casa systems

Course 1010 – CMTS Implementation, Operation & Troubleshooting

Document Revision 7.2.4

September 2017

The information regarding the product in this manual is subject to change without notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express of implied. Users must take full responsibility for their application of the product.

In no event shall Casa or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Casa or its suppliers have been advised of the possibility of such damages.

Table of Contents

1. Course Introduction and Overview

1.1. Course Description

This online self-paced course will give each participant an opportunity to learn Casa Cable Modem Termination System(CMTS) C100 and C40G hardware and software. The course is designed with an emphasis on verifying configurations as opposed to actual configurations. We take this approach because most of our audience are personnel who are not typically changing configurations but rather verifying proper configurations and troubleshooting. We employ interactive use cases for specific CLI syntax and troubleshooting flow charts for each topic. That said, there are some configuration examples and demonstrations for some sections. For those that would benefit from configuration training, we have hands-on labs that can be attended for our CCAP/EdgeQAM and WLAN Gateways products. Please visit our FAQ section for more information on our other courses.

1.2. Audience

Technical professionals, including system engineers, technical support personnel, channel partners, and resellers, who need to understand how to verify and troubleshoot the Casa CMTS implementations and operations.

1.3. Objectives

Chapter 1 Hardware IOT

Given the written guide at the end of this chapter the Course 1 participant should be able to:

- Describe broadband network architectures and the role of the Cable Modem Termination System(CMTS)
- List Chassis components of the C40 and C100G.
- Describe Power connections and options.
- Describe Hardware redundancy components and configurations.
- List the hardware RF and IP service modules and their functions.
- Discuss the downstream and upstream capacities of RF service modules.
- Describe RF and IP service module architecture’s.
- Describe proper replacement and maintenance of the chassis and service modules
- Describe a visual inspection troubleshooting flow.

Chapter 2 Software IOT

Given the written guide at the end of this chapter the Course 1 participant should be able to:

- Describe the data plane and management plane traffic flow in the CMTS Network side and RF side interfaces.
- Articulate the features and modalities of the Casa Command Line Interface(CLI).
- Describe software image and configuration file management.
- List software update procedures.
- Verify High Availability configurations and operations.
- Articulate how to troubleshooting cable modem initialization

Chapter 3 Verifying Configurations and Troubleshooting

Given the written guide at the end of this chapter the Course 1 participant should be able to:

- Describe Best practices and troubleshooting approaches.
- Articulate hardware troubleshooting methods.
- Describe RFI and NSI troubleshooting tools.
- Verify and troubleshoot RFI PHY layer configurations.
- Verify and troubleshoot RFI MAC layer configurations.
- Verify and troubleshoot NSI configurations.
- Verify OSSI configurations
- Verify and troubleshooting routing protocols configurations

Chapter 4 Example Configuration Demonstrations.

This chapter includes demonstration on how to configure:

- RFI Configurations
- MAC domain Configurations
- CM IP Operations Configurations.
- OSSI Configurations.
- Layer 2 configurations.
- BPI configurations.
- Routing Configurations.

1.4. Casa Learning Management System

ON your home page in the Learning Management System(LMS) there are several learning management available these are:

1.4.1. Student Guide

This course comes with a student guide, each participant should download this guide to his or her desktop. The PDF document if downloaded locally allows you to always have access to the content and you can make notes or highlights.

1.4.2. Video presentations

This reference guide will have built in links to take the student directly to the LMS video demonstrations for the subject they wish to review. Most sections written content will have the following graphic to play these video presentations

Click here for a video presentation on this topic.

1.4.3. Feedback Form

The feedback from in the course will allow you to provide feedback to Casa Systems Learning Solutions to help us incorporate your feedback into current and future courses.

1.4.4. Knowledge Check

The knowledge check will contain questions directly taken from the student guide and video presentations. There is no minimum grade it is a tool to help you gauge your comprehension of the material.

1.4.5. Certificate of completion

If you have completed the feedback from and received a grade on the Knowledge Check a certificate of completion will be issued and made available for download on your home page.

1.4.6. Navigating the Learning Management System

Click the graphic below for a video presentation on how to navigate and access learning resources from your home and course pages.

Click here for a video presentation on this topic.

1.5. Product Information and Overview

The Casa CMTS provides both a network side interface (NSI) and a radio frequency interface (RFI). On the NSI, the CMTS provides Ethernet 10/100 Mbps (for system management), GigE, and 10GigE (C10G) interfaces to routing gateways and servers.

The CM connects to the operator's HFC network and to a home network, bridging packets between them. Many CPE devices can connect to the CM's LAN interfaces, can be embedded with the CM in a single device, or they can be separate standalone devices (as shown in Figure 1–1). CPE devices may use IPv4, IPv6 or both forms of IP addressing. Examples of typical CPE devices are home routers, set-top devices, personal computers, etc.

The CMTS connects the operator's back office and core network with the HFC network. Its main function is to forward packets between these two domains, and optionally forward packets between upstream and downstream channels on the HFC network. The CMTS performs this forwarding with any combination of link-layer (bridging) and network-layer (routing) semantics.

Various applications are used to provide back office configuration and other support to the devices on the DOCSIS network. These applications use IPv4 and/or IPv6 as appropriate to the particular operator's deployment. The applications include:

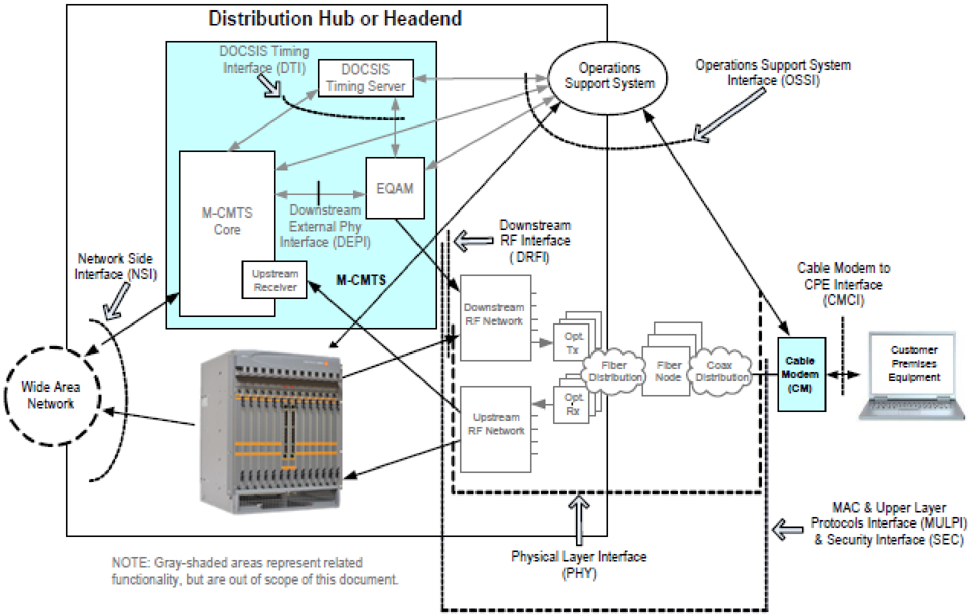
Provisioning Systems:

- The DHCP servers provide the CM with initial configuration information, including the device IP address(es), when the CM boots.
- The Configuration File server is used to download configuration files to CMs when they boot. Configuration files are in binary format and permit the configuration of the CM's parameters.
- The Software Download server is used to download software upgrades to the CM.
- The Time Protocol server provides Time Protocol clients, typically CMs, with the current time of day.
- Certificate Revocation server provides certificate status.

Network Management System (NMS):

- The SNMP Manager allows the operator to configure and monitor SNMP Agents, typically the CM and the CMTS.
- The syslog server collects messages pertaining to the operation of devices.
- The IPDR Collector server allows the operator to collect bulk statistics in an efficient manner.

1.5.1. Reference Architecture


Distribution Hub or Headend
DOCSIS Timing Interface (DTI)
DOCSIS Timing Server
Operations Support System
Operations Support System Interface (OSSI)
M-CMTS Core
EQAM
Downstream External Phy Interface (DEPI)
Upstream Receiver
M-CMTS
Downstream RF Interface (DRFI)
Network Side Interface (NSI)
Wide Area Network
Downstream RF Network
Upstream RF Network
Opt. Tx
Opt. Rx
Fiber Distribution
Fiber Node
Coax Distribution
Cable Modem to CPE Interface (CMCI)
Cable Modem (CM)
Customer Premises Equipment
MAC & Upper Layer Protocols Interface (MULPI) & Security Interface (SEC)
Physical Layer Interface (PHY)

NOTE: Gray-shaded areas represent related functionality, but are out of scope of this document.

The reference architecture for data-over-cable services and interfaces is shown in the figure above. The table below identifies the DOCSIS 3.1 series of specifications pertaining to this architecture.

Designation	Title
CM-SP-PHYv3.1	Physical Layer Specification
CM-SP-MULPIv3.1	Media Access Control (MAC) and Upper Layer Protocols Interface Specification
CM-SP-CM-OSSIv3.1	Cable Modem Operations Support System Interface-Specification
CM-SP-CCAP-OSSIv3.1	CCAP Operations Support System Interface-Specification
CM-SP-SECv3.1	Security Specification
CM-SP-CMCIv3.0	Cable Modem CPE Interface Specification

1.6. Broadband Network Architectures

In this section we will describe the current and evolving broadband network architectures.

1.6.1. Network Evolution Vision

The evolving nature of broadband networks can be summarized in three major inflection points:

- Converge and Upgrade, that is to say, consolidate voice and video with converged cable access platforms, and upgrade these CCAPs to DOCSIS 3.1, in order to make full use of spectrum and boost speeds up to 10 gigabits per second.
- Distribute and Densify, meaning to distribute access deeper into the network and densify deployments.
- Finally, Virtualize, that is, to adopt virtual versions of network functions to enable new service creation, faster provisioning of services and greater operational agility.

1.6.2. Broadband Architectures Overview

In the next few slides, we will describe specific broadband architectures and where they fit in todays networks.

Multiple System Operators (MSOs), i.e. cable companies, typically deploy an access network that is composed of coaxial and optical cables, or a Hybrid Fiber Coaxial, (HFC) network. This network is arranged in a tree and branch architecture with a Fiber node at the root and branches composed of RF analog electronics, such as RF amplifiers, diplex filters, and coaxial cable. This network delivers voice, video and data services to the customer premise equipment (CPEs). The key functional characteristics of this access network are:

- An Integrated Cable Modem Termination System (ICMTS) in the operator's head end or hub site and a Cable Modem (CM) in the customer premise. Note, the Casa CMTS is also a CCAP, or Converged Cable Access Platform. This means the normally separate edge QAM device is collapsed into the CCAP platform, to integrate both data and video services.
- The access network employs separate downstream and upstream transmission paths. Downstream traffic comes from the operator's network to the CMTS. The CMTS then conditions and sends the data to the CM, and the modem switches the traffic to the CPEs. The upstream traffic comes from the CPE and is switched by the modem to the HFC network, to the CMTS and then to the operator's network.
- The downstream is characterized by digitally modulating analog carriers using Frequency Division Multiple Access (FDMA) techniques.
- The upstream is characterized by digitally modulating analog carriers using both Time Division Multiple Access (TDMA) and FDMA techniques.
- For both the downstream and upstream, DOCSIS 3.0 or 3.1 are the MAC and Data Link layer protocol between the CMTS/CCAP and the cable modem.

On the network side interface of the ICCAP, the operators aggregation and core networks can comprise different network designs, depending on the size of the MSO. But most MSOs have some variation of the network described here.

The key functional characteristics of the aggregation layer typically include a Municipal Area Network or Metro Ethernet, with optical transport. Ethernet on the MAN can be used as native Ethernet, Ethernet over SDH, Ethernet over Multiprotocol Label Switching (MPLS) or Ethernet over DWDM.

The core of the network provides connectivity to networks and services such as the public switched telephone network, the Internet, content delivery networks, and fixed services such as IMS,AAA and OSS. Finally, MSOs will have a Master head end or a few master head ends, to collect and distribute satellite video services throughout the national or regional serving area.

1.6.3. Remote PHY

The reference architecture of the Data Over Cable Interface Specifications, DOCSIS, has remained constant across versions 1.0, 1.1 and 2.0. With the introduction of version 3.X, that reference architecture has changed. The integrated CCAP is still widely deployed; however, an emerging technology is garnering much interest in cable broadband deployments: Remote PHY. The essential architectural changes are:

1. Replacing the ICCAP with a software CCAP that implements the DOCSIS MAC layer, which can be run on a generic hardware platform, providing obvious benefits.
2. Moving the PHY layer out of the ICCAP into the remote node. This architecture pushes the fiber deeper into the access network and minimizes the RF analog components of the network, which can be the source of many network errors. This architecture change is also known as deep fiber deployments.

Please refer to course 9 on the Casa Learning Portal for more detail on Casa Systems Remote PHY solution.

1.6.4. Passive Optical Networking

Until now, the architectures we have discussed have largely addressed the low gigabit residential and SOHO needs of MSOs, less than 1 gigabit per second, very well. But in order to provide mid-size and large business bandwidth requirements, 1 gigabit per second or greater, the MSOs will need to leverage different network architectures.

Another broadband network architecture of interest to Cable ISPs is Passive Optical Networking, or PON. The fundamental components of a PON include the Optical Line Terminal (OLT), which usually resides in the operator’s head end or hub site and usually serves more than one PON. The PON contains a trunk fiber feeding an optical power splitter, or often a tree of splitters. Splitters are available in a variety of split ratios, including 1 to 8, 1 to 16, and 1 to 32. From the splitter, a separate drop fiber goes to each subscriber, where it terminates on an Optical Network Unit (ONU) As we see from the figure, the OLT is designed for controlling more than one PON. (In this example it serves four independent networks.) We can see that if every PON has 32 connections, the OLT can distribute data to 128 ONUs. There are obvious advantages to this architecture, in that the fiber is moving deeper and deeper into the access network: in this case, Fiber to the home or FTTH. A single-fiber connection is used for both directions, through specification of separate wavelengths for each direction. This wavelength separation also allows for coexistence of other technologies on the same optical distribution network. For example , downstream and upstream voice and data can be delivered on 1490, and 1310 nm respectively, while broadcast video can be carried on 1550 nm.

Typically, MSOs have approached providing business customers who need higher gigabit symmetrical services than DOCSIS systems can support, with point to point, course wave division multiplexing technology. This technology uses one dark fiber strand or CWDM wavelength per subscriber. While CWDM is suitable for connections of 1 gigabit per second or more, it is a more costly solution than PON for speeds below this level. This solution results in deploying both technologies in the access network to meet all customer requirements.

1.6.5. MSO Broadband Network Evolution

Today, MSO networks have evolved to include separate siloed networks and are comprised of traditional and emerging technologies to include:

- HFC for residential and small business internet and video services with emerging deep fiber, leveraging remote PHY and PON for greenfield deployments and high capacity business services, as well as carrier Ethernet business services and wireless including Wi-Fi backhaul.
- In addition, in an effort to leverage current DOCSIS provisioning and back office services , MSOs are seeking to apply their DOCSIS systems to fiber-based services for business customers. MSOs are moving to adopt and capitalize on the standards-based, scalable ,and cost effective aspects of EPON technology. The use of DPoE or DOCSIS Provisioning of EPON, allows them to integrate EPON into their existing provisioning and operations support systems.

Casa Systems enables all of these architectures, with our high density 8x192 DOCSIS 3.1 downstream modules and our 16x8 upstream modules, our Distributed Access Architecture, CSC module and our DAA series remote phy nodes, as well as our Passive Optical Networking module and our Optical Network Units.

1.6.6. MSO Broadband Network Virtualization

Looking into the future, the broadband network architecture will begin to evolve into an all fiber network, based on passive optical networking, that also begins to replace proprietary vendor hardware, with white box solutions, and software defined networking to virtualize network functions.

The CCAPs will migrate to virtualization of L2 and L3 functionality, using distributed or centralized deployments. Expect this virtualization to continue into the aggregation and core networks. Eventually Wireline and wireless access will converge into a single ultra-broadband access network.

1.6.7. Video Presentation on Broadband Network Architectures

Click here for a video presentation on this topic.

2. C100G/C40G/C1G CMTS Hardware and Software Implementations and Operations

Chapter Overview

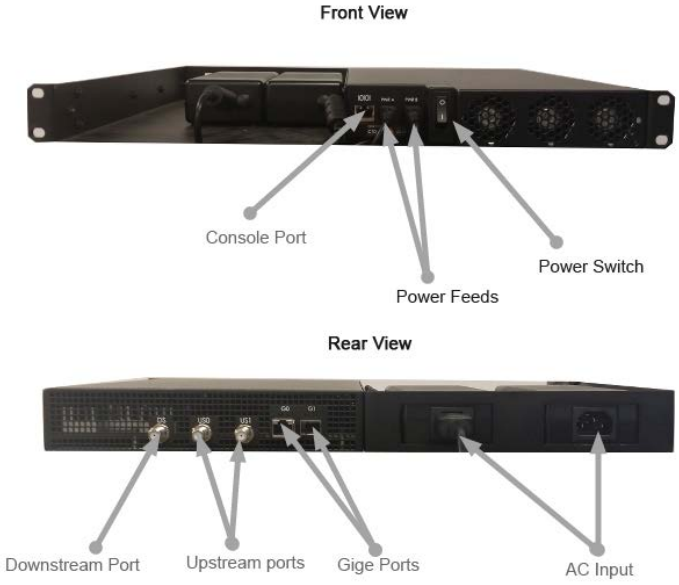
This chapter will describe and discuss CMTS hardware and software implementations.

Objectives

After successfully completing this chapter you will be able to:

- Name the Casa CMTS platforms
- Describe the Casa CMTS Hardware Architecture
- Identify the Casa Line Card models and their capacities
- Explain cooling and power on the C100G
- List the Data Center services the CMTS interacts with
- Explain the Casa Radio Frequency Interface impementations and operations
- Describe the Casa Network Side Interface implementations and how they operate

2.1. C1G Hardware Implementations



The Casa Systems C1G Cable Modem Termination System (CMTS) is a small form factor cable edge device that is suitable for distributed deployments, such as Multi dwelling units (MDUs), resorts, and rural markets. Let’s describe the hardware and RF channel capacities of the C1G platform.

C1G front view. The C1G shown here has an attached optional rack mount installed. This rack mount hardware allows installation of the C1G in a standard 19 inch telecommunications cabinet or rack. An optional wall mount rack is also available for mounting the C1G. Please refer to the C1G Hardware guide for installation instructions, for these two options.

Power switch. The C1G supports redundant 12 volt DC power inputs, each connected to an AC voltage source. The DC power modules are designed to fit into the attached rack mount tray just described.

Console port. For local out of band management, the CLI can be accessed from the console port, using a standard rollover DB9 to RJ45 cable. Optionally, for remote out of band management a terminal server can be connected to the console port. The default serial communications settings are: bits per second 11 5 200, data bits 8, parity none, stop bits 1, and flow control none.

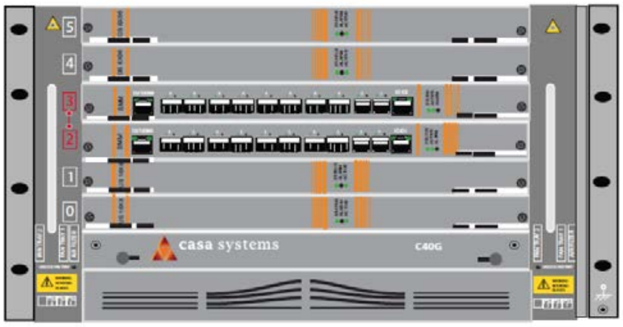
On the rear of the C1G are:

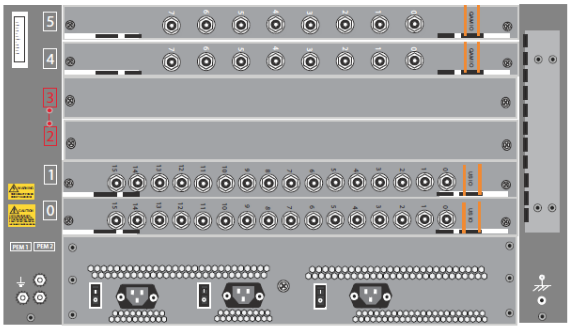
- The AC Power inputs, using the optional rack mount unit
- Two gigabit Ethernet ports, 0 and 1
- Two upstream RF ports, US0 and US1, each capable of 4 upstream channels for a maximum upstream capacity of 8 upstreams
- A downstream RF port with a maximum capacity of 8 downstream channels

2.1.1. Video Presentation on C1G Hardware Implementations

Click here for a video presentation on this topic.

2.2. C40G Hardware Implementations





2.2.1. Overview

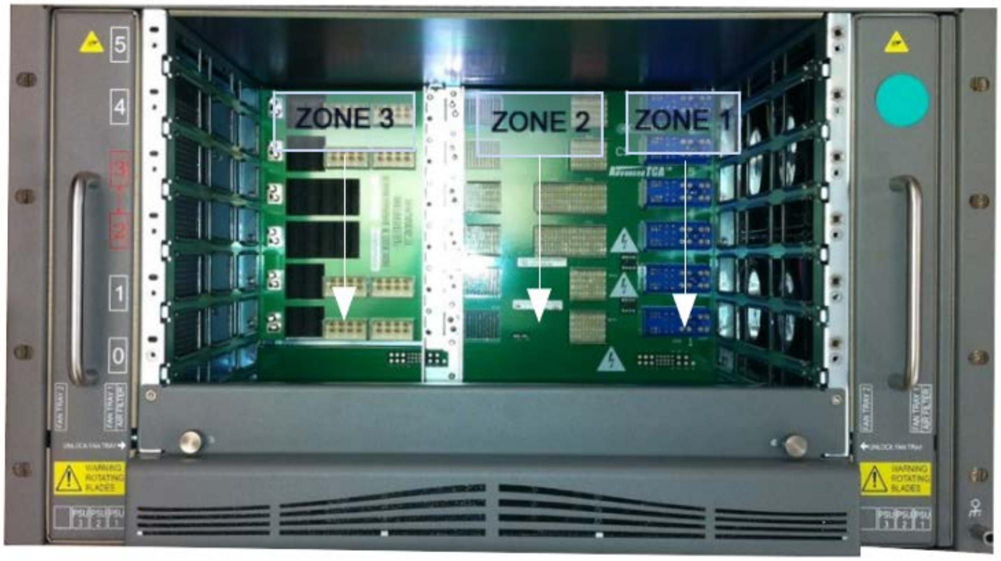
The Casa C40G is a fully integrated CMTS platform that combines CMTS and MPEG video Edge QAM functionality in a medium density, high availability platform.

2.2.1.1. Video Presentation on C40G Hardware Implementations

Click here for a video presentation on this topic.

2.2.2. Chassis

Let’s discuss the chassis in detail.



The Casa CMTS chassis complies with the Advanced Telecommunications Architecture (ATCA). ATCA defines an open, switch fabric based design, that delivers an industry standard high performance, fault tolerant, and scalable solution for next generation telecommunications and data center equipment.

The backplane is entirely passive and delivers high levels of reliability as there are no active components to fail. The backplane defines the overall board layout and connector location, high speed and power connectors, alignment key structures for mechanical integrity, and electrical keying for the modules.

The backplane definition is divided into three sections; Zone-1, Zone-2, and Zone-3. The connectors in Zone-1 provide redundant −48 VDC power and shelf management signals to the boards. The connectors in Zone-2 provide the connections to the Base Interface and Fabric Interface. Zone 3 provides the connections from the switch fabric to the IO modules.

2.2.2.1. Video Presentation on the C40G Chassis

Click here for a video presentation on this topic.

2.2.3. Front Deployment Options

The six slots on the C40G are numbered from 0 to 5, running from bottom to top. These slot numbers are clearly marked on the chassis.

The front slots house the Upstream Modules, and the Downstream Modules, as well as the Switch Management Modules (SMMs).

In this diagram we show a fully populated, redundant configuration. In this configuration, slots 1 and 4 must be populated with backup RF modules and slots 2 and 3 must be populated with SMMs.

Although it is possible to arrange the active modules in any combination, Casa recommends that you populate the lower zone and the upper zone with all of the same type of module.

In other words, put all upstreams in the lower zone and all downstreams in the upper zone, or vice versa. This will enable the CMTS platform to recover from a concurrent upstream and downstream module failure.

If you don't require RF redundancy, you may install downstream and upstream modules in slots 0, 1, 4, and 5 as desired. If you don't desire SMM redundancy, only slot 2 or 3 needs an SMM.

In addition, the C40G gives you front access to the fan trays, the fan filter and, if you are using AC power, your AC power supply units.

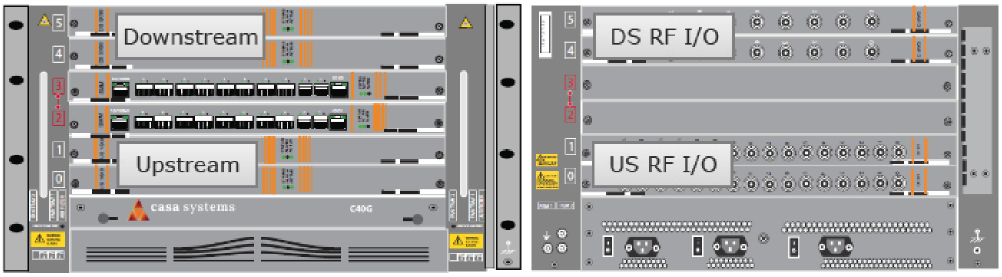
2.2.4. Rear Deployment Options

Install your RF I/O interface modules from the rear. For a fully redundant deployment, install your downstream and upstream cards in slots 0 and 5, and install Line Card switches in slots 1 and 4. Complete your redundancy deployment by installing SMM switch modules in slots 2 and 3.

For a fully loaded, non-redundant deployment, install RF I/O cards in slots 0, 1, 4, and 5, and filler plates in slots 2 and 3.

You can deploy both redundant and fully-loaded non-redundant configurations with either AC or DC power units.

Match Front and Back Modules

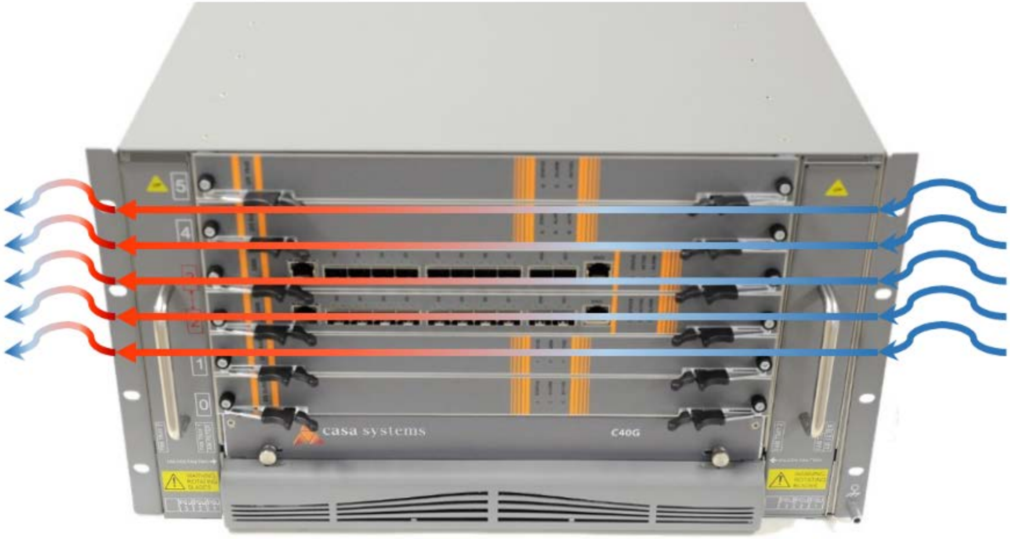


Your rear installed RF I/O modules need to match your front installed modules. This means that if a slot in the front has a Downstream QAM module installed, then a Downstream 8 port RF IO must be installed in the rear slot. If a slot in the front has an upstream QAM module installed, then an upstream 16 or 32 port RF IO must be installed in the rear slot.

2.2.4.1. Video Presentation on Deployment Options

Click here for a video presentation on this topic.

