteIfIndex` MIB object.
 - A value of “remote” indicates that the route is for a network this is located behind a router with an address defined by the `ipCidrRouteNextHop` MIB object.
 - A value of “other” indicates that the route is for a private network in the LAN-Trans realm that must have its traffic translated using the NAPT functions defined by the CableHome specification.
- The `ipCidrRouteProto` indicates the method by which a route is learned. This object is typically set to a value indicating “netmgmt” interface for the method used to configure the LAN side routes.
- The `ipCidrRouteMetric1` indicates the distance to the target in hops. This object should be set to a value of (1).
- The `ipCidrRouteStatus` corresponds to SNMP row-status object which allows for synchronous creation, modification or deletion of `ipCidrRouteEntry` rows within the `ipCidrRouteTable`.

The PS is required to use the route entries in the `ipCidrRouteTable` MIB object for forwarding packets between the WAN and the LAN-Trans and/or LAN-Route address realms. If the PS cannot first find a route entry for a given packet, it is required to use the default route entry for forwarding the packet. The PS creates the default route entry after the provisioning process is complete.

Routes in the `ipCidrRouteTable` are also used to restrict WAN access. Packets will not be forwarded to the WAN unless their source address is within the IP address range, defined by the `ipCidrRouteDest` and `ipCidrRouteMask` MIB objects of any LAN interface route entry (`ipCidrRouteIfIndex` = 255).

The following diagram shows a graphical example of a network with multiple route types. Table 8-2 shows how each of these routes is represented as an entry in the `ipCidrRouteTable`:

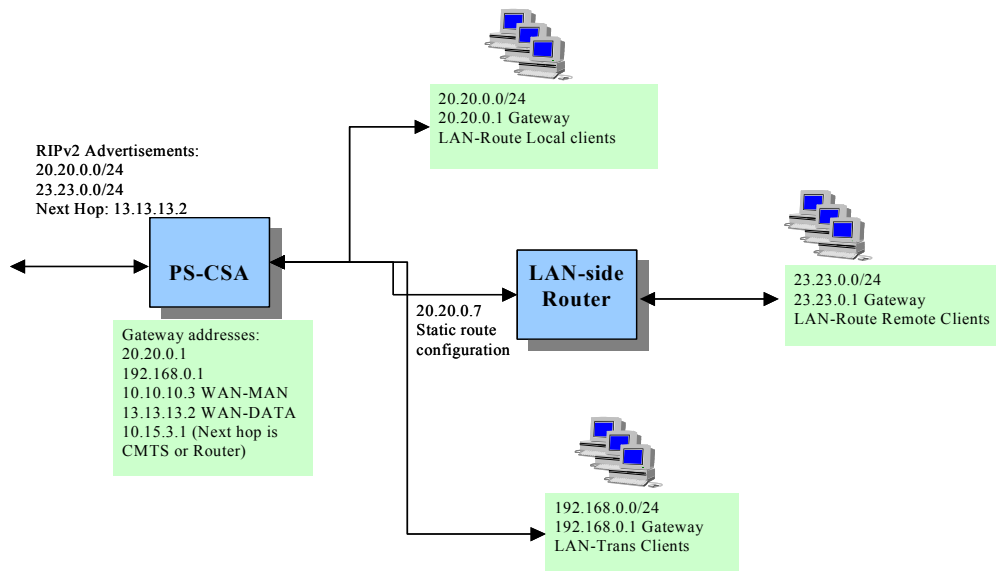


Figure 8-2 Network with Multiple Route Types

Table 8-2 Network Entries in ipCidrRoute Table

	LAN-Route Network	LAN-Trans Network	LAN-Route Remote Network	Default Entry
<i>ipCidrRouteTable</i>				
<i>ipCidrRouteEntry</i>				
ipCidrRouteDest	20.20.0.0	192.168.0.0	23.23.0.0	0.0.0.0
ipCidrRouteMask	255.255.255.0	255.255.255.0	255.255.255.0	0.0.0.0
ipCidrRouteTos	Not used (0)	Not used (0)	Not used (0)	Not used (0)
ipCidrRouteNextHop	20.20.0.1	192.168.0.1	20.20.0.7	10.15.3.1
ipCidrRouteIfIndex	255	255	255	1
ipCidrRouteType	local (3)	other (2)	remote (4)	remote(4)
ipCidrRouteProto	netmgmt (3)	netmgmt (3)	netmgmt (3)	other(1)
ipCidrRouteAge	Not used (0)	Not used (0)	Not used (0)	Not used (0)
ipCidrRouteInfo	Not used {0 0}	Not used {0 0}	Not used {0 0}	Not used (0)
ipCidrRouteNextHopAS	Not used (0)	Not used (0)	Not used (0)	Not used (0)
ipCidrRouteMetric1	1	1	1	1
ipCidrRouteMetric2-5	Not used (-1)	Not used (-1)	Not used (-1)	Not used (0)
ipCidrRouteStatus	row-status	row-status	row-status	row-status

8.2.3 Requirements

The PS MUST use the route entries in the ipCidrRouteTable MIB object and support the requirements defined in [RFC 791] for forwarding packets between the WAN and the LAN-Trans and/or LAN-Route address realms unless specified otherwise.

The PS MUST support at least three entries in the ipCidrRouteTable MIB object.

If a route entry in the ipCidrRouteTable MIB object has an ipCidrRouteIfIndex value of LAN(255) and an ipCidrRouteType value of local (3), then the PS MUST use the address in the ipCidrRouteNextHop MIB object as the gateway address for the address range defined in the ipCidrRouteDest and ipCidrRouteMask MIB objects.

The PS MUST only allow the ipCidrRouteIfIndex MIB object to be configured with the interface values of LAN(255), WAN-Man(1), or WAN-Data(2).

If a route entry in the ipCidrRouteTable MIB object has an ipCidrRouteType of other(1), then the PS MUST only perform network address port translation (NAPT), as defined by the CableHome specifications [CH1.0] and [CH1.1], on all outbound and inbound packets for those LAN IP Devices with an IP address within the address range defined in the ipCidrRouteDest and ipCidrRouteMask MIB objects.

The PS MUST only support one entry in the ipCidrRouteTable MIB object having a ipCidrRouteType of other(1).

The PS MUST first try to find a route entry in the ipCidrRouteTable MIB object for a given packet before applying the default route entry, which is indicated by a value of 0.0.0.0 in the ipCidrRouteDest and ipCidrRouteMask MIB objects.

After the PS has completed provisioning, the PS MUST create a default route entry in the ipCidrRouteTable with the following MIB object settings:

- IpCidrRouteDest = 0.0.0.0
- IpCidrRouteMask = 0.0.0.0
- IpCidrRouteNextHop = The value for this entry is dependent upon the WAN address mode. For WAN address mode 1, this value is the router address (typically the CMTS) returned in option 3 of the DHCP response for the WAN-Man IP address. For WAN address mode 2, this value is the router address (typically the CMTS) returned in option 3 of the DHCP response for the WAN-Data IP address. WAN address mode 0 is not supported since it is not possible to configure CableHome Passthrough mode when the PS is configured for CSA mode (see Section 8.1).
- IpCidrRouteIfIndex = The value for this entry is dependent upon the WAN address mode. For WAN address mode 1, this value is 1 which represents the WAN-Man Interface. For WAN address mode 2, this value is 2 which represents the WAN-Data Interface. WAN address mode 0 is not supported since it is not possible to configure CableHome Passthrough mode when the PS is configured for CSA mode (see Section 8.1).
- IpCidrRouteType = “remote”
- IpCidrRouteProto = “other”
- ipCidrRouteMetric1 = 1

The PS MUST NOT allow packets to be forwarded to the WAN unless their source IP address is within the address range defined by the ipCidrRouteDest and ipCidrRouteMask MIB objects of any LAN interface route entry in the ipCidrRouteTable MIB object with ipCidrRouteIfIndex = LAN(255).

8.3 Routing Protocol Functionality and Configuration

To support routing of packets between the WAN and the LAN, the next upstream router (typically the CMTS) in the MSO’s headend needs to be aware of the routing configuration of the PS. This information is communicated to the upstream router via a dynamic routing protocol. This section describes the routing protocol and its required functionality for supporting this requirement.