2.2.5. Cooling Architecture

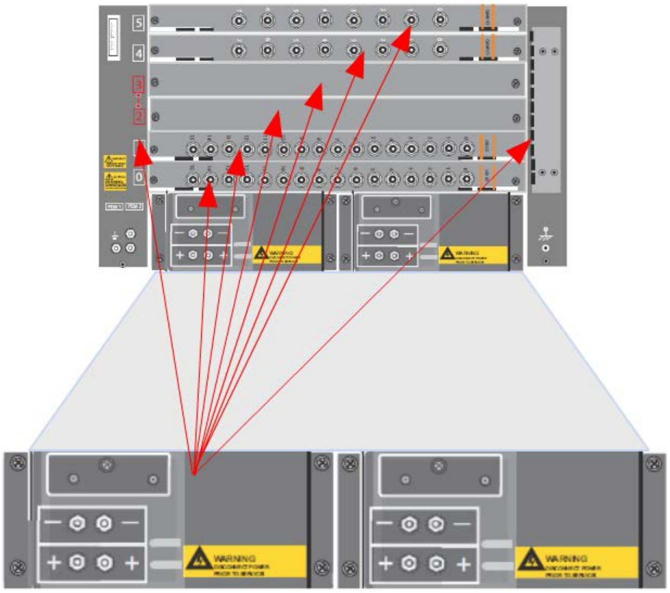


The C40G relies on two redundant, hot-swappable fan trays for cooling. The fan trays pull air across the fan filters into the chassis from the right side, and exhaust the heated air from the left side.

2.2.5.1. Video Presentation on Cooling Architecture

Click here for a video presentation on this topic.

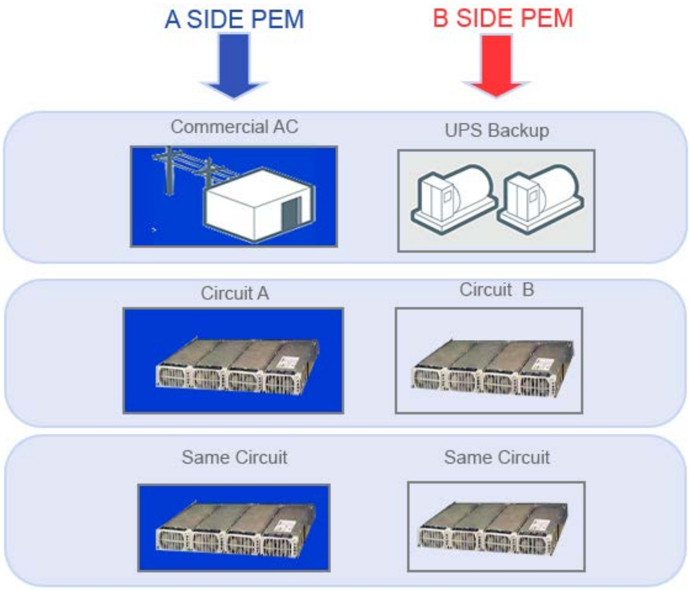
2.2.6. Power Architecture



The Casa C40G CMTS power architecture provides dual redundant -48 Volts DC power, supplied by two pluggable redundant Power Entry Modules (PEMs). The PEMs are located at the rear side bottom of the chassis. Each PEM provides power terminals for two 30 Amp power feeds.

The feeds to the PEMs come from one or two power plants within a head end or hub site facility. Each PEM connects to each slot and both fan trays, so it only requires one PEM to run a fully-loaded chassis. Local DC to DC conversion is accomplished per board.

Power Configurations



The following is a discussion of typical power configurations in a head end or hub site facility.

Scenario 1, Commercial AC to DC plant connected to PEM A and a UPS generator backup for example, connected to the secondary PEM, PEM B. The Internal electronics of the Casa chassis use a FET “Oring” design. This design will always use power from the higher voltage source and the second source will draw no current. Therefore, PEM A should be configured to a higher voltage, so you are not drawing current from your backup system.

Scenario 2: Casa supplied Split shelf rectifiers or similar product for each CMTS. The commercial AC is connected to both sides of the rectifier, but from different facility circuits. Then the rectifier is connected to the A and B PEMs. This configuration only protects against a failure of one side of the rectifier shelf or a facility circuit failure.

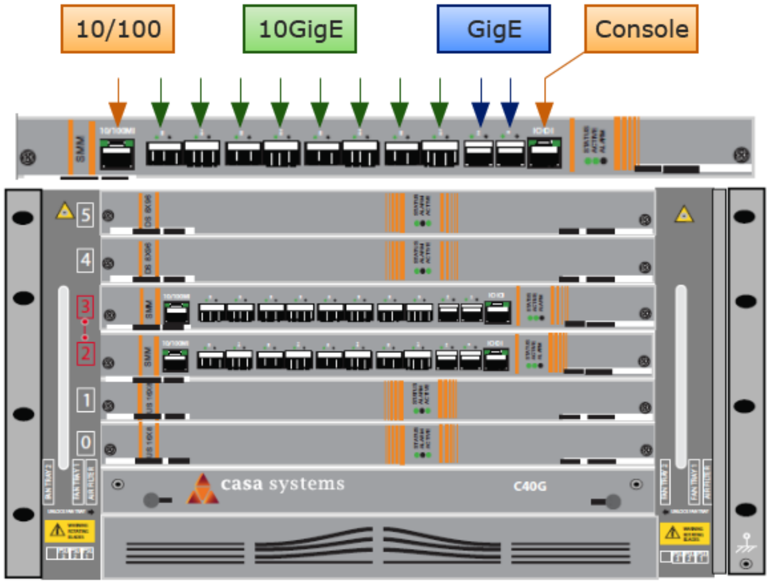
Scenario 3: Casa supplied Split shelf rectifiers or similar product for each CMTS. In this case the commercial AC is connected to both sides of the rectifier, but from the same facility circuit. This configuration only protects against a failure of one side of the rectifier shelf.

In Scenarios 2 and 3, the output of the rectifiers cannot be controlled. Therefore, the internal electronics of the PEMs will determine which PEM is primary and which is secondary, based on which side of the shelf is supplying a higher voltage.

2.2.6.1. Video Presentation on Power Architecture

Click here for a video presentation on this topic.

2.2.7. Switch Management Modules

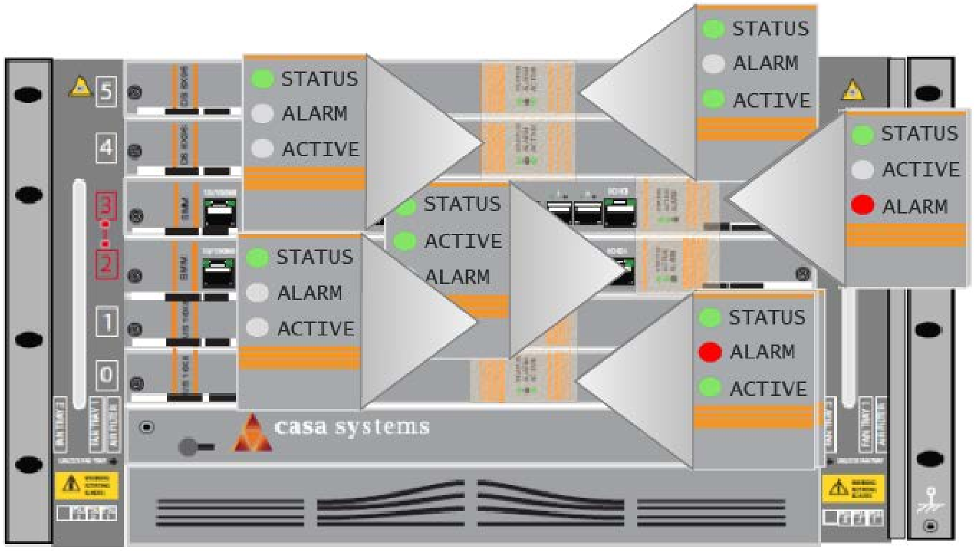


The Switch Management Module (SMM), is a front installed module that provides IP connectivity to the operator’s distribution and core networks.

This Module is available in two options, Standard and High Density. Both SMMs have 12 interfaces. The standard SMM has eight gigE, and two 10gigE ports. The high-density SMM has eight 10 gigE,and two gigE ports.

The two other interfaces on the module, a 10/100 Ethernet port and a serial console port, are used for management.

The 8 in-band Ethernet interfaces are numbered 0 through 7 from left to right. The other two in-band interfaces are numbered 0 and 1 from left to right.



Let’s discuss the LEDs available on the Casa CMTS. All the upstream, downstream and SMM module LEDs are labeled: Status, Active, and Alarm.

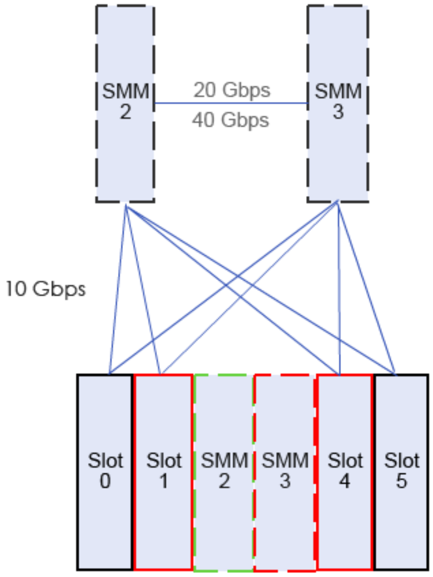
No LED illumination indicates, no power, or system off, condition.

In an SMM redundant configuration under normal conditions, the Primary SMM, usually module 2, will have the Status and Active LED green and the backup SMM, usually module 3, will have only the status LED green.

In an RF redundant configuration, a normal condition for the line cards in slots 0 and 5 is the Status and Active LEDs are green. On the backup line cards in slots 1 and 4 the status LED is green.

Finally, when a fault is detected the Alarm LED will be Red. Note: this alarm can be of a critical or non-critical nature. Casa recommends you check the alarm through a management interface to confirm the nature of the alarm, before replacing any hardware.

SMM Hardware Redundancy



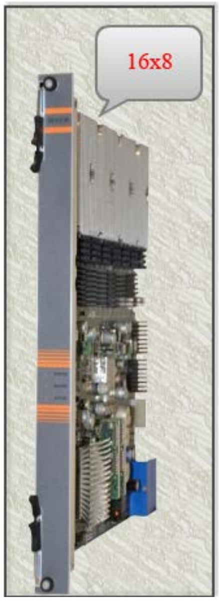
The Casa chassis switch fabric is wired as a dual star topology. Slots 2 and 3 connect to all the other slots. The backplane is wired to support 40 gigabits per second. The 8x96 line card supports 10 gigabits per second to each SMM.

Additionally, there is an SMM interlink between redundant SMMs. This link is 20 gigabits per second for the SMM 2x10, and 40 gigabits per second for the SMM 8x10. Both of these links can be used to route traffic to the downstream line cards. Note, in an SMM fail-over scenario, throughput will be reduced to 100 gigabits per second.

2.2.7.1. Video Presentation on SMM Modules

Click here for a video presentation on this topic.

2.2.8. RF Modules



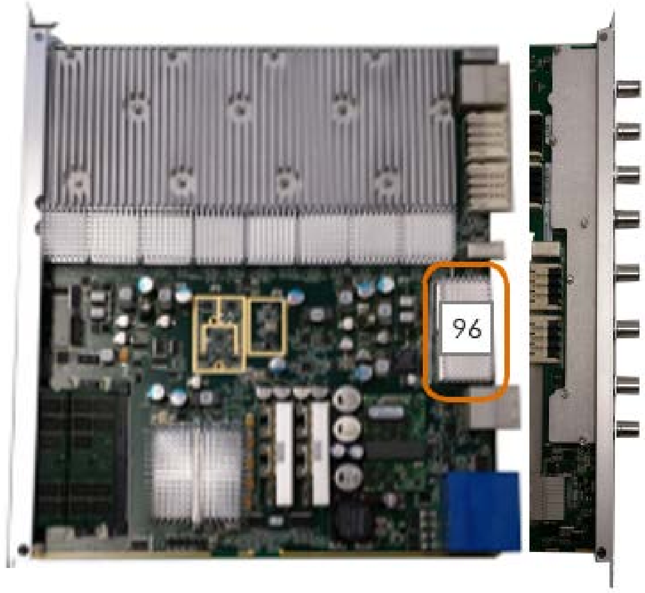
The C40G supports three different Line Card Modules.

For the downstream, you can choose either the 8x96 or the 8x192. For the upstream, install the 16x8. These modules install in the front slots of your chassis.

In the downstream, each I/O port is supported by one dedicated FPGA. That FPGA provides the port with 36 Narrowcast downstream channels. Each I/O port/FPGA pair is fixed; the FPGA will always provide 36 narrowcast channels to its paired port, and only to its paired port.

The two FPGAs on the rear of the line card give you more flexibility. Each FPGA provides you with 48 channels, for a total of 96 channels, that you can allocate across your ports as broadcast channels.

If you require more narrowcast channels you can allocate some, or all, of the additional 96 channels, using the module, module number, narrowcast-channels, number of channels, command.



On the 8 by 96, the valid range for the value of the, number of channels variable, is 36-48.

This command will allocate, from the 96 channels provided by the two rear FPGAs, a sufficient number of narrowcast channels, to bring the total number of narrowcast channels on each port, up to the value you specify. Note that you cannot specify a different number of narrowcast channels per port; the command affects all the ports on the module.

As an example, say you issue the command, module 2 narrowcast-channels 42. To comply with the command, the CCAP allocates to each port 6 additional channels from the 96 channels provided by the rear FPGAs.

Each port then has the 36 channels provided by its dedicated FPGA, plus 6 additional channels allocated to it from the rear FPGAs, for a total of 42 channels. This consumes 48 of the available channels provided by the rear FPGAs (8x6=48).

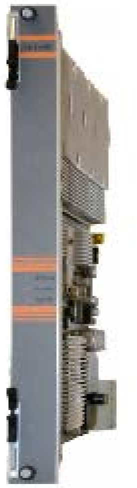
Note that if you configure more than 42 narrowcast channels per port on your module, you begin to cut into your available broadcast channels. For example, if you use the module 2 narrowcast-channels 48 command to allocate an additional 12 narrowcast channels to each port from the 96 channels provided by the two rear FPGAs, it will consume all of those channels (12 channels x 8 ports = 96 channels). This will reduce the number of channels available for broadcast to 0.

Thus, either of two different configurations will provide you with maximum channel usage:

- 32 narrowcast + 96 broadcast channels per port
- 36 narrowcast + 92 broadcast per port

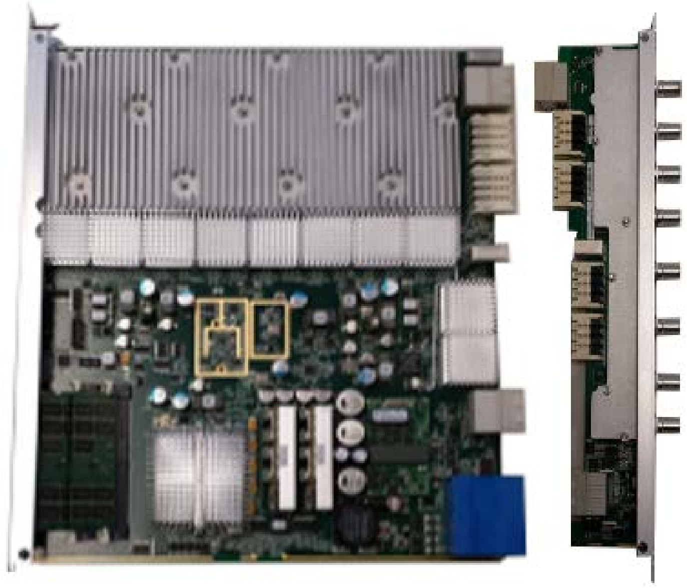
Please note the following limitations on the 8 by 96 module.

- One, If the downstream is operating in Annex A mode, the 8 by 96 is limited to 96 channels per port.
- Two, if you enable DVB simulcrypt, then each FPGA can only do 32 channels.
- Finally, the broadcast (rear) FPGA channels are video only channels.



Although the current capacity of the Casa CCAP is more than sufficient to support today’s network bandwidth needs, Casa's next generation of line card, the 8x192, will support even higher levels of throughput.
The base and fabric interfaces are enabled by high speed connectors in a 4 x10 differential pair configuration. Eight of these signal pairs define a channel or lane. This is the unit of connectivity between the modules in the switch fabric. A single lane operates in a 4x10 gigabits per second link, or 40 gigabits per second to each module, for an aggregate platform bandwidth of 160 gigabits per second.

To support DOCSIS 3.1, the 8x192 hardware has been upgraded to include:
Third generation processor with twice the number of cores resulting in 2 to 3 times the performance of our 8 by 96 card
A new generation FPGA to support Casa's own implementation of OFDM. This FPGA upgrade increases the number of gates by a factor of 4.
A new generation of DAC to implement the increased spectrum range of DOCSIS 3.1.



Similar in design to the 8 by 96, each IO port is supported by one dedicated FPGA. Except now the FPGA provides the port with 64 Narrowcast downstream channels. Each IO port/FPGA pair is fixed; the FPGA will always provide 64 narrowcast channels to its paired port, and only to its paired port.

The two FPGAs on the rear of the line card give you more flexibility. Each FPGA provides you with 64 channels, for a total of 128 channels, that you can allocate across your ports, in two ways.

First, you can allocate some or all of the additional 128 channels as narrowcast channels, using the module <module #> narrowcast-channels <# of channels> command. On the 8x192, the valid range for the value of the <# of channels> variable is 64-80.

This command will allocate, from the 128 channels provided by the two rear FPGAs, a sufficient number of narrowcast channels to bring the total number of narrowcast channels on each port up to the value you specify. Note that you cannot specify a different number of narrowcast channels per port; the command affects all the ports on the module.

As an example, say you issue the command, module 2 narrowcast-channels 70. To comply with the command, the CCAP allocates to each port 6 additional channels from the 128 channels provided by the rear FPGAs.

Each port then has the 64 channels provided by its dedicated FPGA, plus 6 additional channels allocated to it from the rear FPGAs, for a total of 70 channels. This consumes 48 of the available channels provided by the rear FPGAs (8x6=48).

Note that if you configure more than 72 narrowcast channels per port on your module, you begin to cut into your available broadcast channels. For example, if you use the module 2 narrowcast-channels 80 command to allocate an additional 16 narrowcast channels to each port from the 128 channels provided by the two rear FPGAs, it will consume all of those channels (16 channels x 8 ports = 128 channels). This will reduce the number of channels available for broadcast to 0.

Thus, either of two different configurations will provide you with maximum channel usage:

- 72 narrowcast channels and 64 broadcast channels per port
- 80 narrowcast channels per port

2.2.8.1. Video Presentation on RF Modules

Click here for a video presentation on this topic.

2.2.9. I/O Modules

Installing the 16x8 upstream module in the front slot allows you to deploy either the UPS 16x8 I/O or the UPS 32x4 I/O module in the back slot. Thus, you can deploy as many as 32 upstream ports in a fully redundant configuration.

The 32-port I/O uses micro coaxial (MCX) snap-on connectors. These connectors require quad-shielded adaptors, with MCX connectors on one end and standard 75 ohm F-connectors on the other end.

Casa also offers the UPS 32x4 I/O cable retention plate, to help you secure your connections.

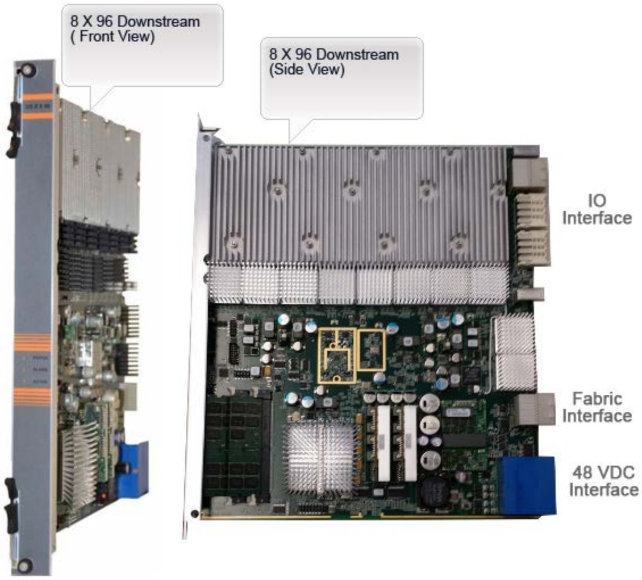
2.2.9.1. Video Presentation on I/O Modules

Click here for a video presentation on this topic.

2.2.10. RF SMM and LC Switch Modules

The C40G is equipped with a built-in RF switch architecture comprising four modules connected to an RF switch backplane. Using two SMM Switch and two LC Switch modules, these devices will process a dropped RF connection at a failed module by transferring the live traffic to the redundant failover module.

2.2.11. Architecture and Traffic Flow



Let’s describe the major hardware components of our downstream modules, using the 8x96 as our example.

The Network Processor is an ASIC that Casa Software interacts with to provide general purpose processing cycles, as well as specific hardware and network acceleration functions. The processor has XAUI interfaces to the switch fabric, and serial gigabit interfaces to the Field Programmable Gate Arrays (FPGAs).

Casa uses an FPGA design in our line cards, as opposed to traditional all-ASIC designs. This FPGA design enables Casa to address bugs and deliver feature upgrades in the DOCSIS PHY layer in the field. Casa saves the cost of doing ASIC spins, and encounters fewer design limitiations, due to the hardware in our downstream modules.

Finally, Digital Up Converters (DUCs) and Digital to Analog Converters (DACs) define frequency agility, modulation technique, and channel width of the digital and RF signals generated out the RF ports.

Traffic Flow on the Upstream Modules

Let’s describe the traffic flow on the upstream modules, using the Casa 16x8 module as our example.

Analog and digital front-end components perform tuning, automatic gain control, channel selection, analog-to-digital conversion, and related functions. Their purpose is to preprocess the signal, so that the individual QAM RF channels are available for further digital processing.

After this, the upstream card uses FPGA designs to implement upstream features such as Adaptive Equalizer. This feature compensates for channel effects, including group delay variation, amplitude slope, and micro reflections. It adapts its filter coefficients to dynamically varying channel responses so as to maximize the receive MER.

An ingress canceller is included in the Casa CCAP burst receiver to remove narrow band interference, such as commercial and private radio transmissions. It operates by dynamically detecting and measuring the interference, and adapting its coefficients to cancel the interfering carriers.

Also included in this stage is the Casa spectrum manager, which enables the operator to configure rules to adjust phy layer parameters of the received upstream based on unacceptable Noise or FEC activity.

In the next stage, Casa implements standard ASIC designs to perform de-interleaving, Reed-Solomon de-coding and MPEG de-framing.
Finally, the de-modulated and de-multiplexed frames are delivered to the Casa MAC FPGAs. The MAC layer controls the physical layer and is the source and sync of PHY data. The MAC layer processes data frames delineated by DOCSIS headers. These FPGAs are also responsible for the request grant scheduling mechanism which controls cable modem service flows.

Casa Switch Management Module (SMM)

The CCAP SMM is responsible for all redundancy, control, and data plane operations. Let's discuss the major component architecture of the SMM.

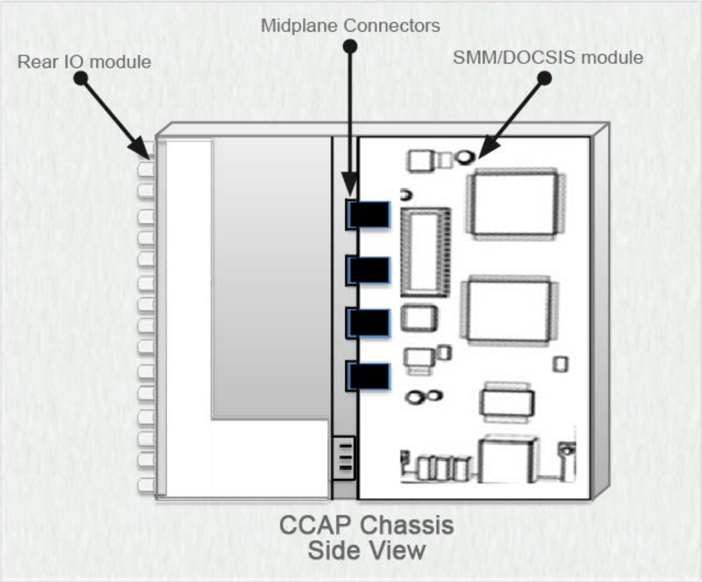
The Network Processor is a feature-rich general purpose processor, with application specific autonomous hardware accelerators and multiple on-chip interconnect options. The Processor enables integrated control plane, data plane, and security processing in a single System-on-a-Chip solution. The network processor connects to the switching components and the backplane through RGMII, SGMII, and XAUI interfaces.

For switching and routing of customer data there is a 10 gigabit multilayer switch. This switch provides many L2 L3 features, including ingress and egress ACLs, multi-tuple lookups, Layer 2 VLANs and Layer 3 tables, IPv4 and IPv6 Virtual Routing with full support for L2/L3 tunnels, trunking and QinQ, etc. Additionally, there is a gigabit switch to enable management traffic to and from the modules and backup SMM.

2.2.11.1. Video Presentation on Architecture and Traffic Flow

Click here for a video presentation on this topic.

2.2.12. Module Installation and Best Practices



Let’s describe some recommended best practices regarding hardware and chassis installation and configuration.

First, let’s describe the proper procedure to remove and install modules.

As already discussed, the rear and front modules are inserted into their slot, and meet at the mid-plane. At the mid-plane, there are several connectors that need to mate in order to establish proper connectivity through the chassis.

Removing and installing any front installed DOCSIS or SMM module is straight forward. Refer to the hardware installation guide for this procedure.

However, in the unlikely event that replacement of the rear installed I/O module is required, the order in which you proceed is important.

When removing the rear I/O, **ALWAYS** remove or loosen the front installed module first, and then remove the rear I/O module. When installing the the rear I/O, keep the front installed module loose or removed from the slot and (then) install and secure the rear I/O. Now you can install and secure the front installed module in its slot.

Further Guidelines

Here are a few other best practices regarding installation and maintenance of the CMTS chassis and modules.

- Ensure proper grounding of the chassis.
- Always be grounded to the chassis with static straps when handling modules.
- Ensure appropriate environmental temperature.
- Clean or replace the fan filter periodically.
- Install blank cards in empty slots to ensure optimal cooling through the chassis.
- When installing modules do not overtighten the captive thumb screws. Hand tight is sufficient.
- Power should be redundant with different sources, ideally with battery backup.

If possible maintain spare modules. Spare modules should be keep in anti static bags when not in use.

2.2.12.1. Video Presentation on Module Installation

Click here for a video presentation on this topic.

2.3. C100G Hardware Implementations and Operations

2.3.1. Overview

The Casa C100G is a next-generation CMTS that offers a high-density architecture in a 14-slot rack-mountable 13RU NEBS-compliant platform. The C100G supports DOCSIS 3.0 CMTS capabilities with integrated video QAM technology to create the first integrated Converged Cable Access Platform (I-CMTS) platform for combining data and digital video into a single hardware solution.

By combining CMTS and video QAM technology into a single platform, cable service providers can now maximize both power and the physical space requirements for equipment positioned at the cable headend. The system can be initially deployed as a full I-CMTS, or as a I-CMTS with later migration to the CMTS with the addition of QAM 8x96 modules for downstream narrowcast services with full redundancy and failover support.

As an I-CMTS, DOCSIS CMTS and video edge QAM services are configured separately on the system when there are no overlapping channels. The system checks to ensure that each QAM channel is operating for either DOCSIS or video. However, DOCSIS and video traffic can share the same network side interface (NSI) over separate VLANs.

2.3.2. Chassis

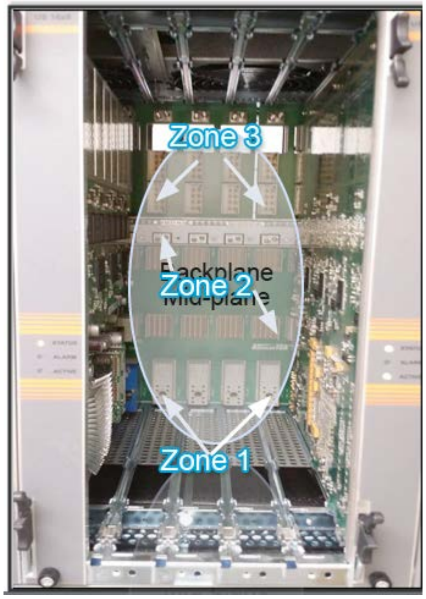
The C100G comprises the following hardware features and capabilities:

- NEBS-compliant 13RU carrier class chassis with 14 module slots (front and rear)
- Dual -48V DC Power Entry Modules
- Redundant hot-pluggable fans
- 40Gb mid-plane architecture
- Two SMM slots (6 and 7) for SMM redundancy and failover
- 12 slots for any combination of QAM downstream and DCU upstream line cards
- Full N+1 redundancy using slots 5 and 8 for downstream and upstream line cards
- Built-in RF switch using rear slots 5, 6, 7, and 8

Flexible Downstream to Upstream Channel Ratio

The C100G supports complete separation of downstream channel capacity and upstream channel capacity in a single physical chassis, providing a flexible downstream-to-upstream channel ratio. Cable operators can add downstream channels and upstream channels independently within the same chassis.