8.3.1 Goals and Design Guidelines

The goals and design guidelines for the CSA routing functionality are:

- Communicate the PS routing information to the next router upstream (typically the CMTS).
- Authenticate the PS routing information using secret keys shared between the PS and the next router upstream.

8.3.2 System Description

CSA routing protocol functionality is described in two sections, Routing Protocol and Routing Protocol Configuration. The Routing Protocol section describes the communication of routing information performed between the PS and the next router upstream. This communication is necessary to allow senders in the WAN to reach the PS LAN Routed domain. The PS Routing Protocol Configuration section describes the configuration of the routing protocol at the PS, which is done through specific MIB objects.

8.3.2.1 Routing Protocol

The PS acts as a router to a group of hosts or servers sitting behind it, which are assigned one range or several ranges of public IP addresses (see Section 8.1). In order to make these ranges accessible from the WAN the PS must communicate them, together with a PS public gateway IP address, to the next router upstream. This next router upstream is typically the CMTS. **NOTE:** In this section the terms ‘next router

upstream' and CMTS will be used indistinctly, but must be understood as the next router upstream. The purpose of this section is to describe the implementation at the PS of a routing protocol.

The PS communicates its routing information upstream through RIPv2 following [RFC 2453]. In addition, the PS should also be able to communicate its routing information through OSPFv2 as defined in [RFC 2328].

The routing information communicated upstream through RIPv2 consists of the ipCidrRouteTable [RFC 2096] routes to the LAN-Route domain, which are identified by the ipCidrRouteType values of 'remote' or 'local' and a ipCidrRouteIfIndex value of 255. Entries with an ipCidrRouteType value of 'other', on the other hand, point to the LAN-Trans domain and thus are not communicated upstream. LAN-Route entries in the ipCidrRouteTable are typically loaded through the configuration file during initialization or through an SNMP operation.

8.3.2.1.1 Authentication of RIP Messages

The PS is required to support two of the three RIP authentication modes currently defined by [RFC 2453] and [RFC 2082]: no authentication and md5 authentication. Support of authentication through password is optional.

The PS implements md5 authentication following [RFC 2082]. **NOTE:** The PS, however, does not follow the key management mechanisms hinted by the RFC. To perform md5 authentication the PS possesses a secret key which is shared with the next router upstream. With this type of authentication the CMTS can preserve the integrity of its routing table by accepting messages that originate from trusted sources only, that is, sources that share the same secret key the CMTS has. The key is downloaded at the PS through the configuration file or an SNMP SET operation and, if desired, the download can be secured through mechanisms defined in CableHome 1.0 or 1.1, such as encrypted SNMPv3 or encrypted configuration file download. The mechanism to load the key at the CMTS or next router upstream is outside the scope of this Annex.

The PS must support at least one key at any given time, while it is assumed that the CMTS can support more than one key at any given time. For operations in RIPv2 multi key environments, the sender identifies to the receiver the key it uses through the RIPv2 Key ID field defined by [RFC 2082]. The CMTS uses the Key ID value to select the right key to authenticate the received message with. The configuration of key ID values at the CMTS is outside the scope of this specification. As with configuration of keys, the configuration of key IDs at the PS is performed through the configuration file or an SNMP SET operation. The specification of key lifetimes, and ways to configure them, are not required by this specification.

NOTE: This is an exception to [RFC 2082].

8.3.2.1.2 Routes Information

As mentioned earlier, there is a direct relationship between the routes information communicated upstream through RIPv2 and the routes information available at the ipCidrRouteTable for local and remote types. The fields used for route information defined in the RIPv2 message format are the destination IP address, the subnet mask, the metric and the next hop fields. The first three fields relate one to one to the ipCidrRouteTable's ipCidrRouteDest, ipCidrRouteMask and ipCidrRouteMetric1 objects, respectively. For the routes it must advertise, the PS communicates to the next router upstream these ipCidrRouteTables object values through RIPv2 using the corresponding RIPv2 message fields. The value of the next hop field is always the PS' WAN-Data IP address. **NOTE:** When the CDC is in WAN Address Mode 1, the WAN-Data and WAN-Man interfaces share a single, common IP address. In WAN Address Mode 2, the WAN-Data and WAN-Man have separate, different IP addresses.

8.3.2.2 Routing Protocol Configuration

The PS implements the RIP Interface Configuration Table of [RFC 1724]. This table is used for the configuration of the RIPv2 protocol at the PS. The PS also implements the cabhPSDevCsaRip2IfConfExtTable MIB object, which is defined as an extension to the RIP Interface Configuration Table and allows the configuration of the keys' corresponding key ID values.

According to [RFC 1724] the configuration of RIP is done per interface. The RIP Interface Configuration Table allows interfaces to be identified, through the rip2IfConfAddress object, by either the interfaces' IP address or the interfaces' ifIndex value. In the case of the PS, however, interfaces within the context of the rip2IfConfAddress object are viewed as unnumbered, and thus are identified by their ifIndex value only. More specifically, the WAN interface is identified in the RIP Interface Configuration table by an ifIndex value of 1 (one), which translates, according to [RFC 1724], to the rip2IfConfAddress value 0.0.0.1.

The RIP options that can be configured per interface are the following:

- The type of authentication that will be applied for RIP, through the rip2IfConfAuthType. The alternatives that the PS must support are no authentication (default mode) and md5 authentication. Optionally the PS can support simple password authentication as well. The operator that wishes the most secure authentication mechanism will select md5 (3).
- The key for md5 or the password for password authentication through the rip2IfConfAuthKey object.
- The type of RIP messages that the interface must send or if no messages must be sent at all, through the rip2IfConfSend object. On the WAN side the PS must accept configuration to not to send messages (default configuration) or to send RIPv2 messages, and is not required to support sending RIPv1, ripV1Demand and ripV2Demand messages.
- The type of RIP messages that the interface is expected to receive, through the rip2IfConfReceive object. On the WAN interface the PS will support configurations to not to receive any RIP message on the interface (default configuration), or to receive RIPv2 messages. Receiving RIPv1 only or RIPv1 in combination with RIPv2 messages is not required by this specification. The operator will typically disable the reception of RIPv2 messages on the WAN interface.
- A metric (cost) value for the default route advertised in route updates, through the rip2IfConfDefaultMetric object. The default value of the object is 0 (zero). The PS MUST not communicate the default route entry in the ipCidrRouteTable via RIP messaging to the WAN.⁴
- The source IP address that will be used for RIP messages sent on the interface, through the rip2IfConfSrcAddress object. The PS ignores this object and always uses the WAN-Man IP address as the source IP address of all RIP messages sent from the WAN Interface. This address is also the default value of the object.
- The key ID value, through the cabhPSDevCsaRip2IfConfExtTable MIB object table, of the key that the PS uses to create the keyed message digest of outgoing RIPv2 messages.

8.3.3 Routing Protocol Requirements

The PS MUST implement RIPv2 as defined in [RFC 2453] for communicating routing information to the upstream router (typically the CMTS).

The PS MUST implement the rip2IfConfTable as defined in [RFC 1724], unless specified otherwise.

The PS MUST use RIPv2 to advertise only the routes of the LAN-Route domain, defined as any entry in the ipCidrRouteTable with a ipCidrRouteType MIB object value equal to 'remote' or 'local' and an IpCidrRouteIfIndex value equal to 255, to the upstream router (typically the CMTS).

⁴ Modified per ECN CO-CSA-N-04.0134-2.

The PS MUST declare its WAN Data IP address as the next hop value for all routes advertised on the WAN side.

For each route in the ipCidrRouteTable to be advertised through RIPv2, the PS MUST communicate the ipCidrRouteDest, ipCidrRouteMask and ipCidrRouteMetric1 objects' values in the RIPv2 message fields IP Address, Subnet Mask and Metric, respectively.

The PS MUST support the authentication modes of no authentication and MD5 authentication. The PS MUST determine whether to use the first or second mode as directed by the rip2IfConfAuthType object values noauthentication (1) and md5 (3) respectively. The PS MAY support simple password authentication.