Chassis Backplane

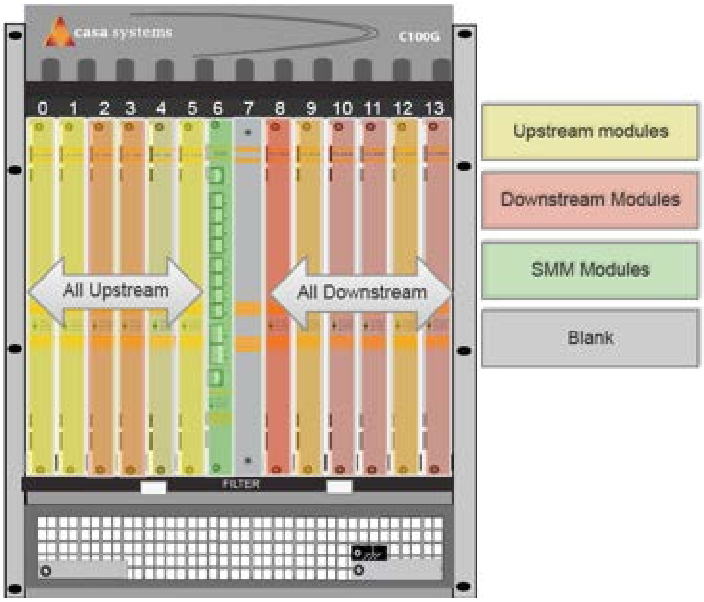


The Casa CMTS chassis complies with the Advanced Telecommunications Architecture (ATCA). ATCA defines an open, switch fabric design, that delivers an industry standard high performance, fault tolerant, and scalable solution for next generation telecommunications and data center equipment.

The backplane is entirely passive and delivers high levels of reliability as there are no active components to fail. The backplane defines the overall board layout and connector location, high speed and power connectors, alignment key structures for mechanical integrity, and electrical keying for the modules.

The backplane definition is divided into three sections; Zone-1, Zone-2, and Zone-3. The connectors in Zone-1 provide redundant –48 VDC power and shelf management signals to the boards. The connectors in Zone-2 provide the connections to the Base Interface and Fabric Interface and Zone 3 which provide the connections from the switch fabric to the IO modules.

Front View and Slot Configurations



Slots are numbered 0 to 13 left to right. These numbers are clearly marked on the chassis. The front slots house the upstream modules and the downstream modules as well as the switch management modules (SMMs).

In this diagram we show a fully populated, redundant configuration. In this configuration, slots 5 and 8 must be populated with backup RF modules and slots 6 and 7 must be populated with SMMs.

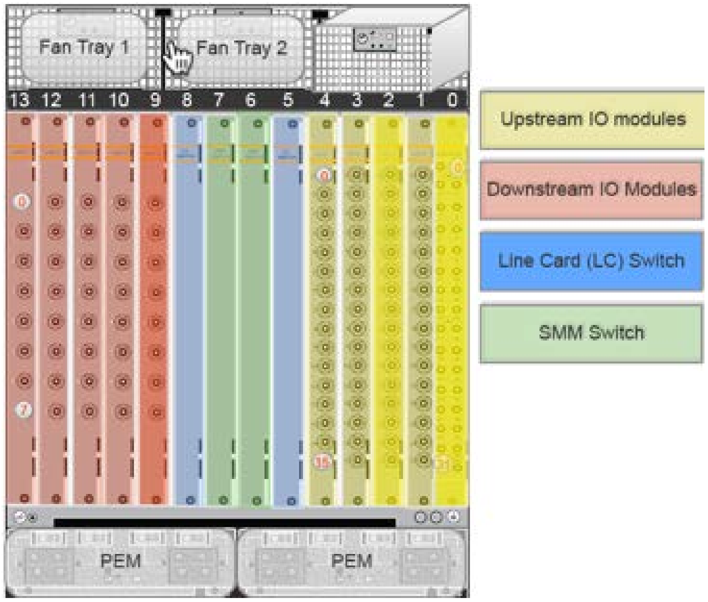
If RF redundancy is not enabled the front line card slots 0 through 5 and 8 through 13 can be installed in any combinations of downstream and upstream modules as desired.

If SMM redundancy is not desired slot 6 or 7 only needs an SMM.

Other functional elements on the front of the chassis are, the fan filter, cold air intake vents and a grounding lug.

Although it is possible to arrange the active modules in any combination, Casa recommends that you populate the the left zone and the right zone with all of the same type of module. In other words, put all upstreams in the left zone and all down streams in the right, or vice versa. This will enable the CMTS platform to recover from a concurrent upstream and downstream module failure.

Rear View and Slot Configurations



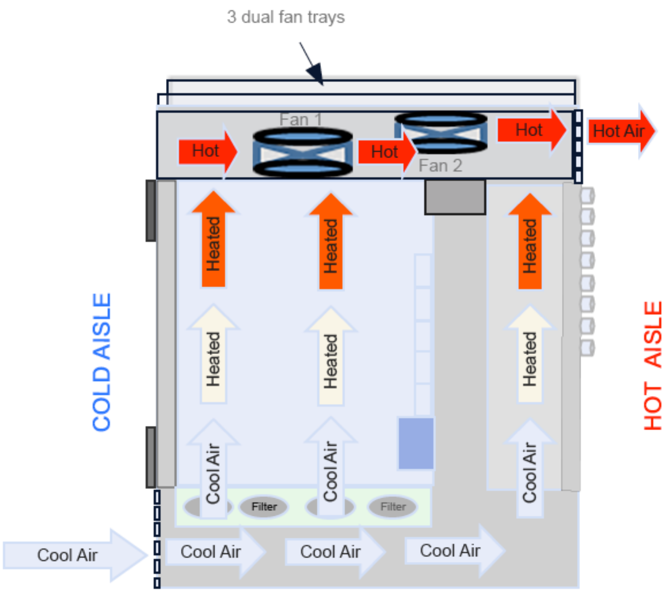
In the rear, slots are numbered 0 to 13 right to left. These slot numbers, unlike the front, are not marked on the Chassis. The rear slots contain RF IO upstream and RF IO downstream interface modules. Rear installed RF I/O modules need to match the front installed modules.

This means that if a slot in the front has a Downstream QAM module installed, then a Downstream 8 port RF IO must be installed in the rear slot. If a slot in the front has an upstream QAM module installed, then an upstream 16 or 32 port RF IO must be installed in the rear slot. RF IO Port Numbering The top RF port is 0 on both the 16 and 8 port versions. The bottom port is 7 for the downstream, and 15 for the upstream. The 32 port IO starts at 0 at the top right row and ends with 31 on the bottom left. The numbering for each port is clearly marked on every module.

The front installed module for the 32 port IO is a 16 by 8 upstream line card. The 32-port IO uses micro coaxial (MCX), snap-on connectors. These connectors require quad-shielded adaptors, with MCX connectors on one end, and standard 75 ohm F-connectors on the other end. Casa also offers a cable retention plate, to help you secure the MCX connections.

When RF redundancy is required, LC switch modules must be installed in slots 5 and 8. If SMM redundancy is required, then SMM Switch modules must be installed in slots 6 and 7. The top of the Chassis also houses and provides access to the 3 hot swappable fan assemblies. Each Fan tray has two fans for redundancy. Additionally, the bottom rear of the Chassis houses the hot swappable dual -48 VDC Power Entry modules.

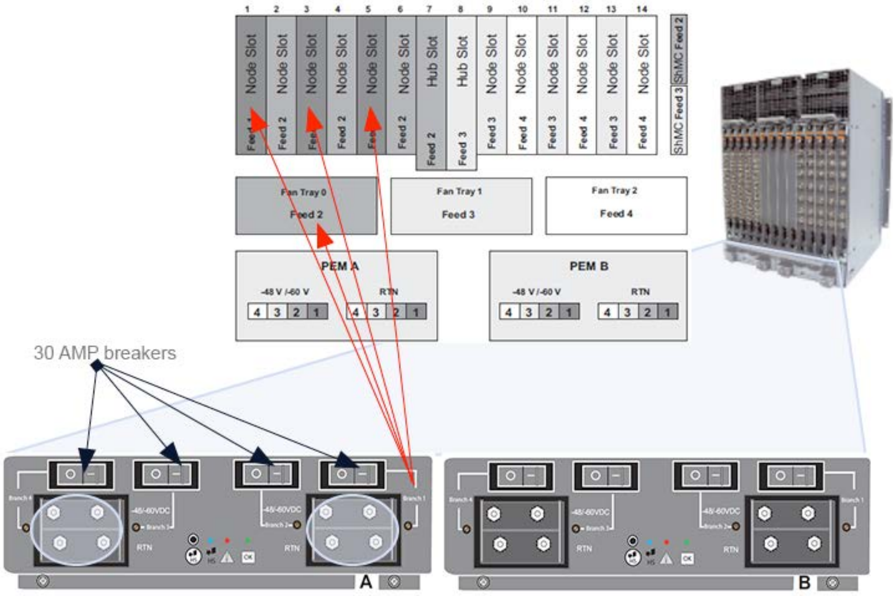
Cooling Architecture



Next, let's describe the chassis cooling architecture. First, because the Casa CMTS supports very dense QAM deployments, maintaining temperature tolerances is critical to proper performance.

Extensive thermal modeling is part of the design of the ATCA board and shelf form factors to be able to support proper power dissipation per board. There are 3 fan trays creating 3 airflow zones. The air flow design is cold aisle/hot aisle; that is, the air intake comes in from the cold aisle and is directed vertically across the cards. The heated air is then exhausted out the rear to the hot aisle.

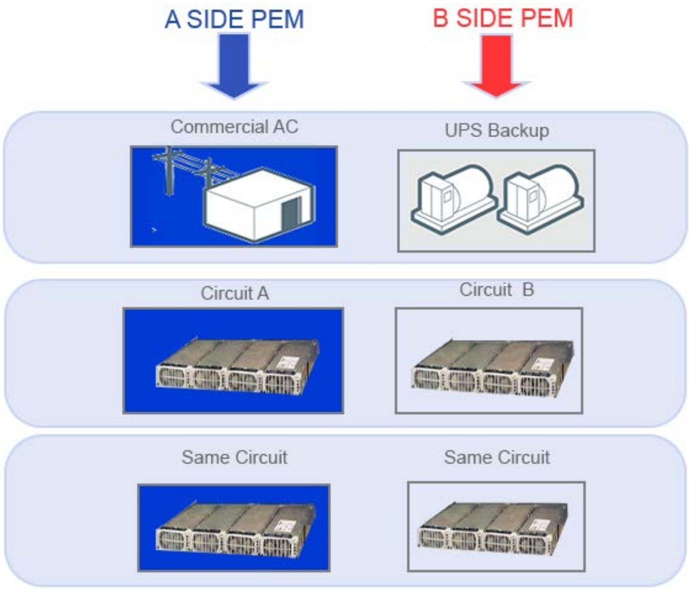
Power Architecture



The Casa CMTS power architecture provides Dual, redundant -48 Volts DC, facilitated by two pluggable redundant Power Entry Modules, or PEMs. The PEMs are located at the rear side bottom of the chassis. Each PEM provides power terminals for four 30 Amp power feeds.

The feeds to the PEMs come from one or two power plants within a head end or hub site facility. The PEMs are split into 4 branches, and are electrically isolated by 30 amp fuses. Local DC to DC conversion is accomplished per board. The four power branches supply power to different parts of the backplane and, therefore, specific boards or fan trays, as illustrated in the diagram. For example branch one powers slot 1, slot 3, slot 5, and fan tray 0.

Power Configurations



The following is a discussion of typical power configurations in a head end or hub site facility.

Scenario 1: Commercial AC to DC plant connected to PEM A, and a U P S, generator backup, for example, connected to the secondary PEM, PEM B. The internal electronics of the Casa chassis use a FET O-ring design. This design will always use power from the higher voltage source, and the second source will draw no current. Therefore, PEM A should be configured to a higher voltage, so you are not drawing current from your backup system .

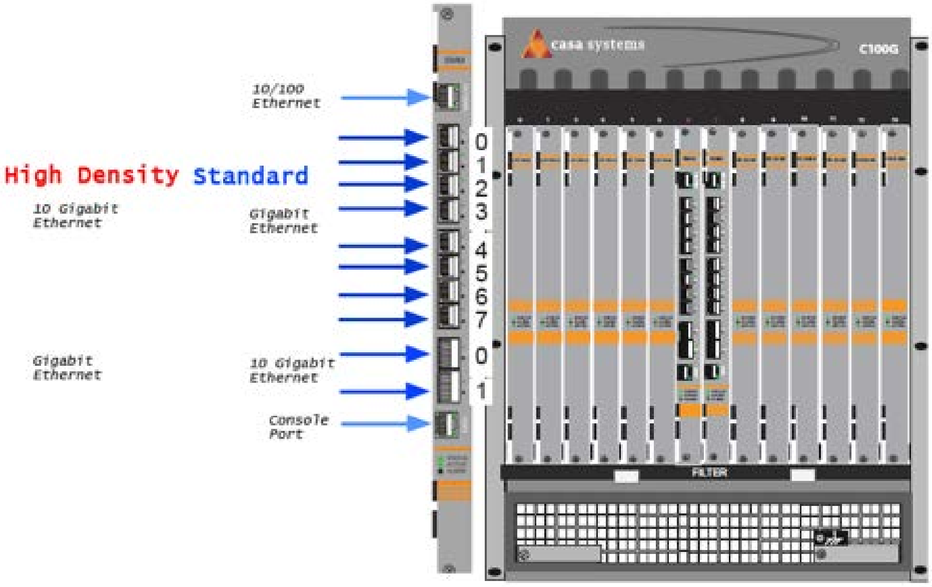
Scenario 2: Casa supplied Split shelf rectifiers, or similar product for each CCAP/CMTS. The commercial AC is connected to both sides of the rectifier, but from different facility circuits. Then the rectifier is connected to the A and B PEMs. This configuration only protects against a failure of one side of the rectifier shelf or a facility circuit failure.

Scenario 3: Casa supplied Split shelf rectifiers, or similar product for each CCAP/CMTS. In this case the commercial AC is connected to both sides of the rectifier, but from the same facility circuit. This configuration only protects against a failure of one side of the rectifier shelf.

2.3.2.1. Video Presentation on the C100G Chassis

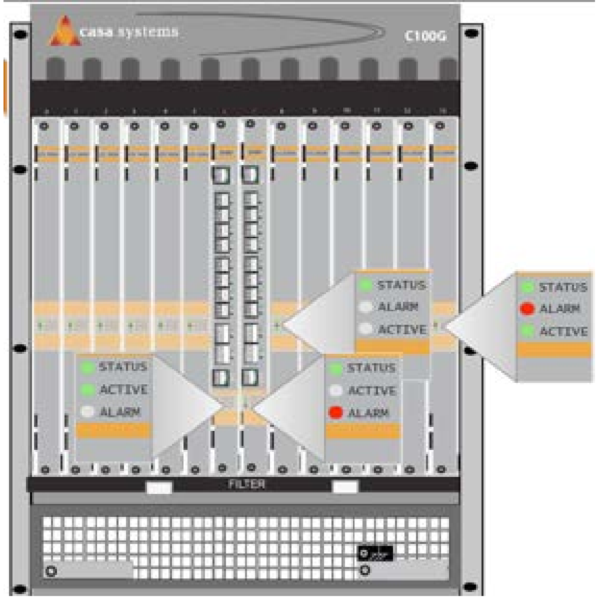
Click here for a video presentation on this topic.

2.3.3. Switch Management Modules



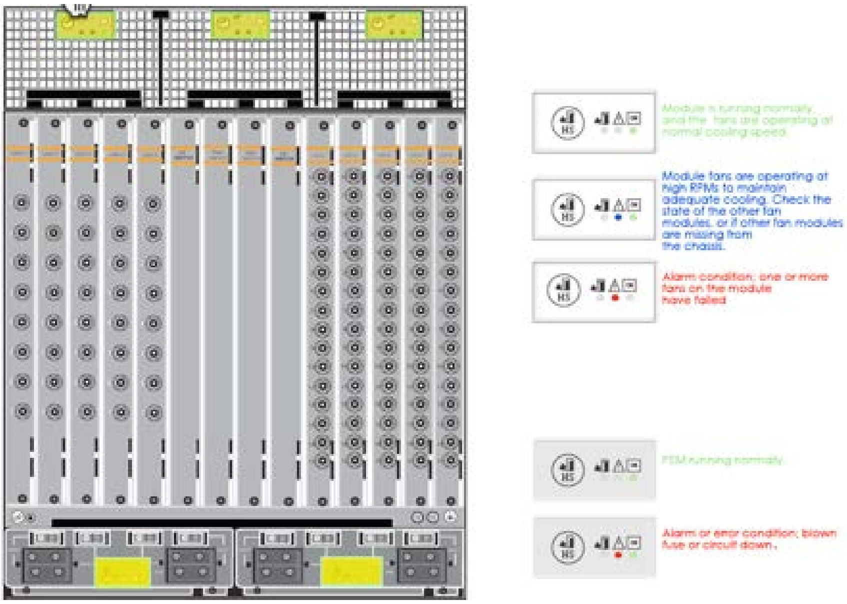
The SMM is a front installed module that provides IP connectivity to the operator’s distribution and core networks. This Module is available in two options, Standard and High Density. Both SMMs have 12 interfaces. The standard SMM has eight gigE, and two 10gigE ports. The high-density SMM has eight 10 gigE,and two gigE ports. The two other interfaces on the module are, a 10/100 Ethernet port and a serial console port for managment traffic. The 8 in-band Ethernet interfaces, are numbered 0 through 7 top to bottom, and the other two in-band interfaces are numbered 0 and 1 top to bottom.

LEDs



All the upstream, downstream and SMM module LEDs are labeled Status, Active, and Alarm. No LED illumination indicates no power, or system off, condition. In an SMM redundant configuration, a normal condition for the SMM modules is the Primary SMM, usually module 6, will have the Status and Active LED green and the backup SMM, usually module 7, will have only the status LED green. In an RF redundant configuration, a normal condition for the line cards in slots, 0 through 4, and 9 through 13 is the Status and Active LED are green and the backup line cards in slots 5 and 8 the status LED is green.

Finally, when a fault is detected the Alarm LED will be Red. Note this alarm could be of a critical or non critical nature. It is recommended the alarm be checked through a management interface before performing any hardware replacement to confirm the nature of the alarm.


HS
Module is running normally, and the fans are operating at normal cooling speed.
HS
Module fans are operating at high RPMs to maintain adequate cooling. Check the state of the other fan modules, or if other fan modules are missing from the chassis.
HS
Alarm condition: one or more fans on the module have failed
HS
PEM running normally.
HS
Alarm or error condition: blown fuse or circuit down.

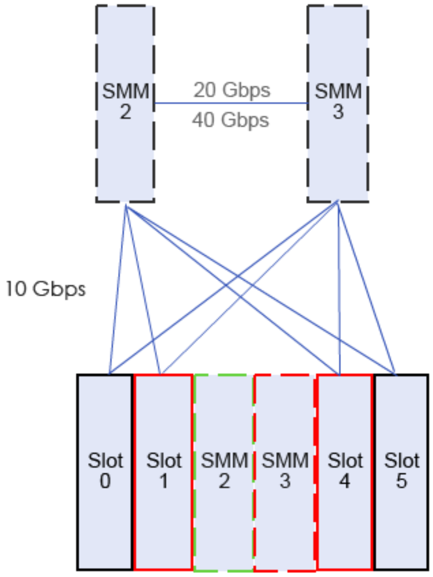
The other system LEDs are located on the rear of the Chassis, for the Fans and the Power entry Modules. There are only two LEDs that are active, the OK LED and the Caution LED. The Caution LED is the triangle with an exclamation point.

For the fan LEDs, green means the fan module is running normally, and the fans are operating at normal cooling speed. A blue Caution LED, means the Module fans are operating at high RPMs to maintain adequate cooling. Check the state of the other fan modules, or if other fan modules are missing from the chassis.

A Red caution LED, means an Alarm condition, one or more fans on the module have failed.

For the PEMs, a green OK LED means the PEM is running normally. A Red caution LED means the PEM has an alarm or error condition possibly a blown fuse or circuit down.

SMM Hardware Redundancy



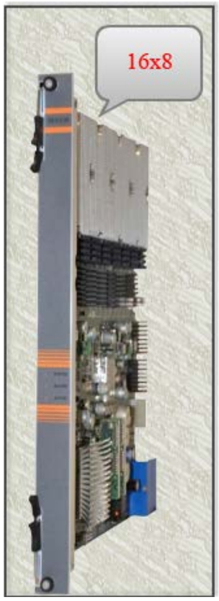
The Casa chassis switch fabric is wired as a dual star topology. Slots 2 and 3 connect to all the other slots. The backplane is wired to support 40 gigabits per second. The 8x96 line card supports 10 gigabits per second to each SMM.

Additionally, there is an SMM interlink between redundant SMMs. This link is 20 gigabits per second for the SMM 2x10, and 40 gigabits per second for the SMM 8x10. Both of these links can be used to route traffic to the downstream line cards. Note, in an SMM fail-over scenario, throughput will be reduced to 100 gigabits per second.

2.3.3.1. Video Presentation on SMM Modules

Click here for a video presentation on this topic.

2.3.4. RF Modules



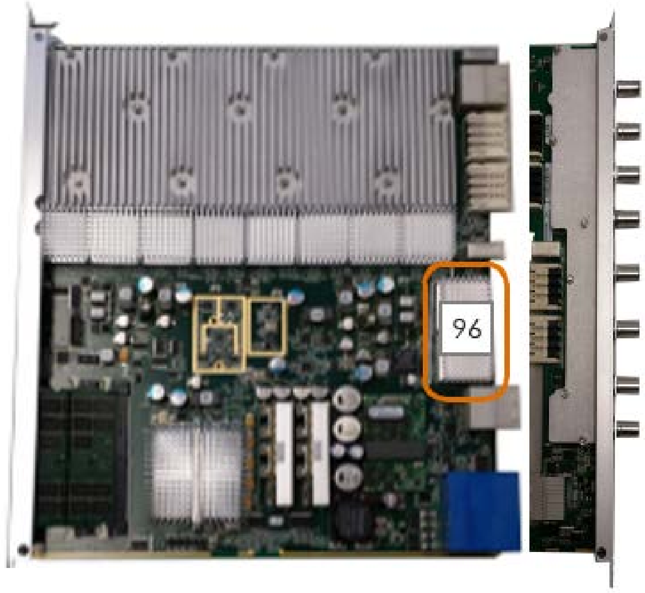
The C100G supports three different Line Card Modules.

For the downstream, you can choose either the 8x96 or the 8x192. For the upstream, install the 16x8. These modules install in the front slots of your chassis.

In the downstream, each I/O port is supported by one dedicated FPGA. That FPGA provides the port with 36 Narrowcast downstream channels. Each I/O port/FPGA pair is fixed; the FPGA will always provide 36 narrowcast channels to its paired port, and only to its paired port.

The two FPGAs on the rear of the line card give you more flexibility. Each FPGA provides you with 48 channels, for a total of 96 channels, that you can allocate across your ports as broadcast channels.

If you require more narrowcast channels you can allocate some, or all, of the additional 96 channels, using the module, module number, narrowcast-channels, number of channels, command.



On the 8 by 96, the valid range for the value of the, number of channels variable, is 36-48.

This command will allocate, from the 96 channels provided by the two rear FPGAs, a sufficient number of narrowcast channels, to bring the total number of narrowcast channels on each port, up to the value you specify. Note that you cannot specify a different number of narrowcast channels per port; the command affects all the ports on the module.

As an example, say you issue the command, module 2 narrowcast-channels 42. To comply with the command, the CCAP allocates to each port 6 additional channels from the 96 channels provided by the rear FPGAs.

Each port then has the 36 channels provided by its dedicated FPGA, plus 6 additional channels allocated to it from the rear FPGAs, for a total of 42 channels. This consumes 48 of the available channels provided by the rear FPGAs (8x6=48).

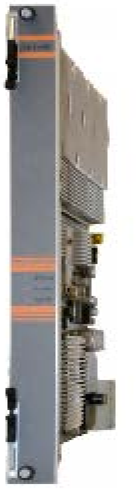
Note that if you configure more than 42 narrowcast channels per port on your module, you begin to cut into your available broadcast channels. For example, if you use the module 2 narrowcast-channels 48 command to allocate an additional 12 narrowcast channels to each port from the 96 channels provided by the two rear FPGAs, it will consume all of those channels (12 channels x 8 ports = 96 channels). This will reduce the number of channels available for broadcast to 0.

Thus, either of two different configurations will provide you with maximum channel usage:

- 32 narrowcast + 96 broadcast channels per port
- 36 narrowcast + 92 broadcast per port

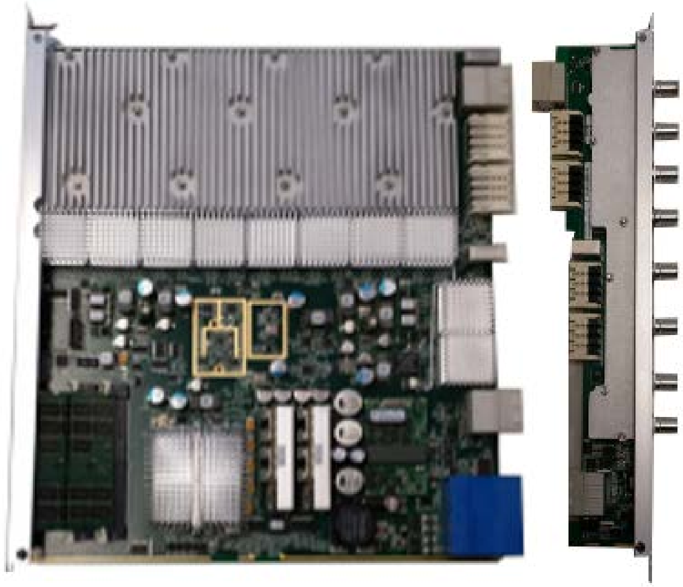
Please note the following limitations on the 8 by 96 module.

- One, If the downstream is operating in Annex A mode, the 8 by 96 is limited to 96 channels per port.
- Two, if you enable DVB simulcrypt, then each FPGA can only do 32 channels.
- Finally, the broadcast (rear) FPGA channels are video only channels.



Although the current capacity of the Casa CCAP is more than sufficient to support today's network bandwidth needs, Casa's next generation of line card, the 8x192, will support even higher levels of throughput.
The base and fabric interfaces are enabled by high speed connectors in a 4 x10 differential pair configuration. Eight of these signal pairs define a channel or lane. This is the unit of connectivity between the modules in the switch fabric. A single lane operates in a 4x10 gigabits per second link, or 40 gigabits per second to each module, for an aggregate platform bandwidth of 160 gigabits per second.

To support DOCSIS 3.1, the 8x192 hardware has been upgraded to include:
Third generation processor with twice the number of cores resulting in 2 to 3 times the performance of our 8 by 96 card
A new generation FPGA to support Casa's own implementation of OFDM. This FPGA upgrade increases the number of gates by a factor of 4.
A new generation of DAC to implement the increased spectrum range of DOCSIS 3.1.



Similar in design to the 8 by 96, each IO port is supported by one dedicated FPGA. Except now the FPGA provides the port with 64 Narrowcast downstream channels. Each IO port/FPGA pair is fixed; the FPGA will always provide 64 narrowcast channels to its paired port, and only to its paired port.

The two FPGAs on the rear of the line card give you more flexibility. Each FPGA provides you with 64 channels, for a total of 128 channels, that you can allocate across your ports, in two ways.

First, you can allocate some or all of the additional 128 channels as narrowcast channels, using the module <module #> narrowcast-channels <# of channels> command. On the 8x192, the valid range for the value of the <# of channels> variable is 64-80.

This command will allocate, from the 128 channels provided by the two rear FPGAs, a sufficient number of narrowcast channels to bring the total number of narrowcast channels on each port up to the value you specify. Note that you cannot specify a different number of narrowcast channels per port; the command affects all the ports on the module.

As an example, say you issue the command, module 2 narrowcast-channels 70. To comply with the command, the CCAP allocates to each port 6 additional channels from the 128 channels provided by the rear FPGAs.

Each port then has the 64 channels provided by its dedicated FPGA, plus 6 additional channels allocated to it from the rear FPGAs, for a total of 70 channels. This consumes 48 of the available channels provided by the rear FPGAs (8x6=48).

Note that if you configure more than 72 narrowcast channels per port on your module, you begin to cut into your available broadcast channels. For example, if you use the module 2 narrowcast-channels 80 command to allocate an additional 16 narrowcast channels to each port from the 128 channels provided by the two rear FPGAs, it will consume all of those channels (16 channels x 8 ports = 128 channels). This will reduce the number of channels available for broadcast to 0.

Thus, either of two different configurations will provide you with maximum channel usage:

- 72 narrowcast channels and 64 broadcast channels per port
- 80 narrowcast channels per port

2.3.4.1. Video Presentation on RF Modules

Click here for a video presentation on this topic.

2.3.5. I/O Modules

The RF Downstream I/O module (RFD) provides the mechanical and electrical QAM connection for downstream RF signals to the HFC network. It contains 8 RF ports with F-type connectors. Each port can output up to 4, 8, or 96 QAM channels. In aggregation, this single-slot I/O module can output a total of 32, 64, or 768 QAM channels.

The RF Upstream I/O modules (RFU) provide the mechanical and electrical upstream connection for RF signals from the HFC network. The standard I/O module contains 16 RF ports with F-type connectors for a total of 32, 64, or 128 channels.

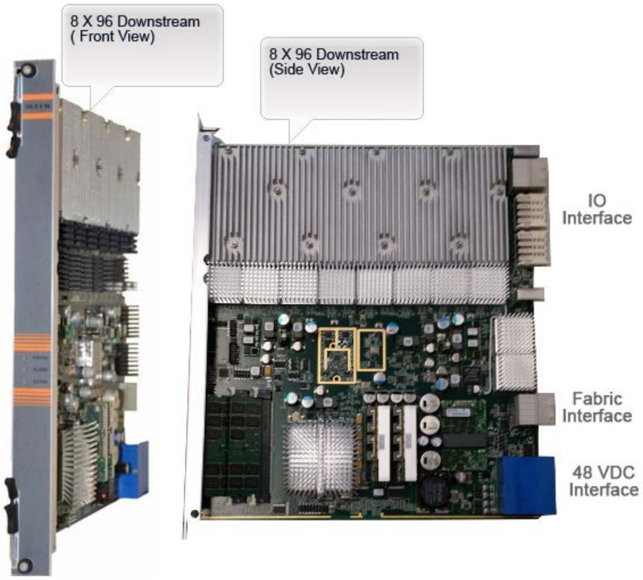
The UPS 32x4 I/O module is a revised version of the UPS 16x8 line card. The module operates with the Casa C100G and other platforms, including the C40G, and C10G CMTS. The 32-port I/O supports the MCX (micro coaxial) snap-on connectors on the CMTS side. Sixteen additional ports (16 to 31; 4 channels per port) are available for configuration after the UPS 32x4 I/O module upgrade. These connectors require quad-shielded adaptors, with MCX connectors on one end and standard 75 ohm F-connectors on the other end.

Casa also offers the UPS 32x4 I/O cable retention plate, to help you secure your connections.

2.3.6. RF SMM and LC Switch Modules

The C100G is equipped with a built-in RF switch architecture comprising four modules connected to an RF switch backplane. Using two SMM Switch and two LC Switch modules, these devices will process a dropped RF connection at a failed module by transferring the live traffic to the redundant failover module.

2.3.7. Architecture and Traffic Flow



Let’s describe the major hardware components of our downstream modules, using the 8x96 as our example.

The Network Processor is an ASIC that Casa Software interacts with to provide general purpose processing cycles, as well as specific hardware and network acceleration functions. The processor has XAUI interfaces to the switch fabric, and serial gigabit interfaces to the Field Programmable Gate Arrays (FPGAs).

Casa uses an FPGA design in our line cards, as opposed to traditional all-ASIC designs. This FPGA design enables Casa to address bugs and deliver feature upgrades in the DOCSIS PHY layer in the field. Casa saves the cost of doing ASIC spins, and encounters fewer design limitiations, due to the hardware in our downstream modules.

Finally, Digital Up Converters (DUCs) and Digital to Analog Converters (DACs) define frequency agility, modulation technique, and channel width of the digital and RF signals generated out the RF ports.

Traffic Flow on the Upstream Modules

Let’s describe the traffic flow on the upstream modules, using the Casa 16x8 module as our example.

Analog and digital front-end components perform tuning, automatic gain control, channel selection, analog-to-digital conversion, and related functions. Their purpose is to preprocess the signal, so that the individual QAM RF channels are available for further digital processing.

After this, the upstream card uses FPGA designs to implement upstream features such as Adaptive Equalizer. This feature compensates for channel effects, including group delay variation, amplitude slope, and micro reflections. It adapts its filter coefficients to dynamically varying channel responses so as to maximize the receive MER.

An ingress canceller is included in the Casa CCAP burst receiver to remove narrow band interference, such as commercial and private radio transmissions. It operates by dynamically detecting and measuring the interference, and adapting its coefficients to cancel the interfering carriers.

Also included in this stage is the Casa spectrum manager, which enables the operator to configure rules to adjust phy layer parameters of the received upstream based on unacceptable Noise or FEC activity.

In the next stage, Casa implements standard ASIC designs to perform de-interleaving, Reed-Solomon de-coding and MPEG de-framing.
Finally, the de-modulated and de-multiplexed frames are delivered to the Casa MAC FPGAs. The MAC layer controls the physical layer and is the source and sync of PHY data. The MAC layer processes data frames delineated by DOCSIS headers. These FPGAs are also responsible for the request grant scheduling mechanism which controls cable modem service flows.

Casa Switch Management Module (SMM)

The CCAP SMM is responsible for all redundancy, control, and data plane operations. Let’s discuss the major component architecture of the SMM.

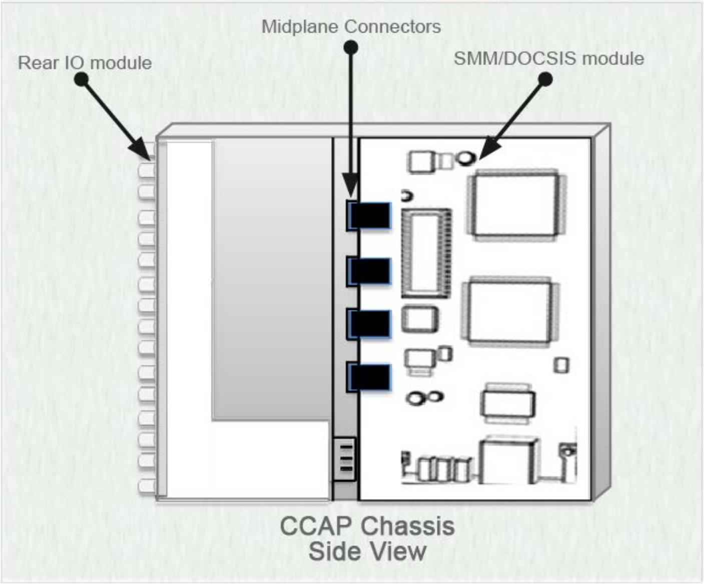
The Network Processor is a feature-rich general purpose processor, with application specific autonomous hardware accelerators and multiple on-chip interconnect options. The Processor enables integrated control plane, data plane, and security processing in a single System-on-a-Chip solution. The network processor connects to the switching components and the backplane through RGMII, SGMII, and XAUI interfaces.

For switching and routing of customer data there is a 10 gigabit multilayer switch. This switch provides many L2 L3 features, including ingress and egress ACLs, multi-tuple lookups, Layer 2 VLANs and Layer 3 tables, IPv4 and IPv6 Virtual Routing with full support for L2/L3 tunnels, trunking and QinQ, etc. Additionally, there is a gigabit switch to enable management traffic to and from the modules and backup SMM.

2.3.7.1. Video Presentation on Module Architecture

Click here for a video presentation on this topic.

2.3.8. Module Installation and Best Practices



Let’s describe some recommended best practices regarding hardware and chassis installation and configuration.

First, let’s describe the proper procedure to remove and install modules.

As already discussed, the rear and front modules are inserted into their slot, and meet at the mid-plane. At the mid-plane, there are several connectors that need to mate in order to establish proper connectivity through the chassis.

Removing and installing any front installed DOCSIS or SMM module is straight forward. Refer to the hardware installation guide for this procedure.

However, in the unlikely event that replacement of the rear installed I/O module is required, the order in which you proceed is important.

When removing the rear I/O, **ALWAYS** remove or loosen the front installed module first, and then remove the rear I/O module. When installing the the rear I/O, keep the front installed module loose or removed from the slot and (then) install and secure the rear I/O. Now you can install and secure the front installed module in its slot.

Further Guidelines

Here are a few other best practices regarding installation and maintenance of the CMTS chassis and modules.

- Ensure proper grounding of the chassis.
- Always be grounded to the chassis with static straps when handling modules.
- Ensure appropriate environmental temperature.
- Clean or replace the fan filter periodically.
- Install blank cards in empty slots to ensure optimal cooling through the chassis.
- When installing modules do not overtighten the captive thumb screws. Hand tight is sufficient.
- Power should be redundant with different sources, ideally with battery backup.
- If possible maintain spare modules. Spare modules should be keep in anti static bags when not in use.

2.3.8.1. Video Presentation on Module Installation

Click here for a video presentation on this topic.

2.4. Casa CMTS Software Operations

The Core software on the SMM, downstream and upstream modules is Linux. Software Modules on the Casa CMTS/CMTS are programmed and controlled by individual instances of the Linux kernel running on each of the module types, and are functionally isolated. Operationally, this means if a single process fails it only affects that one process.

In addition modules also load Casa Firmware, to identify each other, prepare for inter-module messaging and synchronize databases to produce a working CMTS/CMTS platform. For the C100G, there is a single software image that is compatible with all SMMs, downstream, and upstream modules.

System Management is enabled by, Casa CLI, SNMP and , IPDR. There is support for, DOCSIS, IETF and enterprise mibs and the most common IPDR templates Software processes responsible for system management shell.exe, SNMPD and IPDR.

Other major software processes are:

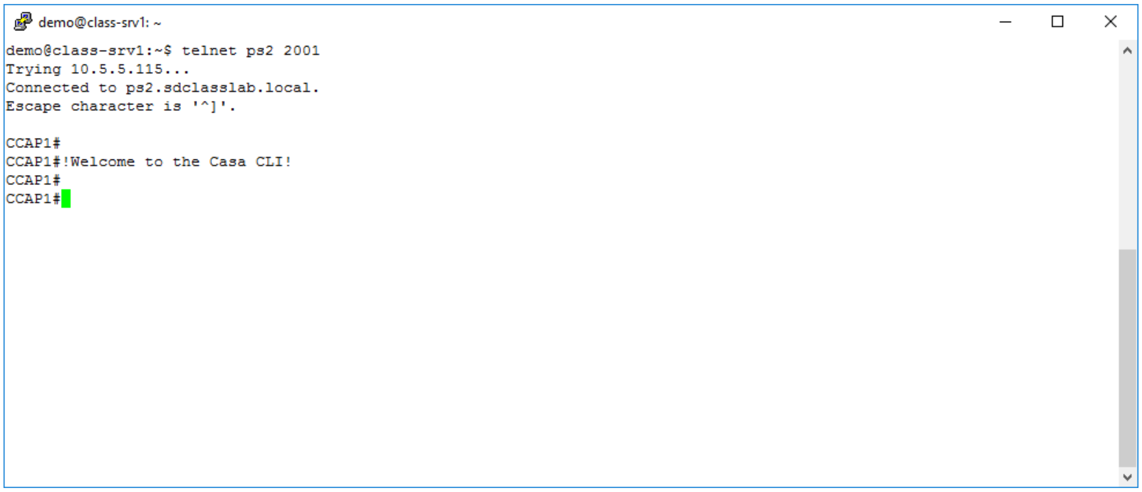
- System Management. System Management is responsible for monitoring and maintaining the state of the downstream and upstream modules as well as managing redundancy.
- The process that handles system management is lcsys manager. This software process reads system parameters via the I2C protocol, and monitors keep-alives across all modules and processes. The lcsys manager also initializes each DOCSIS Module and triggers and executes module failovers.
- CMTS/CMTS state is handled by the process cdb manager, on the SMM. System state information is stored on a block of shared memory and is cdp manager is responsible for maintaining the configuration state, of CPE and CM services for example, DOCSIS quality of service and packet cable multimedia flows.
- Device management and services management is handled by the ddm_rpc_server process on the SMM. This software process is responsible for the implementation of DOCSIS MAC domain configurations, such as, cm registration, load balancing, multicast, service flows and partial service.
- Data Path Downstream (DOCSIS MAC layer) The software processes for the downstream modules are essentially just performing packet processing for a variety of DOCSIS protocol implementations, such as subscriber management filtering , lawful intercept quality of service flows, BSoD, encryption etc. The FPGAs handle the BPI encryption, DOCSIS lower layer implementations like SYNC timestamp, DOCSIS PHY and the number of QAMs.
- Data Path Upstream (DOCSIS MAC layer) Just as in the downstream modules the software processes for the upstream modules are responsible for many of the same functions as the QAM daemon in the downstream. In addition, upstream path processing uniquely handles upstream quality of service flows, DOCSIS MAC fragmentation and reassembly, and PHY signal quality. The upstream

software also is involved in processing IP related functions that are redirected to the SMM, for example, ARP, TFTP proxy, and DHCP Lease Query.

2.4.1. Video Presentation on CMTS Software Operations

Click here for a video presentation on this topic.

2.4.2. Command Line Interface



```
demo@class-srv1:~$ telnet ps2 2001
Trying 10.5.5.115...
Connected to ps2.sdclasslab.local.
Escape character is '^]'.

CCAP1#
CCAP1#!Welcome to the Casa CLI!
CCAP1#
CCAP1#
```

Introduction

The Casa command-line interface (CLI) is the primary user interface used for configuring, monitoring, and maintaining Casa platforms. This user interface allows you to directly and simply execute Casa CLI IOS commands, whether using a console or terminal, or using remote access methods like ssh. The Casa CLI has a very similar structure to the Cisco IOS CLI; in fact, many commands are almost identical. So if you are familiar with Cisco command line syntax the Casa CLI will be familiar to you right away.

When you start a session, you generally begin in *user EXEC mode*, or *non enable mode*, which is one of two access levels of the EXEC mode. For security purposes, only a limited subset of EXEC commands are available in user EXEC mode. This level of access is reserved for tasks that do not change the configuration, such as running show commands.

In order to have access to all commands, you must enter *privileged EXEC mode*, or *enable* mode which is the second level of access for the EXEC mode. Normally, you must enter a password to enter privileged EXEC mode.The default username is *root* and the default password to enter privileged EXEC mode is *casa*.The user root is a special superuser and cannot be deleted. The system always has the user root and the password of this user can be changed by a superuser.

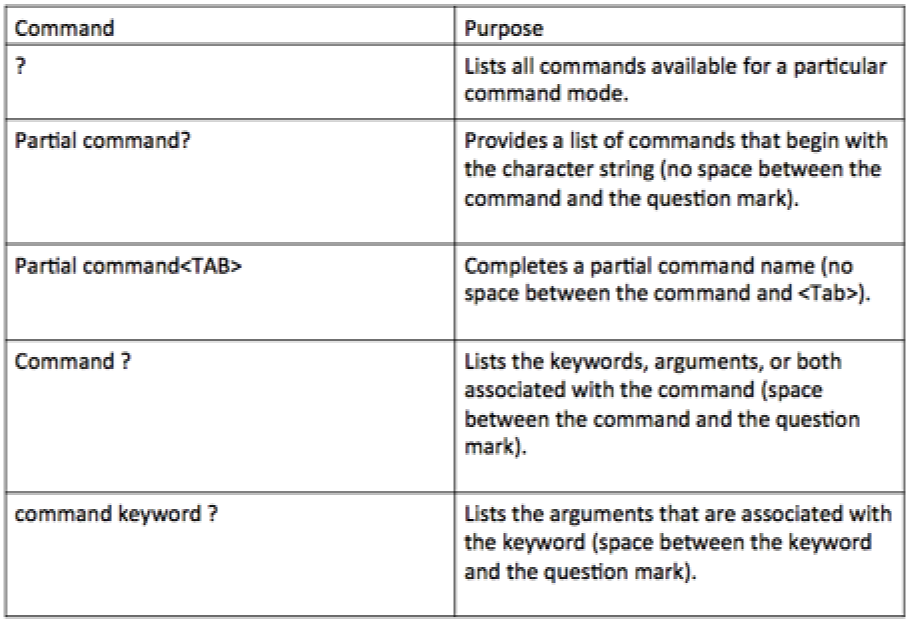
In privileged EXEC mode, you can enter any EXEC command, as the privileged EXEC mode is a superset of the user EXEC mode commands.

2.4.2.1. Video Presentation on the Casa CLI

Click here for a video presentation on this topic.

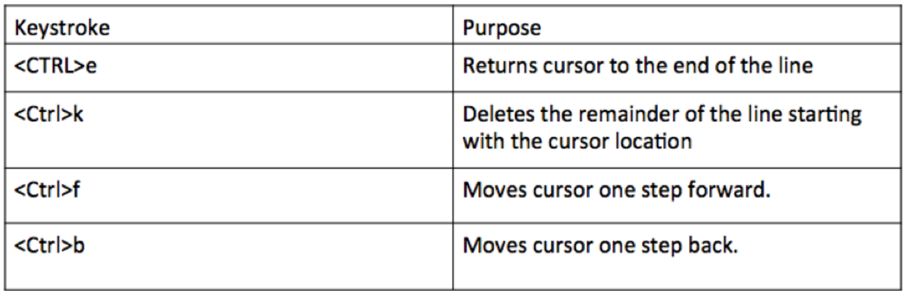
2.4.2.2. Using the Interactive Help Features

The Casa CLI includes interactive help features. The table below describes the purpose of the CLI interactive help commands.



Command	Purpose
?	Lists all commands available for a particular command mode.
Partial command?	Provides a list of commands that begin with the character string (no space between the command and the question mark).
Partial command<TAB>	Completes a partial command name (no space between the command and <Tab>).
Command ?	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
command keyword ?	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

In addition, the CLI responds to keyboard shortcuts to facilitate editing of commands.



Keystroke	Purpose
<CTRL>e	Returns cursor to the end of the line
<Ctrl>k	Deletes the remainder of the line starting with the cursor location
<Ctrl>f	Moves cursor one step forward.
<Ctrl>b	Moves cursor one step back.

2.4.2.2.1. Filtering output

The CLI also provides filtering commands to help with locating specific parameters of the output when the output is verbose. There are three ways to filter the output of the command.

- Built in CLI filters - these allow to include, exclude, count, count only and begin with the defined parameters.
- Less - This is the linux less command and less arguments can be used anytime the output of the command scrolls more than one screen. less commands can be entered at the colon prompt.
- Regular expressions - Regular expressions can be used at the CLI to filter output.

2.4.2.2.2. CLI Command Help Commands

The Casa CLI offers you several help features, many of which are described in the use case at the link below. Please note; this is not an exhaustive list; refer to Casa technical documentation as a further reference.

2.4.2.2.3. Video Use Case on Using the Interactive Help Features

Click here for a video use case on this topic.

The use case contains the commands below.

```
demo@class-srv1:~$ ssh root@ccap2
Password:casa
CCAP2>demo@class-srv1:~$ssh root@ccap2
Password:
CCAP2>enablePassword:casa
CCAP2#
```

```
Hit the TAB key to complete a command.
CCAP2#show cable modem verbose | include 5c35
MAC Address                                       :5c35.3b49.ac04
MAC Address                                       :5c35.3b4a.c236

<include><exclude><count><count only><begin>
<Ctrl>e – Returns cursor to the end of the line.
<Ctrl>k – Deletes the remainder of the line starting with the cursor
location.
<Ctrl>f – Moves cursor one character forward.
<Ctrl>b – Moves cursor one character back.

SUMMARY OF LESS COMMANDS
Commands marked with \* may be preceded by a number, N.
Notes in parentheses indicate the behavior if N is given.

  h  H                 Display this help.
  q  :q  Q  :Q  ZZ     Exit
----------------------------------------------------------------------------
 MOVING
  e  ^E  j  ^N  CR  \*  Forward  one line   (or N lines).
  y  ^Y  k  ^K  ^P  \*  Backward one line   (or N lines).
  f  ^F  ^V  SPACE  \*  Forward  one window (or N lines).
  b  ^B  ESC-v      \*  Backward one window (or N lines).
  z                 \*  Forward  one window (and set window to N).
  w                 \*  Backward one window (and set window to N).
  ESC-SPACE         \*  Forward  one window, but don't stop at end-of-file.
  d  ^D             \*  Forward  one half-window (and set half-window to N).
  u  ^U             \*  Backward one half-window (and set half-window to N).
  ESC-)  RightArrow \*  Left  one half screen width (or N positions).
  ESC-(  LeftArrow  \*  Right one half screen width (or N positions).
HELP -- Press RETURN for more, or q when done
CCAP2#show docsis channel utilization | i 11\/[8-9][.][0-3]|
Downstream               Total-BW    Utilization Online Secondary Channel
Slot/Port/Channel        (Mb/Sec)    Percentage  Modems Modems
Description
----------------------------------------------------------------------
0/0/0  (555000000 Hz)    42.9        1           1      0         FNB
<<output cut>>
0/1/6  (698000000 Hz)    55.6        1           0      0
0/1/7  (706000000 Hz)    55.6        1           0      0
```

2.4.2.3. CLI Global Commands

The Casa CMTS command line interface includes a few global commands in both enable and configuration modes. These commands include ones for configuring users, setting command aliases, resetting functions, pinging, telnetting, and tracerouting. The **show** commands are considered to be part of the global commands set.

Many of these global commands are described in the use case at the link below. Please note; this is not an exhaustive list; refer to Casa technical documentation as a further reference.

2.4.2.3.1. Video Use Case on CLI Global Commands

Click here for a video use case on this topic.

The use case contains the commands below.

```
alias <cmd_alias> <cmd_orig>
no alias <cmd_alias>

dig <string>

hostname <name>
[no] hostname <name>

ping <ip_addr>
ping6 <ip6_addr>
traceroute <ip_addr>
traceroute6 <ip6_addr>

reset password

show
```

2.4.2.4. CLI Modes

The use of specific commands allows you to navigate from one command mode to another. The standard order that a user would access the modes is as follows: user EXEC mode; privileged EXEC mode; global configuration mode; specific configuration modes; configuration submodes; and configuration sub submodes.

When you start a session, you generally begin in *user EXEC mode*, or *non enable mode*, which is one of two access levels of the EXEC mode. For security purposes, only a limited subset of EXEC commands are available in user EXEC mode. This level of access is reserved for tasks that do not change the configuration, such as running show commands.

In order to have access to all commands, you must enter *privileged EXEC mode*, or enable mode which is the second level of access for the EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. The default username is root and the default password to enter privileged EXEC mode is *casa*.The user root is a special superuser and cannot be deleted. The system always has the user root and the password of this user can be changed by a superuser.

In privileged EXEC mode, you can enter any EXEC command, as the privileged EXEC mode is a superset of the user EXEC mode commands.

From privileged EXEC mode, you can enter *global configuration mode*. In this mode, you can enter commands that configure general system characteristics. You also can use global configuration mode to enter specific configuration modes. Configuration modes, including global configuration mode, allow you to make changes to the running configuration.

From global configuration mode you can enter a variety of protocol-specific or feature-specific configuration modes. The CLI hierarchy requires that you enter these specific configuration modes only through global configuration mode.

From configuration modes, you can enter configuration submodes. Configuration submodes are used for the configuration of specific features within the scope of a given configuration mode.

Diag mode is another mode that contains specific diagnostic commands. The default password to enter diag mode is casadiag. Note this password cannot be changed. To exit and return to a mode up one mode type exit or end.

2.4.2.4.1. Video Use Case on CLI Modes

Click here for a video use case on this topic.

2.4.2.5. System Management Commands

The Casa CLI provides you with system management commands in enable and configuration mode. Generally speaking, these commands determine the behavior of the CMTS when you are connecting to it for management purposes. Please note; this is not an exhaustive list; refer to Casa technical documentation as a further reference.

2.4.2.5.1. Video Use Case on System Management Commands

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA (config)#banner login
End the input with a '.' (period) all by itself on a line

CASA# show banner login
************************************
* C10G-105/106 *
* 192.168.8.105 and 192.168.8.106 *
* Console SMM6: 192.168.8.136 2010 *
* Console SMM7: 192.168.8.136 2011 *
************************************

CASA (config)#console baudrate 9600

CASA (config)# console timeout <1:1440>

CASA (config)#device contact “<name>”
CASA (config)#device location “<location>”

CASA (config)#ftp-tftp source-interface loopback <0:255>
CASA (config)#ftp-tftp user-account <name> login <name> password <pwd>

CASA (config)#line vty <1:31>

CASA (config)#reset-console

CASA (config)#service password-encryption

CASA (config)#system monitor ?
cpu                   set cpu monitor
crash                 set application crash monitor
fan                   set fan monitor
memory                set memory monitor
nvram                 set nvram monitor
power                 set power monitor
```

```
temperature          set temperature monitor
watchdog             system monitor watchdog enable

CASA#telnet <ip_addr> [<1:65535>]
CASA#telnet vrf <name> [<ip_addr> [<1:65535>]]
```

2.4.3. Image and Configuration File Management

2.4.3.1. Upgrading the CMTS Image

1. Verify and remove any previously-installed software patches. Use the show patch command to determine if any patches have been applied to the software version you are presently running. If a software patch was previously installed, you MUST remove the patch prior to installing the new image.
2. Verify the boot loader image before installation.
3. Backup the current configuration. Prior to performing an upgrade copy the existing startup configuration file to a separate file for future use in situations where reverting to the current image may be necessary. This will allow the system to boot up to the earlier image without having to reconfigure the software.
4. Copy the new image to the CMTS:
    a. To update the application image, first download the image from the Casa FTP server to your FTP server.
    b. Copy the image to your CMTS. The supported storage device is nvram (non-volatile RAM).
5. Save the running configuration using the copy running-config startup-config command.
6. Set the boot device to the new image and then reboot the system. When the CCAP completes the series of boot-up processes, execute the show version command to verify the software update.

2.4.3.1.1. Video Use Case on Upgrading the CMTS Image

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show patch
CASA#system patch revert
```

```
CASA#remove patch <patch name>

CASA#show version
Running Image: SMM_8x10G Rel 7.2.3, Ver 0,build49e9, Thu Sep 29 19:00:58 EDT
2016,(relmgr)
Configured boot device: nvram
Image booted from: nvram, File name: ccsi.gz.rel7.2.3.0_build49e9
Casa RMI_BootLdr: Major 12, Minor 4 Build 11

PEER SMM VERSION:
Running Image: SMM_8x10G Rel 7.2.3, Ver 0,build49e9, Thu Sep 29 19:00:58 EDT
2016,(relmgr)
Configured boot device: nvram
Image booted from: nvram, File name: ccsi.gz.rel7.2.3.0_build49e9
Casa RMI_BootLdr: Major 12, Minor 4 Build 11
CASA#

CASA#copy nvram startup-config nvram <config name>

copy ftp <username> <ftp server ip address> <image name> nvram

CASA#copy ftp student1 10.4.1.3 ccsi.gz.rel7.2.3.0_build49e9 nvram

CASA#copy running-config startup-config

CASA#system bootdev nvram <image name>

CASA#system bootdev nvram ccsi.gz.rel7.2.3.0_build49e9

CASA#system reboot
```

2.4.3.2. Configuration File Management

When you use the CLI or Simple Network Management Protocol (SNMP) to create, edit, or modify the Casa CMTS configuration, the software maintains the most recent changes in the running configuration. The running configuration controls the current operational state of the CMTS. As you open system configuration objects and edit specific parameters, the CMTS applies the new settings to the system immediately.

When you complete the editing session and are satisfied with the changes that you made in the current session, you need to save the new running configuration to the default file named startup-config. The CMTS loads the startup-config file when it starts or reboots.

Copying the Running Configuration

The CMTS software allows you to copy and save the running configuration file to a uniquely named file at other target locations, including:

- NVRAM (non-volatile random-access memory)
- FTP targets
- TFTP targets

Backing Up the startup-config File

Use the **copy startup-config** command to save a version of the startup-config file to the CMTS NVRAM. Doing this makes a copy of the startup-config file available if you need to restore an earlier configuration.

Copying a Configuration File to the CMTS

You can use TFTP to copy a configuration file to NVRAM on the CMTS, with the **copy tftp** command.

Restoring the CMTS Configuration

If you need to cancel your latest configurations changes and revert to a previously saved configuration,your options depend upon the kind of configuration changes you have made.

The CMTS allows you to copy your startup-config file into running config. Note, however, that doing so does NOT overwrite the running config with the startup-config file. Rather, the CMTS **merges** the startup-config file into the current running configuration. This means:

- If your configuration session changes involve changing existing configurations on the CMTS, merging the startup-config file into the running config will overwrite those changes, and revert your configuration. In this situation you have two options. You can either copy startup-config to running-config, or you can reboot the CMTS to load the startup-config file.
- However, if your configuration session changes involve **adding** additional configurations to the existing running config, merging the startup-config file into the running config will NOT delete those changes. Your only option is to reboot the CMTS to load the startup-config file.

Maintaining Different Config Files on the CMTS

You can store different config files on the CMTS in NVRAM. To load a stored config file into the CMTS's running configuration:

- Backup the current startup-config file.
- Delete the startup-config file.
- Copy the config file you wish to load to startup-config.
- Reboot the CMTS.