The PS MUST be able to perform MD5 authentication of RIP messages as defined in [RFC 2082]. For MD5 authentication the PS MUST use the key defined for the interface by the rip2IfConfAuthKey MIB object and its corresponding key ID value defined by the cabhPSDevCsaRip2IfConfAuthKeyId MIB object for the RIPv2 Key ID field as defined in [RFC 2082].

The PS MUST only support configuration of RIP messaging on the WAN-Man interface defined by entries in the rip2IfConfAddressTable having a rip2IfConfAddress MIB object value of 0.0.0.1.

The PS MUST only support a rip2IfConfDefaultMetric MIB object value of 0 (zero) for entries in the rip2IfConfAddressTable.

For the WAN interface the PS MUST disable or enable the transmission of RIPv2 messages as directed by the rip2IfConfSend values doNotSend (1) and ripVersion2 (4) respectively. The support of the rip2IfConfSend options RIPv1 (2), rip1Compatible (3), ripV1Demand (5) and ripV2Demand (6) is not required by this specification. The PS MUST NOT send any RIP messages to the LAN interface.

For the WAN interface the PS MUST disable the reception of RIP messages and enable the reception of RIPv2 messages as directed by the rip2IfConfReceive values doNotReceive (4) and rip2 (2) respectively. The support of the object's options rip1 (1) and rip1OrRip2 (3) is not required by this specification. The PS MUST NOT accept any RIP messages from the LAN interface.

The PS MUST ignore the values set in the rip2IfConfSrcAddress MIB object. The PS MUST use its WAN-Man IP address as the source IP address of all RIPv2 messages sent on the WAN interface.

9 GENERAL REQUIREMENTS

In addition to the requirements in this Commercial Services Annex 1.0 specification, the PS MUST implement the requirements of either the CableHome 1.0 specification or the CableHome 1.1 specification, unless stated otherwise.

The PS MUST apply the firewall requirements as defined by the version of CableHome specification implemented in the CG device to all packets attempting to pass between the LAN and WAN, including packets sourced or destined to LAN IP Devices in the LAN-Route address realm.

Annex A MIB Objects (Normative)

This annex lists the MIB objects required by the Commercial Service Annex (CSA), as indicated by Section 6.2, that are in addition to the MIB objects required by either the CableHome 1.0 or 1.1 specifications. Implementations of the CSA MIB objects **MUST** be done in concert with either the CableHome1.0 or CableHome1.1 MIB requirements. This annex also identifies the persistence requirement for each listed object.

The term ‘persistent’ as it applies to this annex 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 applies:

- 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
ipCidr [RFC 2096]			
ipCidrRouteTable/ipCidrRouteEntry			
ipCidrRouteDest	read-only	No	N/A
ipCidrRouteMask	read-only	No	N/A
ipCidrRouteTos	read-only	No	N/A
ipCidrRouteNextHop	read-only	No	N/A
ipCidrRouteIfIndex	read-create	No	N/A
ipCidrRouteType	read-create	No	N/A
ipCidrRouteProto	read-only	-	N/A
ipCidrRouteAge	read-only	No	N/A
ipCidrRouteInfo	read-create	-	N/A
ipCidrRouteNextHopAS	read-create	No	N/A
ipCidrRouteMetric1	read-create	No	N/A
ipCidrRouteMetric2	read-create	No	N/A
ipCidrRouteMetric3	read-create	No	N/A
ipCidrRouteMetric4	read-create	No	N/A
ipCidrRouteMetric5	read-create	No	N/A
ipCidrRouteStatus	read-create	No	N/A

rip [RFC 1724]

rip2IfConfTable/rip2IfConfEntry			
rip2IfConfAddress	read-only	No	N/A
rip2IfConfDomain	read-create	No	N/A
rip2IfConfAuthType	read-create	No	N/A
rip2IfConfAuthKey	read-create	No	N/A
rip2IfConfSend	read-create	No	N/A
rip2IfConfReceive	read-create	No	N/A
rip2IfConfDefaultMetric	read-create	No	N/A
rip2IfConfStatus	read-create	No	N/A
rip2IfConfSrcAddress	read-create	No	N/A