2.4.3.2.1. Video Use Case on Configuration File Management

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#copy running-config startup-config

CASA# copy running-config ?
ftp                   use ftp protocol to put the file
ftp-account   use ftp protocol to put the file with defined
                                     ftp     account
nvram                 destination file location
startup-config        startup configuration
tftp                  use tftp protocol to put the file


Copy to FTP target:
CASA# copy run ftp <userid> <ftp IP address> <path/config file name>
CASA# copy run ftp myuserid 192.168.8.0 /cmtsfiles/configfile4_30_2015
Password: abc123

Copy to TFTP target:
CASA# copy run tftp <tftp IP address> <config file name>
CASA# copy run tftp 192.168.8.4 configfile4_30_15

Copy to NVRAM:
CASA# copy run nvram <config file name>
CASA# copy run nvram configfile4_30_15

CASA# copy startup-config nvram configfile1

CASA# copy tftp <host_ip> <file> <device>
CASA# copy tftp 10.4.1.3 golden_config nvram

To merge the startup-config with the current running config:
CASA# copy startup-config running-config

To completely erase the current configuration session:
CASA# system reboot

CASA# del startup-config
CASA# copy nvram <file name> nvram startup-config
CASA# system reboot
```

2.4.4. Local User Management

User management and security control provides the administrative levels for accessing and modifying aspects of the Casa CMTS. User management and security control is possible only by superusers in privileged (enable) mode. The privilege level of a user determines the access rights of the user to view, monitor, change, and maintain the CMTS configuration depending on the commands permitted for that user as determined by privilege commands. A superuser can perform all possible functions. While user management allows valid users to gain access to the system and maintain the status of the users, security control governs the specific actions performed by users.

Users can be added, deleted or modified. Users are assigned a privilege level during creation that can be modified later. The privilege level is a number from 1 through 15, with 1 being the lowest and 15 the highest level. The users with privilege level 15 are called superusers. You need to define the the privilege level of the user and assign the mode and the commands within that mode the user can execute.

2.4.4.1. Video Use Case on Local User Management

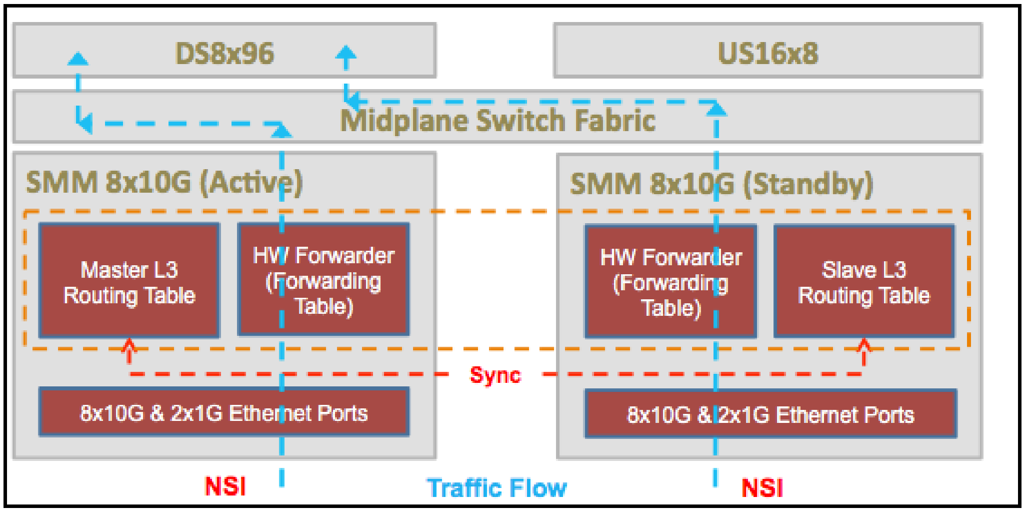
Click here for a video use case on this topic.

The use case contains the commands below.

```
CCAP1#show user
user root privilege 15 encrypted-password vQ5PNUDraqcgc
user docsismaint privilege 10 encrypted-password IJKvVWfO9HjjU
user videomaint privilege 9 encrypted-password 0bY.EumDUMb8Y
CCAP1#

CCAP1#show run | inc "privilege"
user root privilege 15 encrypted-password vQ5PNUDraqcgc
user docsismaint privilege 10 encrypted-password IJKvVWfO9HjjU
user videomaint privilege 9 encrypted-password 0bY.EumDUMb8Y
privilege exec level 10 "channel"
privilege exec level 10 "clear cable modem"
privilege exec level 10 "clear interface"
privilege exec level 10 "clear upstream"
privilege exec level 9 "config"
<<output cut>>

CCAP1#show user current
USER     TTY       TYPE     FROM              LEVEL     SINCE
```

```
----------------------------------------------------------------------------
root     console   console  local             15         Wed Sep 28 20:10:17
2016
ckent    pts/0     ssh      10.4.1.3          15         Wed Sep 28 20:24:45
2016

CCAP1(diag)#deluser ckent session pts/0

CCAP1#system message "Everyone logoff"
Broadcast message from croot (pts/1) (Wed Sep 28 20:38:53 2016):

Message to other users
CCAP1#
Broadcast message from croot (pts/1) (Wed Sep 28 20:38:53 2016):
Everyone logoff
```

2.4.5. High Availability Redundancy Introduction



Casa provides the ha commands in enable and configuration modes for high availability (HA) redundancy. The CMTS supports redundancy and switchover for the Switch and Management Module (SMM) and the DOCSIS line cards, using a combination of front- and rear-installed modules to switch existing RF connections from the module at fault to the redundant standby module for uninterrupted operation.

For redundancy to operate correctly, SMM and DOCSIS line cards must be installed into specific chassis slots, as follows:

- SMM – Slot 6 and Slot 7; install the redundant module in either slot; one will be active and the other will be the redundant standby.
- Downstream – Install the redundant line card in Slot 5 or in Slot 8.
- Upstream– Install the redundant line card in Slot 5 or in Slot 8.

Redundant QAM and UPS line cards installed in slots 5 and 8 must have capacities greater than or equal to the active modules in slots 0 to 4 and 9 to 13 with redundancy enabled. For example, installing a US16x2 upstream line card in redundant slot 5 will not process a US16x4 failover from any of the active slots. In this example, a matching US16x4 must be installed in slot 5 for a redundant failover to be successful.

At the rear of the system, there are two types of RF I/O switching modules that occupy slots 5, 6, 7, and 8.

- LC switch (rear slots 5 and 8) -- Operates with DOCSIS line-card module (either upstream or downstream) to provide N+1 redundancy. If a DOCSIS line-card module fails, a redundant DOCSIS line-card module automatically assumes operation. The LCS switch module cuts off the connection between failed module and its associated RF I/O module and establishes the traffic connection between the redundant and the RF I/O module. With the LC switch module, the front-installed line cards in slots 5 and 8 are available for redundancy operations.
- SMM switch (rear slots 6 and 7) — Operates with the front-installed SMM modules. If the active SMM module fails, the redundant SMM automatically assumes L3 routing operations. The SMM switch module cuts off the routing operations between the failed SMM to the upstream and downstream line-card modules and RF I/Os, and then transfers routing operations to the currently active SMM. These modules connect to the switching backplane and can be installed during system operation. There is no need to power down the CMTS for installation or removal.

Beginning with Casa software Release 6.5, two concurrent redundancy failovers are supported as long as the DS or UPS line card standby in slot 5 or in slot 8 is installed on the same chassis side as the failed line card. For example, UPS line card in slot requires the UPS standby in slot 5; DS line card in slot 11 requires the DS standby in slot 8.

2.4.5.1. Video Use Case on HA Redundancy

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show ha configuration
ha redundancy revert 30
ha redundancy 0,1,2,3,4,6,7,9,10,11,12,13
ha redundancy reboot
ha software auto-recovery

CASA#ha module 6 protect

CASA#ha module 13 revert

CASA#show ha log
time                ha         fail-type fail-sub-type fail take
description
                    type       type      type          slot slot
2016-08-18 17:02:30 SMM        MANUAL    MANUAL           7    6  manually
switch OK
2016-08-18 16:51:36 SMM        MANUAL    MANUAL           6    7  manually
switch OK
2016-08-08 13:43:04 QAM        HW FAIL   HW ERROR         0    5  DUC FIFO
UNDERRUN
<<output cut>>

CASA#ha replace linecard <slot number>
```

2.4.6. HItless Upgrade

The Casa CMTS lets you use its failover mechanisms to upgrade its firmware with minimal interruption to the traffic flow; a process called a “hitless upgrade.” In a hitless upgrade the CMTS begins by failing over the active SMM, then rebooting that now standby SMM to the new image. Once the previously active SMM comes up with the new image, the CMTS fails over the newly active SMM, and reboots that SMM to the new image. This results in both SMMs running the new image, with the original active SMM as the current active SMM.

The CMTS then follows a similar procedure with each of the line modules, individually failing them over and rebooting them to the new image.

This process ensures that when the upgrade is completed all your modules are in their original online or redundant statuses and are running the new image.

2.4.6.1. Video Presentation on Hitless Upgrade

Click here for a video presentation on this topic.

The presentation contains the commands below.

```
CMTS2#system hitless-upgrade ccsi.gz.rel7.2.5.2_build62aa
Verify hardware configuration..ok.
Verify boot image validity..ok.
Verify compatibility..ok.
Hitless upgrade from 7.2.5.2/build 6279.
Configuration has been changed. Do you want to save it before upgrading
(yes/no)?  yes
[Tue Mar  6 09:21:30 2018]-AL-CLI-1: smm6: User root copied running-
config to startup-config
Proceed with upgrade? please type YES to confirm :  yes
```

3. Verifying Configurations and Troubleshooting

Chapter Overview

In this chapter, we will cover diagnosing and troubleshooting issues through use cases to verify configurations and/or troubleshooting flow charts to assist in diagnosing problems.

Objectives

After successfully completing this chapter you will be able to:

- Verify your hardware configurations
- Follow a hardware troubleshooting flow chart
- View, filter, and manage log files
- Verify your DOCSIS PHY configurations
- Verify your MAC Domain configurations
- Perform Cable Modem diagnostics
- Verify your network side Layer 1 configurations
- Verify your network side Layer 2 configurations
- Verify your Layer 3 configurations

3.1. Troubleshooting Overview

3.1.1. Failure Domains

In situations where the system is not functioning, as it should, in other words, the system behaves differently than expected; the underlying cause is usually related to one or more of these three categories.

- Hardware failures.
- Software failures
- Configuration errors.

If Casa hardware and/or software are the suspected cause, the actions that can be taken to resolve the problem are limited. The detailed information necessary to pinpoint a Casa specific hardware or software problem is usually beyond the scope of the on site troubleshooter, and therefore the troubleshooting processes are generally executed as a joint effort with Casa support.

3.1.1.1. Video Presentation on Failure Domains

Click here for a video presentation on this topic.

3.1.2. General Troubleshooting Flow

The troubleshooting process begins with a report of a problem. Depending on your organizational structure, this report can be directly from the customer, or from another tier of your customer support organization. When the report is initially made the customer support engineer will be at least responsible for gathering information and perhaps some initial troubleshooting. Depending on the outcome of the first phase reporting and information gathering there may be an escalation required or the initial support engineer is responsible for full resolution.

In general, troubleshooting is the process that leads to a diagnosis and, if possible a resolution to the problem. Resolutions can be further broken down into permanent solutions, or temporary solutions. The latter, is often referred to as a workaround. Workarounds are a temporary solution that remedies the immediate symptom of a problem, whereas a permanent solution resolves the "root cause" of a problem. Finally, you implement the solution and proceed to either root cause analysis or confirm the permanent resolution.

3.1.2.1. Video Flow Chart on General Troubleshooting Flow

Click here for a video troubleshooting flow chart on this topic.

3.1.3. Network Best Practices

Think of problem reporting and resolution as the beginning and the end of the troubleshooting process. This is not where the technician or engineer spends most of their time. Usually most of the time is spent in the diagnostic phase. So lets look at the process of diagnosing a problem in more detail.

As a review, here are some minimum proactive best practices that should be implemented in any network to assist the troubleshooting process.

Configuration Management, backup configurations should be automatically created on a periodic basis and moved off the Casa platform to a backup server. This will help identify any changes that may have occurred since the last back up.

Control Plane Management, direct login to the platform should be limited. Management tools such as SNMP (read only) or homegrown back office services should be available, for the information gathering stage. Additional tools such as IPDR and Netflow are also commonly implemented.

Accounting, in order to maintain a command history per login commands run on the platform should always be recorded to a file on the management/jump server, or utilize accounting services like TACACS or Radius to record these sessions.

Authorization, local user permissions or authorization services like TACACS should restrict users based on their trust profile to commands that match the trust profile.

Logging, external syslog services should always be configured to capture Casa platform logging messages for analysis. When working in the CLI it is best practice to turn on debug messages, so any debug messages will be viewed in real time.

Network timeservers, for logging messages to be meaningful, it is vital to properly set and synchronize the clocks of the network devices. This ensures correct timestamps on logs, and supports other time-based features such as the use of certificates or time based access controls.

3.1.3.1. Video Presentation on Network Best Practices

Click here for a video presentation on this topic.

3.1.4. Troubleshooting Best Practices

Lets describe some first principles and best practices while troubleshooting.

1. Run the show running config command and check the last configuration and last write to NVRAM. If the last configuration change is around the time the problem presented, you should try to determine what changed. For example, execute a diff on the last known good backup file, and the current running configuration.
2. Check the logs. Check syslog for changes and last logins and error messages. Determine, as well as you can, when the error began to occur. Determine whether the error messages give you any information about the cause of the problem. Determine whether there was a configuration change at the time the error began. Determine whether someone was logged into the device at the time the error began.
3. Identify the problem. Be very disciplined about this step; ensure that you are identifying the problem itself, and not the probable cause of the problem. If a internal user is involved, question the user and identify any changes they may have made. It is a good idea to backup your configuration at this stage, in the event you need to make configuration changes for testing, this will give you a rollback option. Consider a probable cause for the failure. Of your list of possible causes, choose the cause you consider most probable. Be sure to test only one cause at a time.
4. Create a plan to address your probable cause. Analyze your plan for unintended consequences. If you have peers, brainstorm with them about the possible impacts your solution may have. Be sure to test only one cause at a time.
5. Execute your plan. While doing this keep the following points in mind.
6. Do not make any changes you cannot recover from.
7. Make one change at a time.
8. If your plan involves multiple changes, order them based upon their impact on your users. Make the change that will have the least impact on your users first. Observe the results of executing your plan. Have you solved the problem if necessary repeat this process.
9. Document your changes! Keep a troubleshooting log, and update your ticket or predefined internal process with the information in this log, at a minimum the information should include:
   - The problem
   - The symptoms the problem created
   - Samples of the log entries
   - The plan you developed to solve the problem
   - What parts of the plan worked and did not work
   - The effects your solution had on your network

3.1.4.1. Video Flow Chart on Troubleshooting Best Practices

Click here for a video troubleshooting flow chart on this topic.

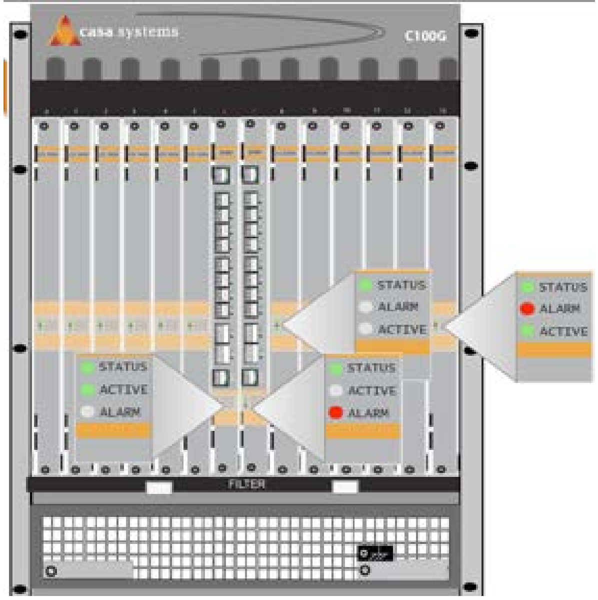
3.2. Hardware Troubleshooting

You can use a number of generic commands to diagnose performance- related hardware issues on the Casa CLI. Even if you don't have access to the CLI there are certain visual inspection tests that can be performed to help you diagnose hardware related issues.

3.2.1. Video Presentation on C100G Hardware Troubleshooting

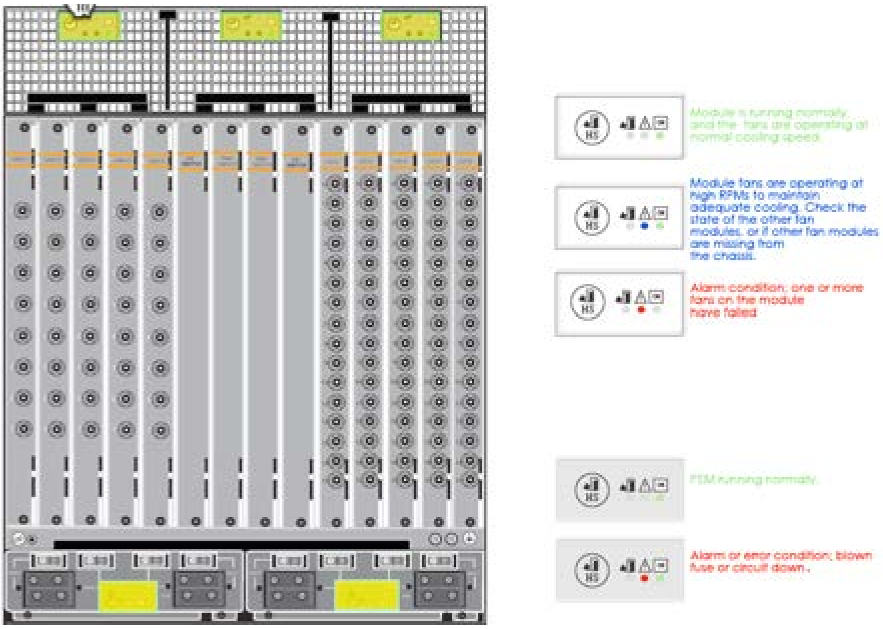
Click here for a video presentation on this topic.

3.2.2. Using the LEDs for Diagnostics



All the upstream, downstream and SMM module LEDs are labeled Status, Active, and Alarm. No LED illumination indicates no power, or system off, condition. In an SMM redundant configuration, a normal condition for the SMM modules is the Primary SMM, usually module 6, will have the Status and Active LED green and the backup SMM, usually module 7, will have only the status LED green. In an RF redundant configuration, a normal condition for the line cards in slots, 0 through 4, and 9 through 13 is the Status and Active LED are green and the backup line cards in slots 5 and 8 the status LED is green.

Finally, when a fault is detected the Alarm LED will be Red. Note this alarm could be of a critical or non critical nature. It is recommended the alarm be checked through a management interface before performing any hardware replacement to confirm the nature of the alarm.


HS
Module is running normally, and the fans are operating at normal cooling speed.
Module fans are operating at high RPMs to maintain adequate cooling. Check the state of the other fan modules, or if other fan modules are missing from the chassis.
Alarm condition; one or more fans on the module have failed
PEM running normally.
Alarm or error condition; blown fuse or circuit down.

The other system LEDs are located on the rear of the Chassis, for the Fans and the Power entry Modules. There are only two LEDs that are active, the OK LED and the Caution LED. The Caution LED is the triangle with an exclamation point.

For the fan LEDs, green means the fan module is running normally, and the fans are operating at normal cooling speed. A blue Caution LED, means the Module fans are operating at high RPMs to maintain adequate cooling. Check the state of the other fan modules, or if other fan modules are missing from the chassis.

A Red caution LED, means an Alarm condition, one or more fans on the module have failed.

For the PEMs, a green OK LED means the PEM is running normally. A Red caution LED means the PEM has an alarm or error condition possibly a blown fuse or circuit down.

3.3. Diagnostic Tools

There are several diagnostic tools availed to you in the Casa CLI.

3.3.1. Debugging

Show commands can tell you many things about what is going on in terms of verifying proper configuration but they can't tell you everything. For example, show commands cannot tell you when routes drop in or out of the routing table, whether a packet really went out the router, or what ICMP error code was received. On the other hand, the debug commands can tell you all these things, and more. Please note: Because debugging output is assigned high priority in the CPU process, it can render the system slow or worse case unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Casa support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users or maintenance windows if possible. Debugging during these periods' decreases the likelihood that increased debug command processing overhead will affect system use.

3.3.1.1. Video Use Cases on Enabling Debugging

Click here for a video use case on this topic.

The Enabling Debugging on VTY use case contains the following commands:

```
CCAP1#no logging
CCAP1#logging debugging
CCAP1#
CCAP1#debug ?
aaa                 aaa debug support
arp                 ARP
bfd                 Bidirectional Forwarding Detection (BFD)
cable               debug cable plant
ddm                 all level debugging trace in ddm
igmp                internet group management protocol
ip                  IP information
ipv6                IPv6 information
isis                IS-IS information
lacp                LACP protocol
ldp                 Label Distribution Protocol (LDP)
nsm                 Network Service Module (NSM)
rsvp                Resource Reservation Protocol (RSVP)
scs                 scs command
video               video configuration
```

```
CCAP1#debug isis all
This may severely impact network performance !!!   Continue? (yes/[no]): yes
[Wed Aug 31 17:19:59 2016]-IN-CLI-1: smm6: update config last changed or
saved time 2016-08-31 17:19:59

CCAP1#show debugging
SMM 6 debugging status
ISIS debugging status:
  IS-IS Interface FSM debugging is on
  IS-IS Neighbor FSM debugging is on
  IS-IS events debugging is on
  IS-IS PDU debugging is on
  IS-IS lsp debugging is on
  IS-IS spf debugging is on
  IS-IS NSM debugging is on
  IS-IS MPLS debugging is on
  IS-IS BFD debugging is on

CCAP1#no debug isis all
[Wed Aug 31 17:24:57 2016]-IN-CLI-1: smm6: update config last changed or
saved time 2016-08-31 17:24:57

CCAP1#show debugging
SMM 6 debugging status

CCAP1#no debug isis all
[Wed Aug 31 17:21:16 2016]-IN-CLI-1: smm6: update config last changed or
saved time 2016-08-31 17:21:16
```

The Enabling Debugging from the Console use case contains the following commands.

```
CCAP1#debug ?
aaa                aaa debug support
arp                ARP
bfd                Bidirectional Forwarding Detection (BFD)
cable              debug cable plant
ddm                all level debugging trace in ddm
igmp               internet group management protocol
ip                 IP information
ipv6               IPv6 information
isis               IS-IS information
lacp               LACP protocol
ldp                Label Distribution Protocol (LDP)
nsm                Network Service Module (NSM)
rsvp               Resource Reservation Protocol (RSVP)
scs                scs command
video              video configuration

CCAP1#debug isis all
This may severely impact network performance !!!   Continue? (yes/[no]): yes
[Wed Aug 31 17:19:59 2016]-IN-CLI-1: smm6: update config last changed or
saved time 2016-08-31 17:19:59
CCAP1#

CCAP1(config)#logging system debugging
[Wed Aug 31 17:15:30 2016]-IN-CLI-1: smm6: update config last changed or
saved time 2016-08-31 17:15:30
CCAP1(config)#

CCAP1#no debug isis all
```

```
[Wed Aug 31 17:21:16 2016]-IN-CLI-1: smm6: update config last changed or
saved time 2016-08-31 17:21:16
CCAP1#

CCAP1#show debugging
SMM 6 debugging status
ISIS debugging status:
  IS-IS Interface FSM debugging is on
  IS-IS Neighbor FSM debugging is on
  IS-IS events debugging is on
  IS-IS PDU debugging is on
  IS-IS lsp debugging is on
  IS-IS spf debugging is on
  IS-IS NSM debugging is on
  IS-IS MPLS debugging is on
  IS-IS BFD debugging is on

CCAP1#no debug isis all
[Wed Aug 31 17:24:57 2016]-IN-CLI-1: smm6: update config last changed or
saved time 2016-08-31 17:24:57

CCAP1#show debugging
SMM 6 debugging status

CCAP1#
CCAP1(config)#no logging system
CCAP1(config)#
```

3.3.2. Showing and Managing Log Files (inc. Interpreting and Filtering Log Messages)

There are several logging tools in the Casa CLI that you can use to diagnose and gather information in the troubleshooting process. These are:

System Logs - It is standard best practice to look at the logs of any network device as a starting point in when gathering information as part of the troubleshooting process. The logs can immediately tell you who and when the last person logged in as well as the last configuration change on the system. The logs can also indicate specific errors to aid you and or Casa support personnel to narrow your problem to root cause.

3.3.2.1. Logging Levels

You should always include checking the logs as part of your troubleshooting skills. Logging levels determine the severity of the information that is collected in the log file; you can set the logging levels as needed. The table below lists the logging levels on the DAA and the corresponding keywords used to set the logging levels for these types of messages. Level 0, emergencies, is the highest level and logs only the most serious errors. Level 7, debugging, is the lowest level. Level 7 logs include the most messages because Level 7 logs include messages from all levels.

Level	Keyword	Description	SYSLOG Definition
0	Emergencies	System unusable	LOG_EMERG
1	Alerts	Immediate action necessary	LOG_ALERT
2	Critical	Critical conditions exist	LOG_CRIT

3	Errors	Error conditions exist	LOG_ERR
4	Warnings	Warning conditions exist	LOG_WARNING
5	Notification	Normal, but significant conditions	LOG_NOTICE
6	Informational	Information messages	LOG_INFO
7	Debugging	Debugging messages	LOG_DEBUG

The command **user log exclusion-list** may be used to selectively disable logging of certain message levels from specified users. Messages associated with the specified log level (and all lower severity levels) for the specified user are disabled and will not be logged. This functionality keep unnecessary messages from filling up the log file.

The CMTS platform supports reporting of collected system logs to as many as 16 different syslog servers. Access to syslog servers are provided through the management interface. Separate logging levels can be configured for various log collection methods. You can direct messages processed to a specified target destination. The target can be a remote SYSLOG host, the system console display, volatile or non-volatile memory, or a loopback interface.   For each logging target, you need to specify the type of message based on a severity level. The system log file capacity is 1 MB. Optional feature logging level selection is supported for all available methods of log collections including the following:

- non-volatile: logging level for local log on non-volatile memory (flash memory)
- syslog: logging level for syslog receiver
- system: logging level for console output
- trap: logging level for trap
- task: logging level for task
- volatile: logging level for local log on volatile memory

3.3.2.2. Video Use Case on Showing and Managing Log Files

Click here for a video use case on this topic.

The use case contains the commands below:

```
CCAP1#show logging all
  /dev/console    :    errors
  system log level    :    errors
  non-volatile log level    :    warnings
  volatile log level    :    off
  syslog level    :    warnings
  trap level    :    off
  system syslog host:10.4.1.3

CCAP1#show log
CCAP1#show log | inc "fail"
[Mon Aug 29 18:11:25 2016]-ER-SYS-1: smm6: Slot 5 failed to become startup
after 3 tries
[Mon Aug 29 18:06:07 2016]-ER-SYS-1: smm6: Slot 5 failed to become startup,
reboot
[Mon Aug 29 18:05:34 2016]-ER-SYS-1: smm6: System rebooting module 0,fail
reason HW ERROR
-output cut-

CCAP1#dir fdsk2
total 2539
-rw-r--r-- 1 croot  root     323964 Apr 26 17:43 bcm_congestion_debug0
-rw-r--r-- 1 croot  root      23460 Aug 29 17:58 cdb.log
-rw-rw-rw- 1 croot  root      34676 Jun 15 13:20 docsislogfile
-rw-rw-rw- 1 croot  root      36608 May 24 00:30 docsislogfile.old
-rw-rw-rw- 1 croot  root      41999 Aug 29 18:06 edge.log
-rw-r--r-- 1 croot  root      42511 Aug 29 18:12 ha_log
-rw-r--r-- 1 croot  root      65621 Aug 27 18:50 ha_log.bak
-rw-rw-rw- 1 nobody nogroup   87612 Apr 26 17:43 lcsysmgr_lc13_debugLocal0
-rw-r--r-- 1 croot  root     480203 Aug 30 14:11 logfile
-rw-r--r-- 1 croot  root     410858 Aug 18 16:57 logfile.bak
---------x 1 croot  root    1048681 Aug 18 16:57 logfile.old
Filesystem            Size  Used Avail Use% Mounted on
/dev/mtdblock4         24M  1.4M   23M   6% /fdsk2

CCAP1#copy fdsk2 logfile.bak tftp 10.4.1.3
putting /fdsk2/logfile.bak to 10.4.1.3:logfile.bak [octet]


CCAP1#show cable event notification-policy
priority      flash-log  mem-log  traps    syslog
-------------------------------------------------
emergency     yes        no       no       no
alert         yes        no       no       no
critical      yes        no       yes      yes
error         yes        no       yes      yes
warning       no         yes      yes      yes
notice        no         yes      yes      yes
informational no         no       no       no
debug         no         no       no       no
CCAP1#
```

3.3.2.3. Interpreting Log Messages

The CMTS generates log messages based on severity to one or more configured logging targets, such as a designated host, syslog server, system memory, or to the system console. By default, log messages are saved in the CMTS top-level directory in the file named **logfile**.

Messages are generated by the many subsystems (hardware and software components) that run on the CMTS platform. These subsystems monitor and communicate with other subsystems to determine the operational status of the system, the current state of the installed hardware, networking status over Ethernet links, and in redundant systems, changes to the current roles of the hardware if a failover has occurred. These subsystems then report status by generating and sending messages to their configured logging targets.

Each logged message is prefixed by the date and time of the event, the subsystem delivering the event, followed by message text.

It is standard best practice to look at the logs of any network device as a starting point in when gathering information as part of the troubleshooting process. The logs can immediately tell you who and when the last person logged in as well as the last configuration change on the system. The logs can also indicate specific errors to aid you and or Casa support personnel to narrow your problem to root cause.

3.3.2.4. Video Use Case on Interpreting and Filtering Log Messages

Click here for a video use case on this topic.

The use case contains the log messages and CLI commands below.

```
User <name> rebooting module <num>
System rebooting module <num>, fail reason REBOOT LC

Related commands:
(diag)# show module <num> active-status
show module <num> {shared-channel | ts}
show ha log
show running-config
show system
show chassis status
```

```
User <name> copied running-config to startup-config

Related commands:
show running-config
show startup-config
show log

GigE port <slot>/<port>, link is up
GigE port <slot>/<port>, link is down

Related commands:
show interface gige
show interface xgige
show this (from the interface configuration mode)
show log | inc shutdown
ping <ip_addr>

Module <num> QAM, in boot state
Module <num> QAM, is up
Module <num> UPS, in boot state
Module <num> UPS, is up

Related commands:
show system
show chassis status

cfg_recover_qam():xx: pid = x, tid = x, err = Success.
recovering config from dbid x database x entries …
cfg_recover_ups():xxx: pid = xxx, tid = xxx, err = Success.
recovering config from dbid xx database x entries …

Related commands:
(diag)# show module <num> active-status
show module <num> {shared-channel | ts}
show system
show chassis status
show running-config

Fan tray <number> back fan low RPM detected (2200 RPM). Check fan intake and
exhaust for blockage. Replace fan tray if defective

Fan tray <number> front fan low RPM detected (0 RPM). Check fan intake and
exhaust for blockage. Replace fan tray if defective

Fan tray <num> back fan speed is back to normal (2500 RPM) and
functional again.

Related commands:
show envm fan {left | middle | right}
show envm temperature [module | qam | smm | ups]
show system
show system monitor threshold fan
system monitor fan enable

Fan tray <num> is pulled out or broken

Related commands:
show envm fan {left | middle | right}
show system
show system monitor threshold fan
show system monitor threshold temperature
system monitor fan enable
```

```
QAM switchover trap notification (HA auto revert, module <num>
gave back, module <num> takes over)
UPS switchover trap notification (HA auto revert, module <num>
gave back, module <num> takes over)

Related commands:
show system
show chassis status
show log
show ha configuration

<username> is not authenticated by the AAA server!

Related commands:
show aaa
ping

no kex alg

CCAP1#show log | inc AL-SYS-1
[Fri Apr  7 14:34:12 2017]-AL-SYS-1: smm6: Module  2 changed to active
status
[Fri Apr  7 14:34:03 2017]-AL-SYS-1: smm6: Module 2 (QAM_8x192) is up
[Fri Apr  7 14:33:25 2017]-AL-SYS-1: smm6: Module  0 changed to active
status
[Fri Apr  7 14:33:21 2017]-AL-SYS-1: smm6: Module  5 changed to standby
status
[Fri Apr  7 14:33:21 2017]-AL-SYS-1: smm6: Module 5 (QAM_8x96) is up
[Fri Apr  7 14:33:20 2017]-AL-SYS-1: smm6: Module 0 (QAM_8x96) is up
-output cut-

CCAP1#show log | inc ER-
[Fri Apr  7 14:42:34 2017]-ER-SYS-1: smm6: Slot 1 failed to become startup
after 3 tries
[Fri Apr  7 14:37:33 2017]-ER-SYS-1: smm6: Slot 1 failed to become startup,
reboot
[Fri Apr  7 14:32:31 2017]-ER-SYS-1: smm6: Slot 1 failed to become loading,
reboot
-Output cut-


[Mon Aug 22 01:18:01 2016]-ER-RPC-1: smm6: lc_cfg_prog_2(): pid 695, module
13,mtype 10005, status 2, rpc call failed: RPC: Timed out
```

3.3.3. Verifying Connectivity - Layer Two and Three

Casa CLI has standard diagnostic tools to allow you to diagnose Layer 2 and Layer 3 connectivity. These are:

ping DOCSIS – Pings a DOCSIS modem, specified by its IPv4, IPv6 or MAC address. If you ping by MAC address this command will send three station maintenance opportunities to the modem.

extended ping - An extension to the common ping command. Extended ping is used to perform a more advanced check of host reachability and network connectivity. The extended ping command works only in enable mode. The normal ping works both in the user non-enable mode and enable mode.

traceroute -Where ping can be used to verify connectivity between devices, the traceroute command can be used to discover the paths packets take to a remote destination, as well as where routing breaks down. The purpose behind the traceroute command is to record the source of each ICMP "time exceeded" message in order to provide a trace of the path the packet took to reach the destination.

arp and **IPv6 neighbor** - although these are not utilities in and of themselves, they are part of the show commands. For IPV4 if there are not the proper entries in the ARP cache there is no connectivity between IPv4 hosts and or next hop devices. Because the IPv6 protocol does not use ARP, the IPv6 neighbor table serves the same function as the ARP table did for IPV4. You should always check these tables as part of troubleshooting connectivity in the network.

3.3.3.1. Video Use Case on Verifying Layer 2 Layer 3 Connectivity

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#ping repeat 20 size 84 source ip-bundle 1 ttl 5 10.4.1.3
PING 10.4.1.3 (10.4.1.3): 84 bytes of data.
92 bytes from 10.4.1.3: icmp_seq=0 ttl=62 time=1.790 ms
92 bytes from 10.4.1.3: icmp_seq=1 ttl=62 time=2.064 ms
92 bytes from 10.4.1.3: icmp_seq=2 ttl=62 time=2.078 ms
92 bytes from 10.4.1.3: icmp_seq=3 ttl=62 time=2.072 ms
<<Output Cut>>

CASA#ping quiet 10.4.1.3
PING 10.4.1.3 (10.4.1.3): 56 bytes of data.
--- 10.4.1.3 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.869/1.992/2.083/0.090 ms


CASA#ping docsis 192.168.3.103 verbose
PING DOCSIS 5c35.3b2f.67d3
RNG-REQ from 5c35.3b2f.67d3 8 ms, p-offset=2, f-offset=-39, t-offset=0
RNG-REQ from 5c35.3b2f.67d3 13 ms, p-offset=3, f-offset=-39, t-offset=0
RNG-REQ from 5c35.3b2f.67d3 10 ms, p-offset=3, f-offset=-39, t-offset=0
RNG-REQ from 5c35.3b2f.67d3 12 ms, p-offset=2, f-offset=-39, t-offset=1
RNG-REQ from 5c35.3b2f.67d3 11 ms, p-offset=3, f-offset=-39, t-offset=-1
--- 5c35.3b2f.67d3 ping docsis statistics ---
5 station maintanence scheduled, 5 RNG-REQ received 100% success

CASA#show arp
Interface    Age      Hardware Addr  State   Type IP Address
CATV-MAC 1  00:00:01 0000.0001.0000 static  ARPA 172.16.1.1
CATV-MAC 1  00:00:03 5c35.3bac.c173 dynamic ARPA 172.16.1.120
CATV-MAC 1  00:00:01 0000.0001.0000 static  ARPA 172.16.11.1
CATV-MAC 1  00:00:01 0000.0001.0000 static  ARPA 192.168.1.1
CATV-MAC 1  00:00:03 5c35.3bac.c0df dynamic ARPA 192.168.1.61
<<output cut>>

traceroute to casalabs.training (198.0.133.50), 64 hops max, 40 byte packets
 1  10.3.11.5  0.850 ms
 2  10.5.5.5  1.810 ms
<<output cut>>

CASA#ping6 repeat 10 size 84 source ip-bundle 1 ttl 5 fdf6:556d:f7e3:7adf::3
PING fdf6:556d:f7e3:7adf::3 (fdf6:556d:f7e3:7adf::3): 84 data bytes
92 bytes from fdf6:556d:f7e3:7adf::3: icmp_seq=0 ttl=62 time=1.762 ms
92 bytes from fdf6:556d:f7e3:7adf::3: icmp_seq=1 ttl=62 time=1.087 ms

CASA#show ipv6 neighbor
Interface    Hardware Addr  State           IP Address
CATV-MAC 1  0017.1088.ad82 reachable-local fd8c:ad35:46e5:461d::1
<<output cut>>
CATV-MAC 1  5c35.3b4a.a0f6 delay           fd8c:ad35:46e5:461d::c904:9a07
CATV-MAC 1  5c35.3bac.bfc7 delay           fd8c:ad35:46e5:461d::cbf6:6c3e
CATV-MAC 1  5c35.3bac.ae55 delay           fd8c:ad35:46e5:461d::fe44:2347
CATV-MAC 1  0017.1088.ad82 reachable-local fe80::217:10ff:fe88:ad82
<<output cut>>
```

3.3.4. TCPdump and Cable Mirror

TCPdump - TCPdump is a common packet analyzer that runs under the Casa CLI. It allows the user to display TCP/IP and other packets being transmitted or received over the CMTS/CMTS gige and Line card modules interfaces. The Casa tcpdump accepts all the same arguments as unix tcpdump, however, these arguments need to escaped with quotes. Example: *CMTS1(diag)#tcpdump "-c 100 -i lc0 -w /fdsk/dumptest -U".* Here the trace will capture 100 packets (-c) on interface lc0 or slot 0 and write it to a file on nvram called dumptest. The -U argument buffers the output of the file to write to the file line by line rather than waiting for the buffer to fill.

Cable Mirror- The Casa CLI employs a packet trace feature that enables you to capture traffic from specified cable modems to help troubleshoot DOCSIS or RF network issues.

3.3.4.1. Video Use Case on TCPdump and Cable Mirror

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA(diag)#tcpdump "-c 100 -i lc0 -w /fdsk/dumptest -U"
*****   Type Ctrl-C to exit   *****
tcpdump: listening on lc0, link-type EN10MB (Ethernet), capture size 262144
bytes
100 packets captured
104 packets received by filter
0 packets dropped by kernel

CASA(diag)#tcpdump "-r /fdsk/dumptest"
*****   Type Ctrl-C to exit   *****
reading from file /fdsk/dumptest, link-type EN10MB (Ethernet)
19:36:37.093055 00:00:00:1c:80:00 (oui Ethernet) > 00:00:00:1c:00:ff (oui
Ethernet), ethertype Unknown (0x0998), length 60:
       0x0000:  0001 0005 4ba4 0601 c408 1122 3344 0000  ....K......"3D.
<<output cut>>


CASA(diag)#mirror cm traffic 127.1.1.7 5c35.3b49.ac04
Mirroring traffic for MAC 5c.35.3b.49.ac.04 ff.ff.ff.ff.ff.ff
to 7f010107 fr idx=-1 00000000  f=3 us_id=0 ds_id=0
CCAP2(diag)#
```

```
CASA(diag)#tcpdump "-i eth2 port 0xcace or udp port 0xcacf -xx -s 0 -w
/fdsk/cm_capture.pcap"
*****   Type Ctrl-C to exit   *****
tcpdump: listening on eth2, link-type EN10MB (Ethernet), capture size 262144
bytes
8 packets captured
8 packets received by filter
0 packets dropped by kernel
```

3.3.5. Verifying System Utilization

Before you escalate a problem to support, it is prudent to check your system resources. The symptoms of overtaxed system resources can include a system where the CLI is slow or unresponsive, or control plane traffic (like DHCP) timing out for modems, or routing protocol flapping.

Possible root causes for these symptoms could be over utilization of cpu resources due to internal (software bug) or external (DOS attacks) factors.

3.3.5.1. Video Use Case on Verifying System Utilization Statistics

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show cpu-process
CASA#show cpu-process | in ospf
UID        PID  PPID   LWP  C NLWP STIME TTY         TIME        CMD
croot      830     1   830  0    3 Sep08 ?        00:01:02 /casa/bin/ospfd -
d
croot      830     1   861  0    3 Sep08 ?        00:00:03 /casa/bin/ospfd -
d
<<Output Cut>>

CASA#show cpu-memory process-list
CASA#show cpu-memory process-list
SMM CPU and Memory information:
COMMAND             PID USER        %CPU   %MEM
init                  1 croot       0.00   0.02
kthreadd              2 croot       0.00   0.00
<<Output Cut>>
12:55:38 up 12 days,  3:00,  0 users,  load average: 15.16, 15.11, 15.02
85188908 processes: 83819821 sleeping, 1368751 running, 317 zombie, 0
stopped
CPU states:   0.0% user,   3.5% system,   0.4% nice,   95.9% idle
Mem:   1996616K total,   982540K used,   1014076K free,   240076K buffers

CASA(diag)#show bcm throughput
Bcm 0 , rx pkt rate: 0, rx byte rate: 0
        tx pkt rate: 0, tx byte rate: 0
Bcm 1 , rx pkt rate: 0, rx byte rate: 0
        tx pkt rate: 0, tx byte rate: 0
Bcm 2 , rx pkt rate: 0, rx byte rate: 0
        tx pkt rate: 0, tx byte rate: 0
Bcm 3 , rx pkt rate: 0, rx byte rate: 0
        tx pkt rate: 0, tx byte rate: 0
Bcm 4 , rx pkt rate: 0, rx byte rate: 0
        tx pkt rate: 0, tx byte rate: 0
<<Output Cut>>
Bcm 21, rx pkt rate: 0, rx byte rate: 0
        tx pkt rate: 0, tx byte rate: 0
Bcm 22, rx pkt rate: 1, rx byte rate: 64
        tx pkt rate: 0, tx byte rate: 0
Bcm 23, rx pkt rate: 0, rx byte rate: 0
        tx pkt rate: 0, tx byte rate: 0
Bcm 24, rx pkt rate: 0, rx byte rate: 0

CASA#(diag)#show datapath-config smm-pkt-counts
ttl=3226638 special=4 lc_tftp=0 lc_igmp=0 (0 0)
<<Output Cut>>
SMM ARP LAST SECOND PROCESSED PACKET COUNTS:
enq drop: arp=0 dh4=0 v4=0 nd=0 dh6=0 v6=0
deq drop: arp=0 dh4=0 v4=0 nd=0 dh6=0 v6=0

CASA#(diag)show qos ds cm qam 0 ip address 192.168.3.102
nx=0 ty= 1 lc= 0 mc=0000 pcnt=
<<Output Cut>>
sf->bw_rate_chk: 0
        cnt pkt=59337 byte=5340362  v6pkt=59337 v6byte=5340362 pkt
sent=59337 byte sent=5340362 over_mx drop_pkt=0 drop_byte=0sf->bw_rate_chk:
0
        cnt pkt=59337 byte=5340362  v6pkt=59337 v6byte=5340362 pkt
sent=59337 byte sent=5340362 over_mx drop_pkt=0 drop_byte=0
```

3.4. RFI PHY Verification and Troubleshooting

On the RFI, the CMTS provides both upstream and downstream interfaces for transmission and receipt of digitized content and data services over fiber network trunks and coaxial cable to and from the subscriber distribution areas. Cable network administrators and operators who are maintaining and troubleshooting the CMTS RF cable interfaces in the cable headend with their existing network infrastructure should have experience with:

- Internet Layer 2 and Layer 3 networking technologies and transports
- Frequency management on upstream and downstream interfaces

3.4.1. Verifying Modulation Profile Configuration

A modulation profile is a collection of burst profiles sent to cable modems in upstream channel descriptor (UCD) messages to configure modem transmit parameters. Primary and secondary modulation profiles are supported in an upstream logical channel configuration. Secondary profiles are not supported on logical channel 1. Making the number of forward error correction (FEC) bytes smaller in the modulation profile to reduce overhead helps increase throughput.

There are five predefined modulation profiles. This means that any new ones added by your organization have an ID of 6 or higher.

3.4.1.1. Video Use Case on Verifying Modulation Profile Configurations

Click here for a video use case on this topic.

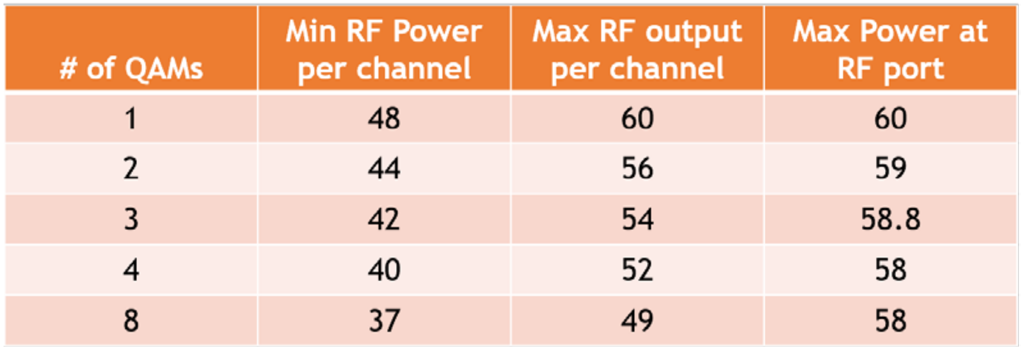
The use case contains the commands below.

```
show modulation-profile [<id>] [table]

CASA#show modulation-profile
modulation-profile 1
request tdma qpsk off 64 0 16 338 0 16 fixed on
initial tdma qpsk off 640 5 34 338 0 48 fixed on
station tdma qpsk off 384 5 34 338 0 48 fixed on
short tdma qpsk off 84 6 75 338 13 16 shortened on
long tdma qpsk off 96 8 220 338 0 16 shortened on
-Output cut-

CASA#show run | beg modulation-profile

CASA#show modulation-profile 10 table
modulation-profile 10
iuc-type        request initial station short long a-short   a-long    ugs
channel-type    atdma   atdma   atdma   -     -    atdma     atdma     -
modulation-type qpsk    qpsk    qpsk    -     -    qpsk      qpsk      -
diff-encoding   off     off     off     -     -    off       off       -
preamble-len    64      640     384     -     -    104       104       -
FEC-T           0       5       5       -     -    12        16        -
FEC-K           16      34      34      -     -    75        220       -
scrambler-seed  338     338     338     -     -    338       338       -
max-burst-size  0       0       0       -     -    6         0         -
guard-time      16      48      48      -     -    16        16        -
last-codeword-len fixed fixed   fixed   -     -    shortened shortened -
scramble-mode   on      on      on      -     -    on        on        -
interleaver-depth 1     1       1       -     -    1         1         -
interleaver-block 1536  1536    1536    -     -    1536      1536      -
preamble-type   qpsk0   qpsk0   qpsk0   -     -    qpsk1     qpsk1     -
interleaver-step -      -        -      -     -    -         -         -
spreader         -      -        -      -     -    -         -         -
subframe-code    -      -        -      -     -    -         -         -
TCM-encode       -      -        -      -     -    -         -         -
```

3.4.2. Verifying RF Power Levels

Overview: Verifying RF Power

Diagram: Downstream Power Table



# of QAMs	Min RF Power per channel	Max RF output per channel	Max Power at RF port
1	48	60	60
2	44	56	59
3	42	54	58.8
4	40	52	58
8	37	49	58

Downstream Power Considerations

Regarding downstream power, there are two considerations: maximum total power allowed, and maximum per-channel power allowed.

The power setting for the RF output port is also the sum of all enabled QAM channels on the same port. The actual QAM channel output level depends on how many QAM channels are enabled on that port.

As the number of channels increase total power must be maintained and as a consequence individual channel power must decrease.

Let's say a QAM modulator is configured for one QAM channel per port. The maximum output is +60 dBmV. If you then increased the number of channels to 4, using the formula defined in the DOCSIS RFI specification, the max power per channel is ~8 dB lower.

Upstream Power Considerations

The CMTS by default will ask the CM to adjust its transmit power so that the CMs transmissions reach the CMTS with a power level of 0. It is possible to modify this setting, however, consider the following before adjusting the upstream power levels.

Input power level should not be adjusted by more than 5 dBmV in a 30-second interval. If the power level is increased or decreased by more than 5 dBmV within 30 seconds, this adjustment could cause significant changes in total power from the modems. As a consequence, the return path lasers could enter a nonlinear mode (clipping) and all communication would become unreliable.

Also, raising upstream power from the modems will create a better carrier-to-noise ratio (C/N), but will generate increased distortion products. For example, composite second and third order distortions worsen by 2 dB for every 1 dB increase in power level.

3.4.2.1. Video Use Case on Verifying RF Power Levels

Click here for a video use case on this topic.

The use case contains the commands below.

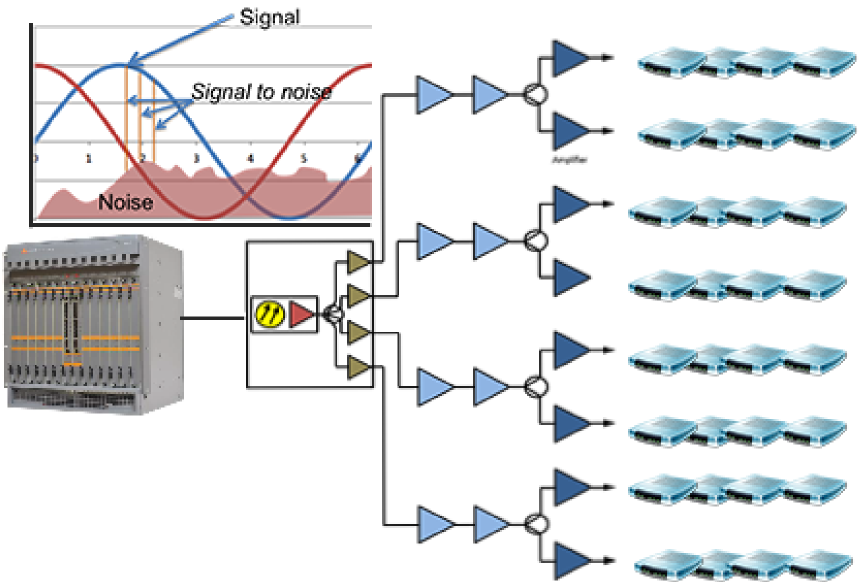
```
CCAP1#show cable modem phy

MAC Address    US IF     DS IF   Sid  USPwr(dB)   USSNR TXTime MicroReflec
DSPwr DSSNR Mode
                                       TX    RX    (dB)  Offset (dBc)
(dB)  (dB)
2476.7d98.b798 13/0.0/0  0/0/0   27   45.3  -0.2   42.1  2390     38
7.0  46.3  tdma
Output Cut.......


CCAP1#show cable modem phy

MAC Address    US IF     DS IF   Sid  USPwr(dB)   USSNR TXTime MicroReflec
DSPwr DSSNR Mode
                                       TX    RX    (dB)  Offset (dBc)
(dB)  (dB)
2476.7d98.b798 13/0.0/0  0/0/0   27   45.3  -0.2   42.1  2390     38
7.0  46.3  tdma
Output Cut.......

CCAP1#show cable modem phy

MAC Address    US IF     DS IF   Sid  USPwr(dB)   USSNR TXTime MicroReflec
DSPwr DSSNR Mode
                                       TX    RX    (dB)  Offset (dBc)
(dB)  (dB)
2476.7d98.b798 13/0.0/0  0/0/0   27   45.3  -0.2   42.1  2390     38
7.0  46.3  tdma
Output Cut.......

demo@class-srv2:~$ snmpwalk -v2c -c public 192.168.2.85
1.3.6.1.4.1.4491.2.1.20.1.2.1.1
SNMPv2-SMI::enterprises.4491.2.1.20.1.2.1.1.4 = INTEGER: 453

transmit power level at CM
docsIf3CmStatusUsTxPower

snmpwalk -v2c -c readmibs 10.3.12.10 1.3.6.1.4.1.4491.2.1.20.1.4.1.3
SNMPv2-SMI::enterprises.4491.2.1.20.1.4.1.3.1.5003328 = INTEGER: 0
Output Cut ....
```

```
receive power per CM at the CCAP
docsIf3CmtsCmUsStatusRxPower

demo@class-srv2:~$ snmpwalk -v2c -c public 192.168.2.85
1.3.6.1.2.1.10.127.1.1.1.1.6
SNMPv2-SMI::transmission.127.1.1.1.1.6.3 = INTEGER: 70

docsIfDownChannelPower
```

3.4.3. Viewing RF Noise Measurements

3.4.3.1. Measuring Noise in the Upstream

Diagram: Signal to Noise



SNR (signal-to-noise ratio) is another important diagnostic parameter. It compares the level of a desired signal to the level of background noise and is expressed in decibels. At the CM, a query to the SNR mib will give you an idea of the SNR of the downstream channel as received by the CM. In the use case example, this query returns a value of 459 or 45.9 db. At the CMTS, the same mib can be used to read the SNR per upstream channel. In the use case example,the query returns a value of 421 or 42.1 db, for each of the four upstreams enabled on the CMTS.

From an RF plant perspective, the upstream SNR is usually the root cause of throughput and partial service issues. There are several CLI commands that can be used to display SNR values. To establish a baseline, you can use the command, **show spectrum snr threshold default,** to display the CMTS SNR values. These values are used by features such as Casa Spectrum management and partial service upstream impairment. The designed values in your RF plant may differ from these numbers, but these serve as a frame of reference as to what is good versus bad SNR, per modulation technique.

Alternatively, you can also use the DOCSIS MER MIB, which provides an in-channel MER (modulation error ratio) measurement or the DOCSIS CNIR MIB, which provides an in-channel carrier-to-noise plus interference ratio. It's especially ingress noise that is reflected in SNR.

3.4.3.1.1. Video Use Case on Viewing Noise Measurements

Click here for a video use case on this topic.

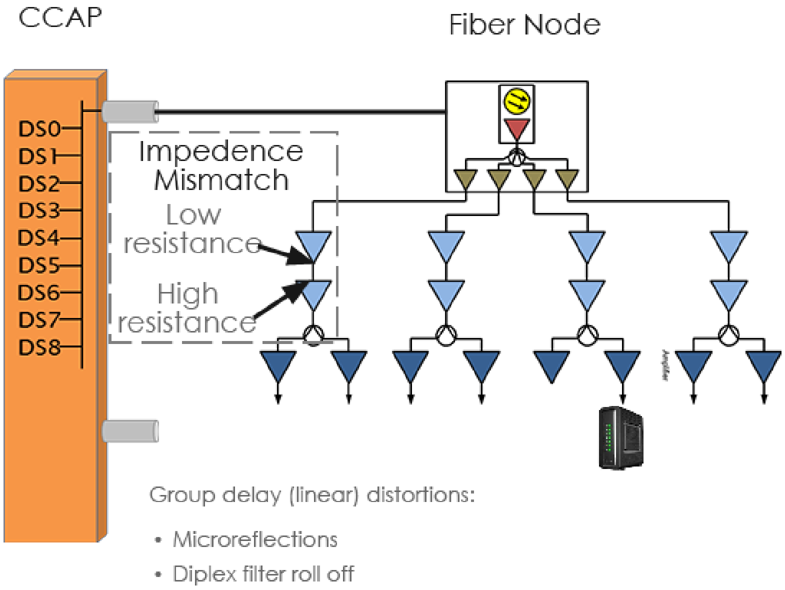
The use case contains the commands below.