MIB NAME/Parameter Entries	Max-Access	Persistent	# of Persistent
---------------------------------------	-------------------	-------------------	------------------------

cabhPsDevCsaRipExtension

cabhPSDevCsaRip2IfConfExtTable/cabhPSDevCsaRip2IfConfExtEntry			
cabhPSDevCsaRip2IfConfAuthKeyId	read-create	No	N/A

cabhCdpCsa

cabhCdpCsaServerEnable	read-write	No	N/A
------------------------	------------	----	-----

Appendix I Layer 2 Tunneling Functionality (Informative)

Layer 2 Tunneling Protocol version 3 (L2TPv3) functionality has been identified as a desired, but not mandatory, feature for products implementing the CSA specification. This protocol allows a pair of routers connected via an IP network to provide transparent Layer 2 connectivity between a pair of interfaces. Supported Layer 2 technologies include Ethernet, Frame Relay, and ATM. This enables networks located at different sites to appear as if they are connected directly together at a single site. Layer 2 network services, such as provisioning, management tools, intranet, and file sharing, at one site could be used for both.

Implementing L2TPv3 functionality in the CSA gateway will allow MSOs to use their existing IP/DOCSIS infrastructure to offer Layer 2 tunneling services to business customers without having to build a Layer 2 core infrastructure. General Internet access can also be offered using the same CSA gateway avoiding the need for different connections for multiple services, such as a connection for Internet access and discrete private lines for intranet access – a common enterprise problem.

The following figure illustrates an example of how MSOs intend to use L2TPv3 functionality in CSA devices.

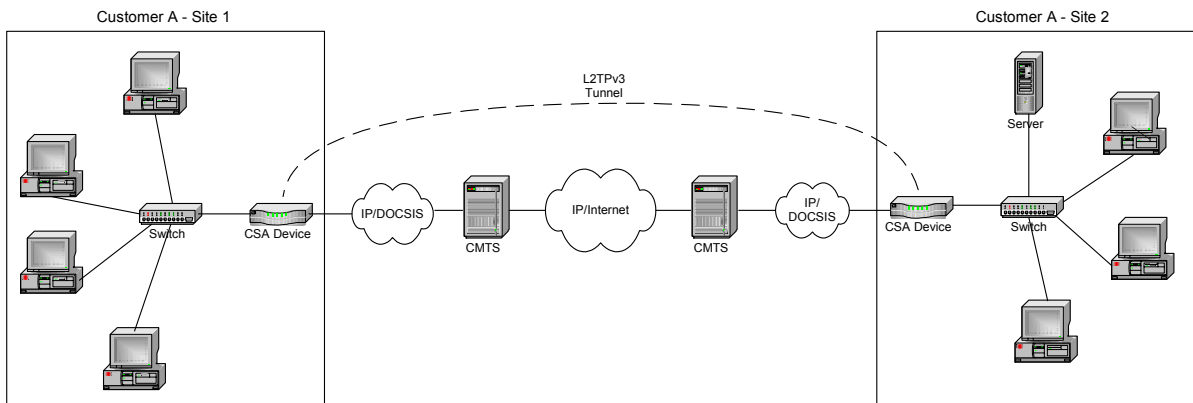


Figure I-1 Use of L2TP-v3 Functionality in CSA

Appendix II Acknowledgements

This specification was developed and influenced by numerous individuals representing many different organizations. CableLabs hereby wishes to thank everybody who participated directly or indirectly in this effort. In particular, CableLabs wishes to recognize the following individuals for their significant involvement and contributions to this specification.

Ray Farhat----- Broadcom
Jim Hinsey ----- Broadcom
Amol Bhagwat----- CableLabs
Ralph Brown----- CableLabs
Stuart Hoggan ----- CableLabs
Kevin Luehrs ----- CableLabs
Steve Saunders ----- CableLabs
Shengyou Zeng----- Cisco
Donald Mah----- Linksys
Greg Nakanishi----- Motorola
Diego Mazzola ----- Texas Instruments
John Bevilacqua ----- YAS Broadband Ventures

Appendix III Revision History

The following Engineering Change Notices were incorporated into CH-SP-CO-CSA-I02-040806:

ECN Number	ECN Date	Summary
CO-CSA-N-04.0134-2	4/22/04	Miscellaneous corrections and clarifications