```
CASA#show cable modem phy
MAC Address    US IF     DS IF   Sid  USPwr(dB)   USSNR TXTime MicroReflec
DSPwr DSSNR Mode
                                       TX    RX    (dB)  Offset (dBc)
(dB)  (dB)
2476.7d98.b798 13/0.0/0  0/0/0   27   45.3  -0.2   42.1  2390     38
7.0  46.3  tdma
-output cut-

CASA#show upstream signal-quality | inc "13/0.0/0"
13/0.0/0                    42.1
CCAP1#show upstream signal-quality | inc "13/0.0/0"
13/0.0/0                    42.1
CCAP1#show upstream signal-quality | inc "13/0.0/0"
13/0.0/0                    42.1
CCAP1#show upstream signal-quality | inc "13/0.0/0"
13/0.0/0                    42.1
CASA#

CASA#show upstream signal-quality
upstream channel            cnr
13/0.0/0                    42.1
13/0.0/1                    0.0
-output cut-

CASA(config)#show service group Euro_DOCSIS_mdms upstream signal-quality
upstream channel  frequency  channel-width  signal noise
13/1.0/0          20000000   3200000        42.1
13/1.0/1          20000000   3200000        0.0
-output cut-

demo@class-srv1:~$ snmpwalk -v2c -c readmibs 10.3.12.10
1.3.6.1.4.1.4491.2.1.20.1.24.1.1 --MER
demo@class-srv1:~$ snmpwalk -v2c -c readmibs 10.3.12.10
1.3.6.1.4.1.4491.2.1.20.1.25.1.1 --CNIR
SNMPv2-SMI::enterprises.4491.2.1.20.1.24.1.1.5006656 = INTEGER: 421
```

```
SNMPv2-SMI::enterprises.4491.2.1.20.1.24.1.1.5006657 = INTEGER: 0
-output cut-

On the CCAP:
demo@class-srv1:~$ snmpwalk -v2c -c readmibs 10.3.12.10
1.3.6.1.2.1.10.127.1.1.4.1.5
SNMPv2-SMI::transmission.127.1.1.4.1.5.5006656 = INTEGER: 421
-output cut-

On the CM:
demo@class-srv1:~$ snmpwalk -v2c -c public 192.168.2.85
1.3.6.1.2.1.10.127.1.1.4.1.5
SNMPv2-SMI::transmission.127.1.1.4.1.5.3 = INTEGER: 459

docsIfSigQSignalNoise
```

3.4.3.2. Overview: Linear Distortion and Pre-Equalization

Diagram: Linear Distortion



Cable plants have a class of impairments known as linear distortions. A particular linear distortion called “micro reflections” is the difference in delays between the signal on the lower part and higher part of the signal pass band. This is generally caused by impedance mismatches in the cable plant. A second example of a linear distortion occurs at the diplex filter roll off around 42 MHz.

Pre-equalization is especially helpful in mitigating these types of “group delay” distortions that contribute to poor signal quality.

Let’s describe the pre-equalization process at a high level.

STEP 1-The cable modem transmits an un-equalized ranging burst to the CMTS. Typically, the signal gets impaired as it passes through the cable plant.

The CMTS uses the preamble of the upstream burst as a training signal for its equalizer. The equalizer derives equalizer coefficients, based on the channel impairment(s) the received signal demonstrates. These equalizer coefficients account for the signal distortions the cable plant has introduced into the signal.

STEP 2-The CMTS transmits the derived equalizer coefficients to the modem in a RNG-RSP message.

STEP 3-The cable modem uses the equalizer coefficients it receives from the CMTS to program its upstream adaptive equalizer to pre-equalize or pre-distort the signal it transmits into a mirror image of the signal the CMTS received. In theory, the cable plant will modify the pre-distorted signal in transit in the same way it distorted the preamble, so when the CMTS receives the signal it will be unimpaired.

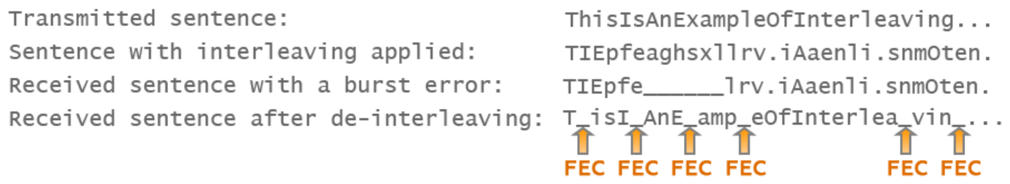
Once the CMTS has determined the equalizer coefficients for a CM, the CM will continue to use those coefficients on all its transmissions. However, cable plants change their transmission characteristics over time. As this occurs, the original adjustments the CM makes to its transmission can actually make matters worse.

To account for this process, Casa implements an option called pre-equalization auto-reset.With auto-reset enabled, the CMTS monitors the SNR in ranging packets it receives from DOCSIS 2.0, 3.0, and 3.1 modems. If the SNR is lower than the correctable FEC error threshold (for example, 25 dB for 64 QAM), the CMTS recalculates the equalization coefficients, and sends them to the CM. The CM then uses these new coefficients to pre-equalize its transmissions.

You cannot directly map your pre-equalization coefficients into a graphing tool from the CLI of the CMTS. However, many third-party tools will collect your coefficient values from the CMTS using SNMP, and plug them into algorithms that give you a snapshot of your cable plant.

3.4.3.3. Overview: Burst Noise and Interleaving

Diagram: Interleaving



```
Transmitted sentence:                   ThisIsAnExampleOfInterleaving...
Sentence with interleaving applied:     TIEpfeaghsxllrv.iAaenli.snmOten.
Received sentence with a burst error:   TIEpfe______lrv.iAaenli.snmOten.
Received sentence after de-interleaving: T_isI_AnE_amp_eOfInterlea_vin_...
```

Interleaving addresses burst noise, a common RF impairment in CATV systems. Burst noise is transient RF energy external to the physical wires of the CATV system being introduced into the RF path, causing errors in the data stream. Interleaving is an efficient way to protect against burst noise. Interleaving spreads data over time. The symbols on the transmit end are intermixed, then reassembled on the receive end. As a result, the errors will appear spread apart. Thus, interleaving plays into the strengths of Forward Error Correction (FEC), because FEC is very effective against errors that are spread apart. Even errors caused by a relatively long burst of interference can still be corrected.

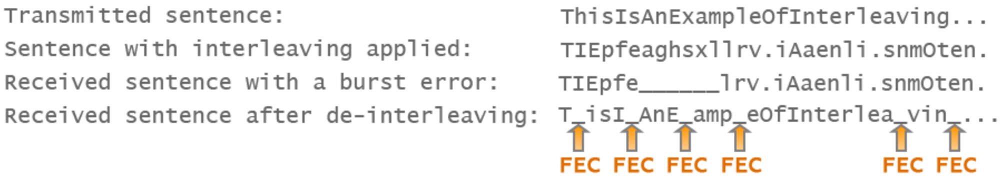
Interleaving can help mitigate errors in the downstream data. The trade off, however, is added latency. The higher the interleaving level, the more latency is introduced into the transmission of data. Interleaving doesn’t add overhead bits the way FEC does, but the added latency could affect voice, gaming, and real-time video. It also increases the Request/Grant round trip time (RTT).

3.4.3.4. Overview: Upstream Power Swings and Small Signal Compensation

Your cable plant may occasionally generate sudden upstream power swings (up to 12 dB) that could result in modem de-registration. (Loose connections are the most common cause of this behavior.) The CMTS supports small signal compensation to manage this situation. By default, small signal compensation is off. Turning it on results in a slight decrease in SNR, so Casa recommends you only use this feature in conditions where known power swings occur.

3.4.4. Cable Modem Diagnostics: Displaying FEC Statistics

Diagram: FEC



```
Transmitted sentence:                  ThisIsAnExampleOfInterleaving...
Sentence with interleaving applied:    TIEpfeaghsxllrv.iAaenli.snmOten.
Received sentence with a burst error:  TIEpfe______lrv.iAaenli.snmOten.
Received sentence after de-interleaving: T_isI_AnE_amp_eOfInterlea_vin_...
```

Forward Error Correction (FEC) is a technique used to detect and correct transmission failures that happen at the physical transmission layer. This is a powerful feature increasing the reliability on noisy channels and preventing that packets are dropped. Recall these are 32 bit counters which roll over to zero after the max counter has been reached.The best way to use these values is calculating the CER (Codeword Error Rate) and CCR (Corrected Codeword Rate) as a percentage over time.

Monitoring FEC correctable and un-correctables is common practice, and a way to determine upstream and downstream transmission quality. Uncorrectable errors indicate the number of code words which were detected and are damaged beyond the possibility of repair by the FEC system. For example, if downstream count is increasing, then downstream signal conditions are unacceptable, no matter how good the SNR and power figures look. Another use of this particular data is to combine it with other MIBs to determine where to look. For example, if you notice that uncorrectable code words are low in the downstream, and the T3 time-out counter is incrementing, this will indicate an upstream path problem. These are a just a few examples of how you can use these FEC variables.

View FEC statistics using the CLI

To view FEC statistics on all your upstream interfaces, type,**show controller**. To view the FEC statistics on a particular upstream module, type, **show controller upstream <module number>**. In the use case example, note the number of unerrored code words, the number of corrected code words, and the number of uncorrectable codewords.

Calculate % correctable codewords

To calculate the percentage of correctable code words, divide the number of corrected code words, by the sum of the number of unerrored code words, plus the number of corrected code words, plus the number of uncorrectable code words, and multiply the result by 100. In the use case example, we divide 760,804 by 14,669,742, and multiply by 100 for a value of 5.19 percent.

Calculate % uncorrectable code words

To calculate the percentage of uncorrectable code words, divide the number of uncorrected code words, by the sum of the number of unerrored code words, plus the number of corrected code words, plus the number of uncorrectable code words, and multiply the result by 100. In the use case example, we divide 47,090 by 14,669,742, and multiply by 100 for a value of 0.32 percent.

3.4.4.1. Video Use Case on Viewing FEC Statistics

Click here for a video use case on this topic.

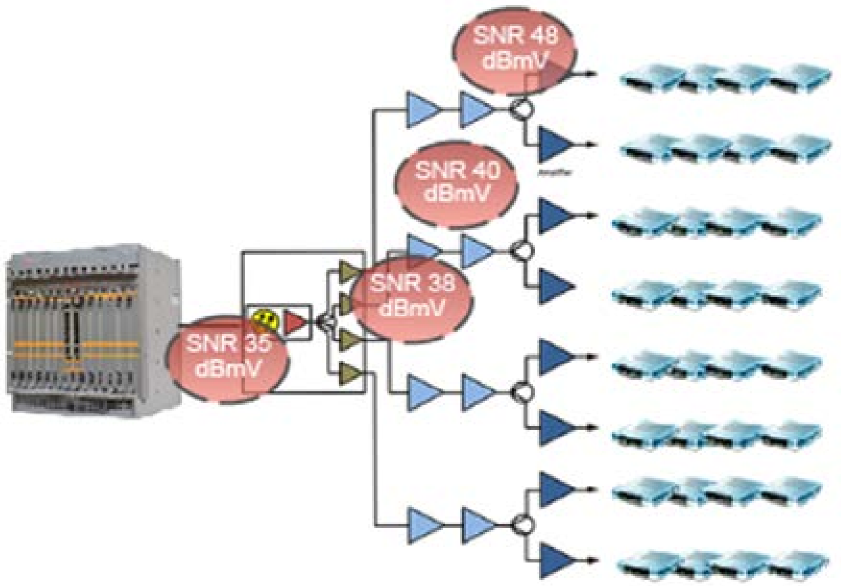
The use case contains the commands below.

```
CASA#show controller
Upstream module information:

Interface upstream 13/0.0/0 information:
    IfIndex :            5006656
    Admin status:        UP
 --output cut-
    Statistics:
    Received 81 broadcasts, 4829 multicasts, 48280 unicasts
    0 discards, 3983 errors, 0 unknown protocol
    13861878 Unerroreds, 760804 Correcteds, 47090 Uncorrectables
 -output cut-

CASA#show cable modem fec
MAC Address     US IF     USSNR Unerrored    Corrected    Uncorrectable
5c35.3b4a.a0f6  13/0.1/0  40.4  167781       0            0
5c35.3baa.60b1  13/1.0/0  42.1  167777       0            0
-output cut

CASA#show cable modem 5c35.3b4a.a0f6 fec
MAC Address     US IF     USSNR Unerrored    Corrected    Uncorrectable
5c35.3b4a.a0f6  13/0.1/0  40.4  168060       0            0
CASA#

CASA#show upstream fec docsis-mac 1
  US chan    frequency   status    cFEC         uFEC
  13/0.0/0   20000000    UP        0            0
  13/0.1/0   24000000    UP        0            0
  13/0.2/0   28000000    DOWN      0            0
  13/0.3/0   32000000    UP        0            0

 To calculate the percentage of correctable code words:
[#correcteds / (#unerroreds + #corrected + #uncorrectables)} * 100
[760804 / (13861878 + 760804 + 47090 )] * 100 = 5.19%

To calculate the percentage of uncorrectable code words:
[#uncorrecteds / (#unerroreds + #corrected + #uncorrectables)} * 100
[47090 / (13861878 + 760804 + 47090 )] * 100 = 0.32%
```

```
Codewords received without errors:
demo@class-srv2:~$ snmpwalk -v2c -c readmibs 10.3.12.10
1.3.6.1.2.1.10.127.1.1.4.1.2
SNMPv2-SMI::transmission.127.1.1.4.1.2.5006656 = Counter32: 13861878

Codewords received with correctable errors:
demo@class-srv2:~$ snmpwalk -v2c -c readmibs 10.3.12.10
1.3.6.1.2.1.10.127.1.1.4.1.3
SNMPv2-SMI::transmission.127.1.1.4.1.3.5006656 = Counter32: 760804

Codewords received with uncorrectable errors:
demo@class-srv2:~$ snmpwalk -v2c -c readmibs 10.3.12.10
1.3.6.1.2.1.10.127.1.1.4.1.4
SNMPv2-SMI::transmission.127.1.1.4.1.4.5006656 = Counter32: 47090
```

3.4.5. Viewing Spectrum Management Statistics

Diagram: SNR Measurements



Casa Spectrum Management (CSM) allows the Casa CMTS to monitor the quality of upstream paths and automatically perform correcting actions when upstream plant impairments are detected. The monitored upstream plant impairments include Signal to Noise Ratio (SNR), correctable Forward Error Corrections (FECs), and uncorrectable FECs. The CMTS can be configured to take one, two, or all three of the following corrective actions when it detects impairment:

- frequency hopping
- upstream channel-width adjustment
- dynamic upstream modulation profile changes

CSM can be configured in either of two management modes: Fast Fourier Transform (FFT) mode, and cable modem (CM) mode. In FFT mode, the FFT screening results, signal-to-noise ratio (SNR) and Forward Error Correction (FEC) errors in particular, are the main error events monitored to determine whether plant noise exists and corrective actions are necessary. In contrast, CM mode uses the upstream SNR of a group of CMs to determine the overall quality of the upstream channel. The CSM approach is tolerance control, that is, how many CMs to tolerate on a particular channel that suffer low signal quality. CSM polls the CMs, counts how many on a logical channel have a lower-than-threshold SNR, and will take the action you have configured when this count is exceeded. The default is 15. In CM mode, roll-back provisions, called "hopback" in the CLI, are also included based on the tolerance.

CSM maintains a list of discrete channel frequencies and/or one or more frequency bands for each upstream interface as frequency hopping targets. This is called a spectrum map. CSM scans through the spectrum map to select the cleanest channel. The spectrum map is updated when a hop is performed. CSM uses spectrum rules to manage the corrective actions. A spectrum rule consists of a set of thresholds and a sequential list of actions. An action can be frequency hopping, channel width adjustment, or modulation profile. An FFT or CM mode procedure is triggered when a monitored indicator to an upstream interface hits a defined or default threshold.

CSM also provides a means to report the configurations and actions, along with some test facilities. If your deployment has CSM configured to take action on the basis of a poor SNR, note that Casa implements a 1 second sliding window, and averages the SNR of all packets which come in over that interval. Note also that CSM calculates the average SNR in linear units, not in logarithmic (dB) units. This allows CSM to more effectively respond to the impairment a single bad cable modem causes to the SNR in the channel.

For detailed information on the operation of Casa Spectrum Management, consult the Casa technical documentation.

3.4.5.1. Video Use Case on Viewing Spectrum Management Statistics

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show spectrum impair-flag
Port channels
2/ 0: 0 0 0 0 0 0 0 0
2/ 1: 0 0 0 0 0 0 0 0
2/ 2: 0 0 0 0 0 0 0 0
2/ 3: 0 0 0 0 0 0 0 0
2/ 4: 0 0 0 0 0 0 0 0

CASA#show spectrum snr-threshold-default
Default SNR threshold per modulation type (tenth dB):
QPSK: 130
8QAM: 190
16QAM: 220
32QAM: 250
64QAM: 280
128QAM: 310

show spectrum upstream <slot>/<port>[.<chan>] [chan-width <freq>] [raw]

CASA(config)# show spectrum upstream 13/0
interface upstream 13/0.0
FREQUENCY NOISE-LEVEL at channel-width 3200000
(dBmV)
5000000: -42.1 8200000: -42.1
11400000: -42.1 14600000: -42.1
17800000: -42.1 21000000: -42.1
24200000: -42.1 27400000: -42.1
30600000: -42.1 33800000: -42.1
-output cut-

show spectrum-map upstream <slot>/<port>[.<chan>]

CASA#show spectrum-map upstream 13/2.0
interface upstream 13/2.0
Spectrum Map for interface 13/2.0
band 0: [5000000, 18400000]
band 1: [21600000, 40000000]

show spectrum-meas upstream <slot>/<port>[.<chan>]

CASA#show spectrum-meas upstream 11/3.0
11/3.0 (0) Spectrum MEAS data (in Hz):
chan cnter freq: 40960000
```

```
frequency span: 81920000
number of bins: 1024
resolution bw: 80000
bin spacing: 80000
EF 8E EF 8E EF 8E EF 8E EF 8E EF 8E EF 8E EF 8E EF 8E EF 8E EF 8E
EF 8E EF 8E EF 8E EF 8E EF 8E EF 8E EF 8E EF 8E EF 8E EF 8E EF 8E
EF 8E EF 8E EF 8E F1 E8 F1 E8 F1 E8 F1 E8 F1 E8 F1 E8 F1 E8 F1 E8
```

3.5. RFI MAC Verification and Troubleshooting

Objectives

In this section of the course, you will learn how to verify:

- Downstream channel configurations
- Upstream interface configurations
- MAC domain configurations
- Channel bonding
- Load balancing configuration
- Partial service

3.5.1. Verifying Downstream Channel Configurations

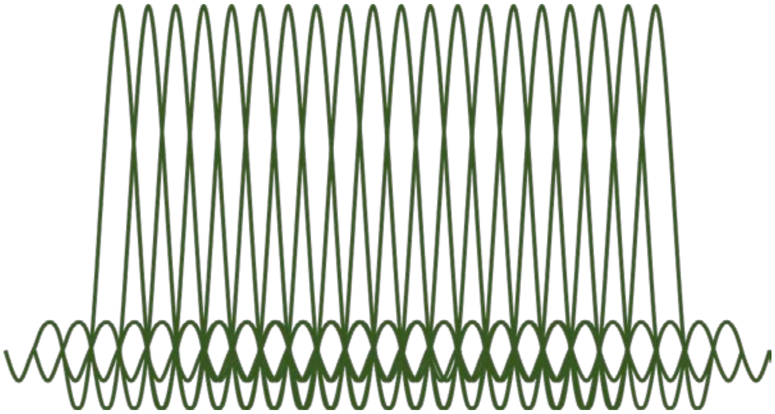
OFDM

Orthogonal Frequency Division Multiplexing (OFDM) is a data transmission method where a large number of closely spaced or overlapping very-narrow-bandwidth orthogonal (mutually exclusive) QAM signals are transmitted in a given channel.

Earlier versions of DOCSIS specified downstream signals either 6 MHz or 8 MHz in width. DOCSIS 3.1 calls this signaling “Single Channel QAM”, or SC-QAM, because each channel could only support one modulation technique at a time.

In contrast, OFDM generates multiple signals that have a very narrow frequency - either 25 KHz or 50 KHz in DOCSIS 3.1 - and a long transmission time.

Diagram: OFDM Subcarriers



The OFDM process gains you four benefits:

- Processing Speed: The transmitter uses the Inverse Fast Fourier Transform (IFFT) function to sum many sine waves into a single complex signal.
- Signal Robustness: Because each signal is transmitted over a long time period, it is less subject to interference.
- Signal Flexibility: You can configure modulations on individual subcarriers to account for specific cable plant conditions.
- Signal Density: Wider channels mean you can use more of the available spectrum and deploy fewer guard bands.

In OFDM, each signal is called a “subcarrier.” The sending device transmits each subcarrier so that the peak of any given subcarrier always occurs when all the nearby subcarriers are at phase 0. The subcarriers in a given channel do not need to be contiguous. You can configure excluded subcarriers to account for your cable plant conditions, and you can configure exclusion bands to account for other transmissions on your network - e.g., legacy DOCSIS 3.0 SC-QAMs.

SC-QAM

Quadrature Amplitude Modulation (QAM) is the modulation scheme for digital cable and CMs for downstream traffic.

3.5.1.1. Video Use Case on Verifying Downstream Channel Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show ofdm channel

interface qam 2/0
  ofdm-channel 0 lower-freq 118400000 upper-freq 308400000 plc-freq 
200000000
  ofdm-channel 0 cyclic-prefix 192
  ofdm-channel 0 rolloff-period 64
  ofdm-channel 0 interleave 1
  ofdm-channel 0 sc-spacing 50
  ofdm-channel 0 pilot-scale-factor 48
  ofdm-channel 0 ncp-modulation qpsk
  no ofdm-channel 0 up-down-trap-enable
  ofdm-channel 0 profile 0 1
  ofdm-channel 0 profile 1 9
  no ofdm-channel 0 shutdown
CASA#

CASA#show ofdm profile

ofdm profile 1
  profile-modulation 16qam

-output cut-

ofdm profile 9
  profile-modulation 256qam
  subcarrier-group 1 118400000 120300000 modulation 256qam
  subcarrier-group 2 120500000 122900000 modulation 512qam
  subcarrier-group 3 123000000 130000000 modulation 128qam
  subcarrier-group 4 131100000 137400000 modulation 64qam
CASA#

CASA#show ofdm exclusion-band

ofdm exclusion-band 1
  exclusion-subcarrier-group 1 137500000 147500000
CASA#

CASA# show cable dpd msg ofdm 2/0/0 profile 0
-output cut-

Dest. Address : 01e0.2f00.0001
Source Address: 0017.1082.c733
Message Length: 16 (decimal) DSAP: 00 SSAP: 00
Control: 03 Version: 05
Type: dpd(50) RSVD: 00
Downstream Channel ID: 32
Profile Identifier: 00
Configuration Change Count: 01
Subcarrier Assignment Range/List(5): 2c 00 00 0f ff

CASA# show cable ocd msg ofdm 4/0/0
-output cut-
…
Dest. Address : 01e0.2f00.0001
Source Address: 0017.1084.0121
Message Length: 68 (decimal) DSAP: 00 SSAP: 00
```

3.5.2. Verifying Upstream Interface Configuration

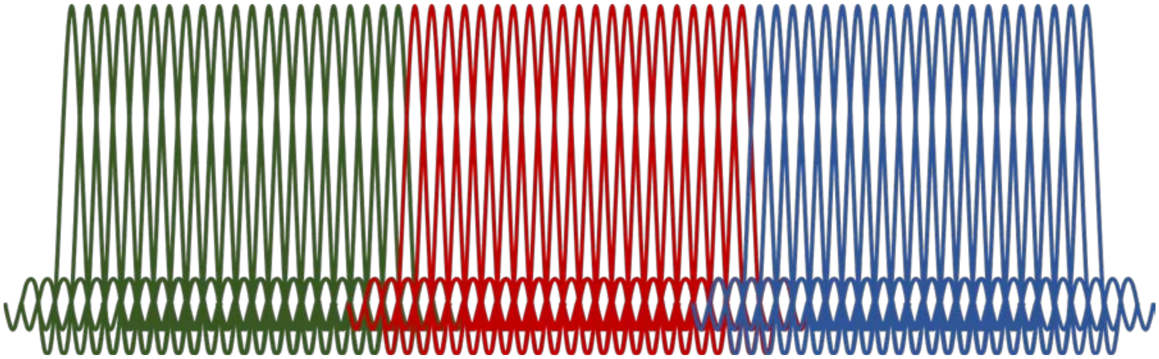
Upstream Interfaces

Upstream ports are physical interfaces the cable modem return paths connect to. The Casa CMTS allows up to two logical channels in each upstream port in two different A-TDMA modes. Each upstream port and logical channel can be enabled or disabled independently. The default state for all upstream ports and channels is shutdown. If an upstream port is disabled, individual logical channels cannot be enabled.

OFDMA

Orthogonal Frequency Division Multiple Access (OFDMA) is a multi-user version of Orthogonal Frequency Division Multiplexing (OFDM) where many users can transmit and receive over a single channel simultaneously. OFDMA uses distributed subcarriers among users to enable multiple user transmissions over one channel. DOCSIS Version 3.1-specific modems are necessary to support OFDMA in the cable network.

Diagram: OFDMA Subcarriers



You must understand how minislots work in DOCSIS 3.1 to get the maximum benefit from the increased upstream bandwidth. Unlike DOCSIS 3.0, a minislot in DOCSIS 3.1 has nothing to do with time, per se. Instead, DOCSIS 3.1 defines a minislot as a specific number of contiguous subcarriers, transmitted for a specified number of OFDMA symbols, ie, a minislot is defined in terms of width and duration. Each minislot is 400 kHz wide, comprising either 8 subcarriers if you are using 2K FFT, or 16 subcarriers if you are using 4K FFT.

The minimum length for a minislot is 6 symbols. The maximum length for a minislot is determined by how much total bandwidth is available in the OFDMA channel. All the minislots in a given OFDMA channel must be of the same duration.

3.5.2.1. Video Use Cases on Verifying Upstream Interface Configurations

Click here for a video use case on this topic.

The Verifying Upstream SC-QAM Configurations use case contains the commands below.

```
To verify the general parameters of an upstream SC-QAM interface, type show
interface upstream <interface name>.

Verify that your network has the interleaver set to dynamic mode to account
for burst noise in the upstream with the show modulation-profile <profile
number>command. A 0 in the position shown means the interleaver is in
dynamic mode. Burst duration immunity is set by the next value, 2048 is the
maximum.

CASA#show modulation-profile 6
modulation-profile 6
-output cut-
 a-short atdma qpsk off 104 12 75 338 13 8 shortened on 0 2048 qpsk1
 a-long atdma qpsk off 104 16 223 338 0 8 shortened on 0 2048 qpsk1
 ugs atdma qpsk off 104 16 223 338 0 8 shortened on 0 2048 qpsk1

To verify adjustments made in your deployment to account for linear
distortion, type show interface upstream <interface name> and look for the
setting, “logical-channel 0 pre-equalization.” This setting means that pre-
equalization is turned on.

CASA#show interface upstream 13/0.0

interface upstream 13/0.0
  frequency 20000000

-output cut-

  logical-channel 0 ranging-backoff 0 4
  logical-channel 0 pre-equalization auto-reset 1440
  logical-channel 0 power-offset 0
-output cut-

Type show modulation profile <profile name> and examine your FEC-T and FEC-K
settings (shown below in red), to check on how your network has been
configured to account for non-linear distortion. FEC-T has a range of 0-16,
and FEC-K has a range of 16-255.

CASA#show modulation-profile 6
modulation-profile 6
 request atdma qpsk off 64 0 16 338 0 16 fixed on 1 1536 qpsk0
 initial atdma qpsk off 640 5 34 338 0 48 fixed on 1 1536 qpsk0
 station atdma qpsk off 384 5 34 338 0 48 fixed on 1 1536 qpsk0
 a-short atdma qpsk off 104 12 75 338 13 8 shortened on 0 2048 qpsk1
 a-long atdma qpsk off 104 16 223 338 0 8 shortened on 0 2048 qpsk1
 ugs atdma qpsk off 104 16 223 338 0 8 shortened on 0 2048 qpsk1

CASA#

To verify adjustments made in your deployment to account for a highly-
attenuated RF path, type show interface upstream <interface name> and check
the setting for power-adjustment continue.  The default is 2.

CASA#show interface upstream 13/0.0

interface upstream 13/0.0
  frequency 20000000
  channel-width 3200000
  power-level 0
  power-adjustment continue 2
  power-adjustment threshold 1
-output cut-
```

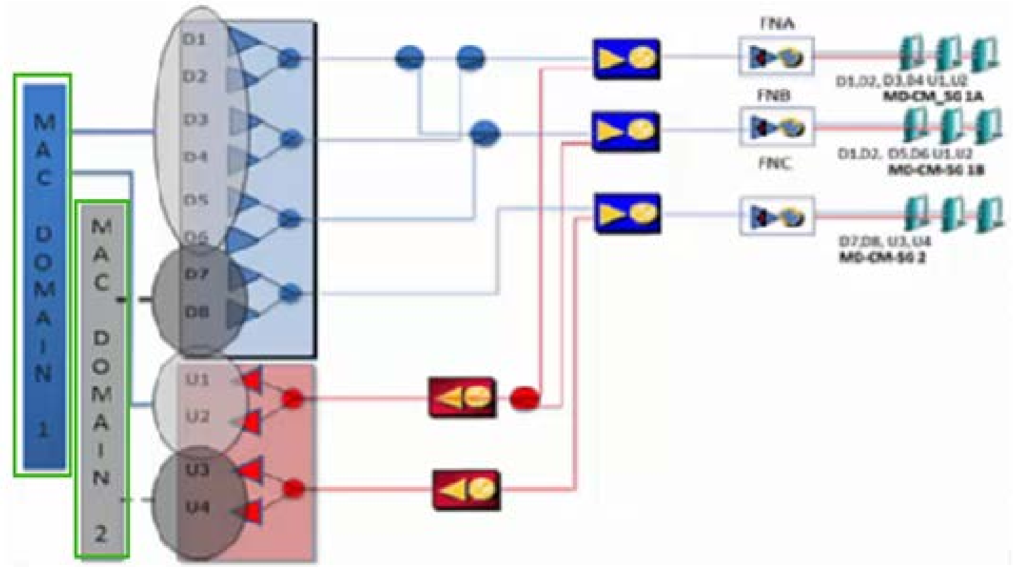
The Verifying OFDMA Configurations use case contains the commands below.

```

To view the configuration of a specific OFDMA interface, use the show
interface ofdma <interface name> command.

CASA#show interface ofdma 13/0

interface ofdma 13/0.0
 exclusion-band 1
 lower-freq 5000000 upper-freq 101000000
 symbols-per-frame 18
 iuc-profile 1
 no shutdown
CASA#

Type, show ofdma exclusion-band, to view all the OFDMA exclusion band
profiles configured on the CMTS/CCAP.

CASA#show ofdma exclusion-band

ofdma exclusion-band 1
  exclusion-sc-group 1 8000000 10000000
  exclusion-sc-group 10 19000000 36000000
  exclusion-sc-group 20 85000000 90000000
CASA#

View all the OFDMA minislot profiles configured on the CCAP with the show
ofdma minislot-cfg command.

CASA#show ofdma minislot-cfg

ofdma minislot-cfg 1
  subcarrier-group-minislot 1 5000000 11400000 modulation 256qam pilot-
pattern 1
  subcarrier-group-minislot 2 37000000 43400000 modulation 64qam pilot-
pattern 8
CASA#

View all the OFDMA IUC profiles configured on the CCAP with the show ofdma
iuc-profile command.
```

```
CASA#show ofdma iuc-profile

ofdma iuc-profile 1
 fine-ranging-iuc 32 10000
 initial-ranging-iuc 64 10000
 data-iuc 5 modulation 8qam pilot-pattern 2
 data-iuc 6 modulation 64qam pilot-pattern 3
 data-iuc 9 modulation qpsk pilot-pattern 1
 data-iuc 13 modulation 64qam pilot-pattern 2
```

3.5.3. Verifying MAC Domain Configuration Overview

Diagram: MAC Domains



A MAC domain is the set of downstream and upstream frequencies that reach a group of cable modems. A MAC domain must contain at least one downstream channel and at least one upstream channel. The MAC domain performs the following functions:

- A MAC Domain implements DOCSIS functions on a set of downstream channels and upstream channels.
- A MAC Domain provides layer 2 data transmission services between the CMTS Forwarders and the set of CMs registered to that MAC Domain.
- The MAC Domain classifies downstream packets into downstream "service flows" based on layer 2, 3, and 4 information in the packets.
- The MAC Domain schedules the packets for each downstream service flow to be transmitted on its set of downstream channels.

- In the upstream direction, the MAC Domain indicates to a CMTS Forwarder component when a Layer 2 packet has been received from a particular CM.

MAC domains interact with service groups and load balancing groups. Specifically, a MAC Domain Cable Modem (MD-CM) is a set of downstream and upstream channels from the same MAC domain that reach a single CM. A MAC Domain Cable Modem Service Group (MD-CM-SG) corresponds to a general load balancing group. A general load balancing group forms the set of channels among which a non-bonding CM can be moved, while remaining registered in the same MAC Domain.

MAC Domain Restrictions

- Max Number of MAC Domain Interfaces: C100G is 96
- Max Number of Upstream Channels Per MAC Domain Interface: 255
- Max Number of Downstream Channels Per MAC Domain Interface: 255
- Max Number of CMs per MAC Domain: 8191

3.5.3.1. Video Use Case on Verifying MAC Domain Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

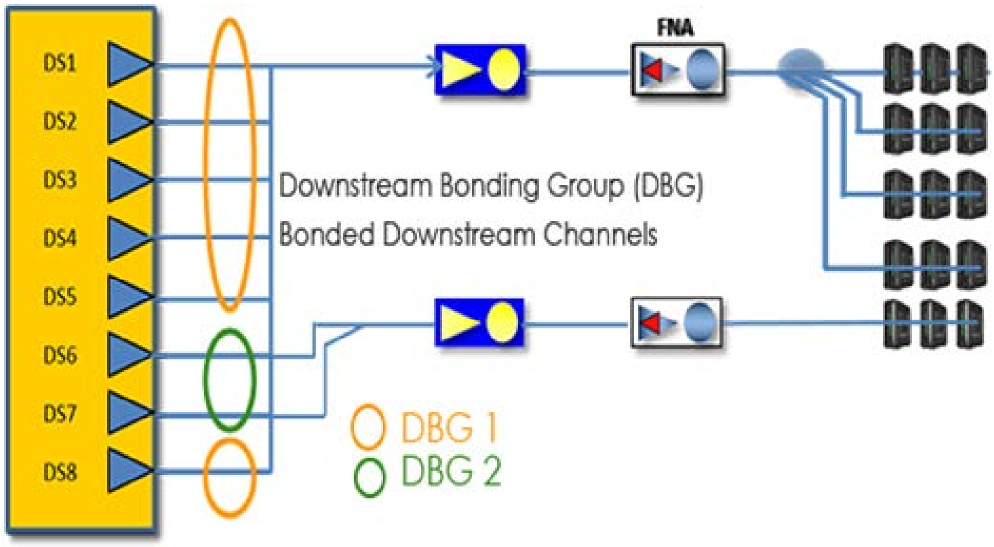
```
CASA#show interface docsis-mac 1 brief

interface docsis-mac  1
  no shutdown
  ip-provisioning-mode dual-stack
  no early-authentication-encryption
  no multicast-dsid-forward
  no tftp-proxy
  ip bundle 1
  downstream 1 interface qam 0/0/0
  downstream 2 interface qam 0/0/1
  downstream 3 interface qam 0/0/2
  downstream 4 interface qam 0/0/3
  downstream 5 interface qam 0/0/4
  downstream 6 interface qam 0/0/5
  downstream 7 interface qam 0/0/6
  downstream 8 interface qam 0/0/7
  downstream 9 interface ofdm 2/0/0
  upstream 1 interface upstream 13/0.0/0
  upstream 2 interface upstream 13/0.1/0
  upstream 3 interface upstream 13/0.2/0
  upstream 4 interface upstream 13/0.3/0
  upstream 5 interface ofdma 13/0.0
  router-advertisement enable
  router-advertisement managed-flag true
  router-advertisement other-config-flag true
CASA#

CASA#show interface docsis-mac brief

interface docsis-mac  1
  no shutdown
  ip-provisioning-mode dual-stack
  no early-authentication-encryption
-output cut -

interface docsis-mac  2
  no shutdown
  ip-provisioning-mode dual-stack
  no early-authentication-encryption
-output cut -

CASA#show interface docsis-mac 1 topology
interface docsis-mac  1
=======================================
DS        Cable Chan Oper                   Mod   Power    Service
Int       Mac   ID   State Annex Freq(Hz)   Type  (.1dBmV) Group(s)
0/0/0     1     1    UP    B(US) 555000000  q256  460
0/0/1     1     2    UP    B(US) 561000000  q256  460
-output cut-

US        Cable Chan Oper  Chan             Channel Mini Mod  Power  Service
Int       Mac   ID   State Type  Freq(Hz)  Width   Slot Prof (dBmV) Group(s)
13/0.0/0  1     1    UP    tdma  20000000  3200000 2    2    0
13/0.1/0  1     2    UP    tdma  24000000  3200000 2    2    0
-output cut-

CASA#show cable modem summary mac-domain
Upstream   Mac Total   Active  Registered Secondary  Offline  Bonding
Non_Bonding Channel
Interface  Int Modems  Modems  Modems     Modems     Modems   Modems
Modems      Description
13/0.0/0   1   12      12      12         0          0        0        12
13/0.1/0   1   2       2       2          0          0        0        2
13/0.3/0   1   0       0       0          0          0        0        0
13/0.0w    1   0       0       0          0          0        0        0
ofdma
-output cut-

CASA#show cable modem summary total mac-domain
Upstream  Mac Total  Active Registered Secondary Offline Channel
Interface Int Modems Modems Modems     Modems    Modems  Description
9/0.0/0   0   0      0      0          0         0
9/0.1/0   0   0      0      0          0         0
-output cut-

CASA#show downstream channel set mac-domain 1
MAC    Chan  Channel
 ID     Set     List
  1       1  0/0/0
  1       2  0/0/1
-output cut-
```

3.5.4. Verifying Channel Bonding

3.5.5. Overview: Channel Bonding

Channel bonding, a DOCSIS 3.0 capability, is the CMTS process that logically combines multiple downstream or upstream channels for extended bandwidth for cable modems that have multiple transmitters and receivers. This feature enables a DOCSIS 3.0 CMTS to schedule packets for a single service flow across multiple channels. The major benefit is increased data rates. The amount of increase depends on the number of channels that are bonded, and on the transmission efficiencies gained through statistical multiplexing.

Diagram: Downstream Bonding Groups

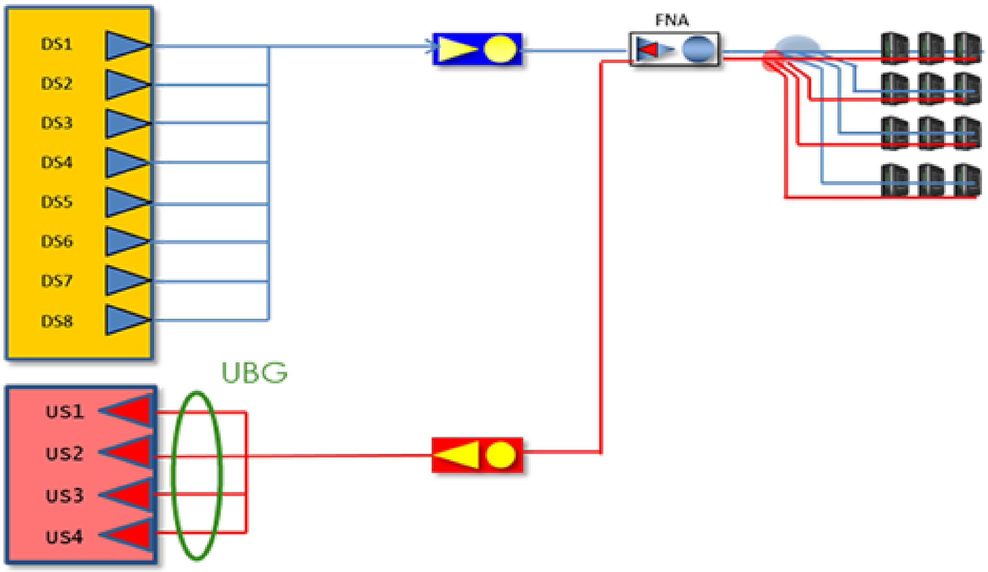


Let's consider downstream bonding first. The term "downstream channel bonding" means the distribution of packets from the same service flow over different downstream channels. A "Downstream Bonding Group" (DBG) refers to the group of Downstream Channels over which the CMTS distributes the packets of a downstream service flow. Although you can statically provision a DBG, Casa recommends you allow the CMTS to dynamically determine your DBGs. A DBG need not be composed of adjacent RF channels.

In a typical deployment, an MSO will have a large number of cable modems tuned to the same DBG. These CMs may have various bonding capabilities. Some will only receive one downstream channel; some will receive 4, 8, or, in rare cases, 16 channels. (The theoretical maximum is 32 channels.)

In this case, the MSO normally would create a DBG with the same number of channels as the most powerful CM, and assign a variety of CMs to that DBG. The CMTS will then use a Receive Channel Configuration (RCC) message to assign downstream channels to each CM based on that CM’s bonding capabilities. The set of downstream channels assigned to an individual CM is called its Receive Channel Set (RCS).

Diagram: Upstream Channel Bonding



Now let’s discuss Upstream Channel Bonding.The CM makes a request for bandwidth for a given service flow on one of the service flow’s associated upstream channels. This request is called a queue depth request. This type of request asks for the number of bytes to be transmitted, as opposed to requesting a number of mini slots as in the regular request grant process. DOCSIS enables this process with a protocol element call the segment header.

The CMTS controls the upstream bonding as part of the scheduling process by way of data grants in the MAP. When the CM receives the grant, it stripes its transmission across all of the bonded upstream channels.

The individual channels can be any mix of modulation types, symbol rates, TDMA or S-CDMA and can be any mix of adjacent or non-adjacent upstream channels. They must, however, be all on the same line card.

The CM places an incrementing sequence number in the traffic transmitted in each grant. The CMTS then uses the sequence number in the traffic to reconstruct the original data stream.

This upstream process is called Continuous Concatenation and Fragmentation (CCF). CCF treats each service flow from the CM as a continuous stream of data regardless of the channel on which that data arrives.

Note: The Casa CMTS supports channel bonding in the same line card module. It does not support bonding of channels across line cards. In a DOCSIS 3.0 implementation, the maximum number of channels per bonding group is 32.

3.5.6. Static Bonding Groups and Channel Blocks

In networks where traffic from a particular modem or service area must use a specific downstream or upstream channel, upstream and downstream bonding groups can be configured using the bonding-group object to direct traffic streams to specific channels configured at the CMTS. This means that the CMTS uses the configured bonding group and only the specific channels defined in the group. The CMTS does not make the channel selection dynamically from a group of available channels at the MAC domain. Up to 480 upstream bonding groups can be configured.

Casa highly recommends the dynamic service group configuration over the static bonding group configuration, which should only be used in very specific cases where dynamic channel selection is not feasible.

The channel-block downstream group 4 command automatically creates groups of four (or fewer) channels from the downstream channels defined for a DOCSIS MAC domain, each with a separate block ID. A group can have fewer than four channels if the defined QAM channels for a MAC domain are not in multiples of four. The allowed block IDs for each MAC domain range from 1:255.

The Casa CMTS globally supports a maximum of 1024 channel blocks.

3.5.6.1. Video Use Case on Verifying Channel Bonding

Click here for a video use case on this topic.

The use case contains the commands below.

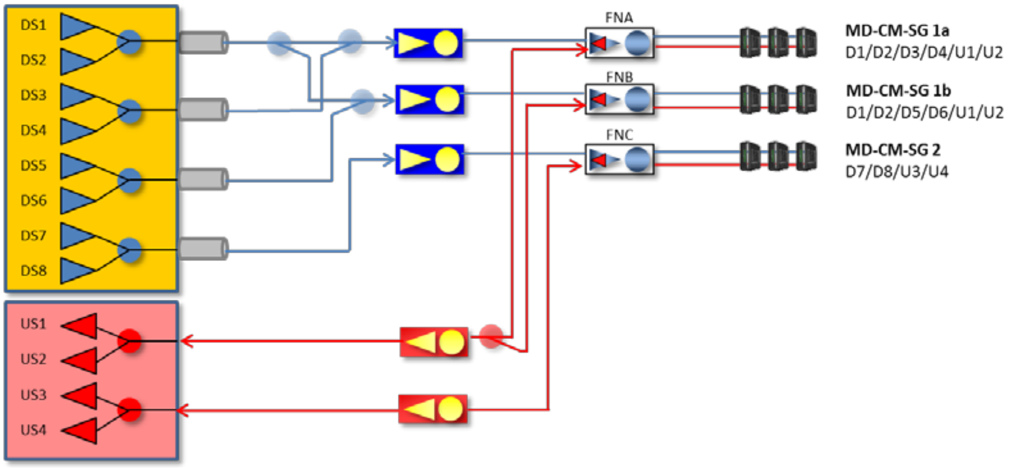
```
CASA#show cable modem
MAC Address    IP Address      US          DS        MAC          Prim RxPwr
Timing Num  BPI
                               Intf        Intf      Status       Sid  (dB)
Offset CPEs Enb
5c35.3b4a.a0f6 192.168.1.56    13/0.1/0*  0/0/4*   online(pt)  408  0.0
2435   0    yes
5c35.3baa.60b1 192.168.1.74    13/1.0/0   0/1/1    online(pt)  178  0.0
1242   0    yes
5c35.3baa.6294 192.168.1.55    13/1.0/0   0/1/1    online(pt)  179  0.0
1242   0    yes
5c35.3bac.ae55 192.168.1.62    13/0.0/0*  0/0/2*   online(pt)  429  0.0
2429   0    yes
-output cut-

CASA#show cable modem bonding
MAC Address   MAC US        DS      US  DS           US/DS CHAN EXCLUDED
               id Intf      Intf    SET SET
5c35.3b4a.a0f6  1 13/0.1/0  0/0/4   257 256(3*8)
5c35.3bac.ae55  1 13/0.0/0  0/0/2   257 256(3*8)
-output cut-

CASA#show cable modem 5c35.3bac.c172 bonding
MAC Address   MAC US        DS      US  DS           US/DS CHAN EXCLUDED
               id Intf      Intf    SET SET
5c35.3bac.c172  1 13/0.0/0  0/0/2   257 256(3*8)

CASA#show cable modem non-bonding
MAC Address    IP Address      US          DS        MAC          Prim RxPwr
Timing Num  BPI
                               Intf        Intf      Status       Sid  (dB)
Offset CPEs Enb
5c35.3baa.60b1 192.168.1.74    13/1.0/0   0/1/1    online(pt)  178  0.0
1242   0    yes
5c35.3baa.6294 192.168.1.55    13/1.0/0   0/1/1    online(pt)  179  0.0
1242   0    yes
-output cut-

CASA#show cable modem 5c35.3bad.8d6e non-bonding
MAC Address    IP Address      US          DS        MAC          Prim RxPwr
Timing Num  BPI
                               Intf        Intf      Status       Sid  (dB)
Offset CPEs Enb
5c35.3bad.8d6e 192.168.1.53    13/1.0/0   0/1/0    online(pt)  183  0.0
1245   0    yes

CASA#show downstream channel set mac-domain 1
MAC    Chan  Channel
 ID     Set     List
  1       1  0/0/0
  1       2  0/0/1
  1       3  0/0/2
  1       4  0/0/3
  1       5  0/0/4
  1       6  0/0/5
  1       7  0/0/6
  1       8  0/0/7
  1     256  0/0/0-0/0/7

CASA#show upstream channel set mac-domain 1
MAC    Chan  Channel
 ID     Set     List
```

```
  1       1  13/0.0/0
  1       2  13/0.1/0
  1       3  13/0.2/0
  1       4  13/0.3/0
  1       5  13/0.0w
  1     256  13/0.0/0-13/0.3/0, 13/0.0w
  1     257  13/0.0/0-13/0.1/0, 13/0.3/0

CASA#show bonding-group

bonding-group upstream mac-domain 3 group-id 3
   upstream 13/3.0/0
   upstream 13/3.1/0
-output cut-
 prov-attr-mask 0x80000001

bonding-group downstream mac-domain 3 group-id 3
   qam 0/3/0
   qam 0/3/1
-output cut-
 prov-attr-mask 0x80000001
 reseq wait-time 180
 reseq warn-thrshld 0

CASA#show channel-block

channel-block downstream mac-domain 3 block-id 1
   qam 0/3/0
   qam 0/3/1
-output cut-
 prov-attr-mask 0x80000000

channel-block downstream mac-domain 3 block-id 2
   qam 0/3/4
   qam 0/3/5
-output cut-
 prov-attr-mask 0x80000000
```

3.5.7. Verifying Load Balancing Configuration

Overview: Load Balancing

Diagram: Load Balancing Group



DOCSIS 3.0 Cable Modems are able to operate in Multiple Receive Channel (MRC) mode/Multiple Transmit Channel (MTC) mode. This enables load balancing, which is the ability of the CMTS to move Cable modems to different upstream and downstream channels based on criteria you configure.

Load balancing supports multiple methods to achieve greater bandwidth availability. These include static and dynamic load balancing schemes, inter-line card and intra-line card support, and in some circumstances, configuration of load balancing groups that entail multiple interfaces, multiple load balancing policies, and the option to configure multiple additional load balancing parameters.

A CMTS channel can be load-balanced using one of two methods:

- Number of CMs — Load balancing according to the number of CMs on theinterface, or based on how modems are classified by **cable tag**.
- Utilization — Load balancing according to the current percentage of channel utilization.

Each of the methods can further be operated in two types: static or dynamic.

- *Static* — Load balancing is done at ranging request time. When a CM sends its initial ranging request message, the CMTS responds with a ranging response message that includes either a Downstream Frequency Override or an Upstream Channel ID Override field that instructs the CM which channels it should use.
- *Dynamic* — A form of load balancing in which CMs are moved among upstream and downstream channels within the same service group after their initial difference between two interfaces exceeds a user-defined percentage. The CMTS will use DCC/UCC messages to move CMs with single upstream/

downstream channels, and Dynamic Bonding Change (DBC) messages to move CMs with bonding upstream/downstream channels, to different bonding groups.

A Load Balancing Group (LBG) is essentially the same as a MAC Domain Cable Modem Service Group (MD-CM-SG). That is, an LBG is a set of upstream and downstream channels over which a CMTS load balances a set of CMs. The CMTS creates a Load Balancing Group for every MD-CM-SG that is instantiated by the topology configuration. This type of LBG is referred to as a "General" Load Balancing Group.

You can also configure "Restricted" Load Balancing Groups that specify a subset of the channels in a Cable Modem Service Group (CM-SG) to which a CM can be assigned. Restricted Load Balancing Groups are used to accommodate a topology specific or provisioning specific restriction, e.g., a set of channels reserved for business customers. The CMTS can associate an upstream or downstream channel with any number of Restricted Load Balancing Groups. Restricted Load Balancing Groups can be configured through the CMTS CLI, or with the Service Type Identifier or the Load Balancing Group Identifier TLVs in the CM configuration file.

Since Release 7.1, the restricted load balancing configuration commands now accept a range of QAM or upstream channels instead of having to specify each channel as a separate entry.

3.5.7.1. Video Use Case on Verifying Load Balancing Configurations

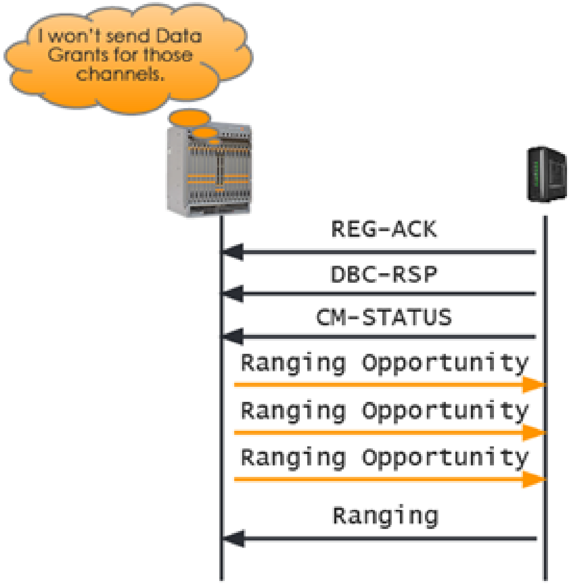
Click here for a video use case on this topic.

The use case contains the commands below.

```
To verify the CCAP’s load balancing configuration, type show run | beg “load
balancing commands”.

CASA#show run | beg "load balance commands"
! load balance commands
!

load-balance enable

load-balance basic-rule 1
  enable

load-balance execution-rule 1
  method modem
  method utilization dynamic
  threshold load 10 enforce 20 minimum 20 dynamic minimum 60

load-balance policy 1
  rule execution 1
  rule basic 1

load-balance general-group default-settings
  policy-id 1

-output cut-

To view a specific load balancing parameter, type show load-balance ?, and
specify the parameter you wish to view.

CASA#show load-balance ?
basic-rule          show load-balance basic rule
dynamic             dynamic load-balance
exclusion           load-balance exclusion
execution-rule      show load-balance execution-rule
general-group       general-group
policy              show load-balance policy
restricted-cm       show restricted-cm
restricted-group    restricted-group
running-config      show load-balance running configuration
static              static load-balance
CASA1#
```

3.5.8. Verifying Partial Service

Diagram: Partial Service Signaling



Whenever a CM is unable to use one or more channels in the Transmit Channel Set (TCS) and/or the Receive Channel Set (RCS), that CM is said to be operating in a "partial service" mode in the upstream and/or downstream respectively.

A channel is deemed to be unusable when the CM is unable to acquire one or more channels during registration, during a Dynamic Bonding Change, or if the CM loses an upstream and/or downstream channel during normal operation.

The CM signals that it is in a partial service mode of operation to the CMTS through one of the following:

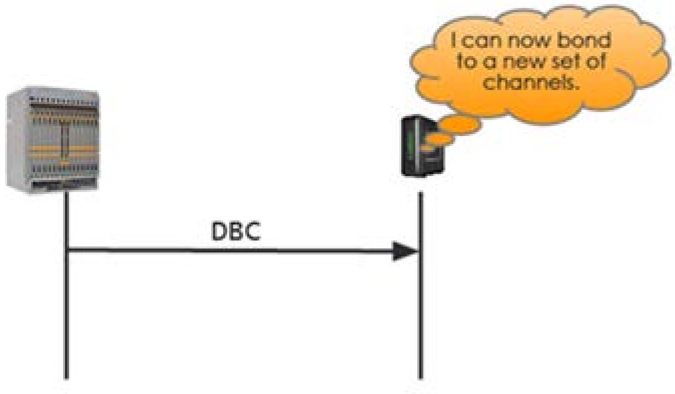
- The REG-ACK message, if it is unable to acquire a channel or channels during registration.
- The DBC-RSP message, if it is unable to acquire one or more channels assigned to it during the DBC request process.
- The CM-STATUS message, if the channel becomes unusable during normal operation.

In these cases, if the CM's upstream bonding group is comprised of all the upstream channels in the service group, the Casa CMTS will attempt to resolve partial service by:

- Not sending any data grants for the unusable channels
- Continuing to send ranging opportunities on the unusable upstream channels

When the channel recovers sufficiently, the CM will begin ranging on and will acquire the previously unusable channel.

Diagram: Dynamic Bonding Change



However, if there are additional upstream channels available in the Service Group, the CMTS will send the CM a Dynamic Bonding Change (DBC) message, allowing the CM to come out of partial service by bonding to a new set of channels.

3.5.8.1. Video Use Case on Verifying Partial Service

Click here for a video use case on this topic.

The use case contains the commands below.

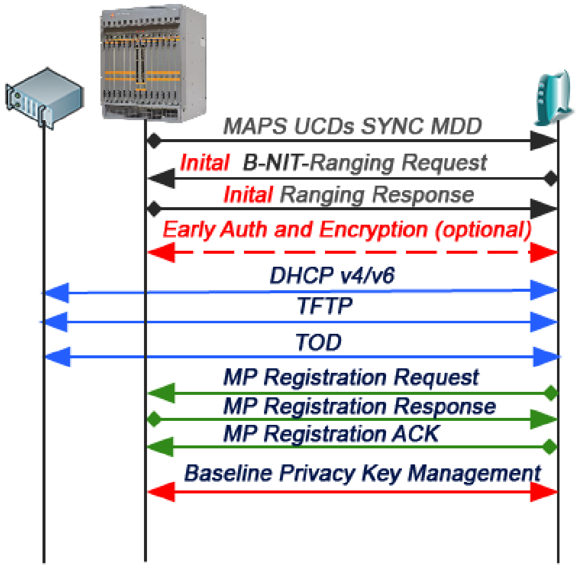
```
CASA#show cable modem
MAC Address    IP Address      US         DS       MAC         Prim RxPwr
Timing Num  BPI
                               Intf       Intf     Status      Sid  (dB)
Offset CPEs Enb
5c35.3b4a.a0f6 192.168.1.56    13/0.1/0*  0/0/4*   online(pt)  408  -0.2
2434   0    yes
5c35.3baa.60b1 192.168.1.74    13/1.0/0#  0/1/1    online(pt)  178  0.0
1242   0    yes
5c35.3baa.6294 192.168.1.55    13/1.0/0#  0/1/1    online(pt)  179  0.0
1243   0    yes
5c35.3bac.ae55 192.168.1.62    13/0.0/0*  0/0/2*   online(pt)  429  -0.2
2429   0    yes

CASA#show cable modem partial-service
Reason code: x/y/z(reason_code)
  1 MDD timeout               2 FEC lock failure
  3 Bad tcc                   4 Bad rcc
  5 Reg ack                   6 DBC rsp
  7 TR power bad              8 NCP profile failure
  9 Impaired channel         10 Channel unreachable
 11 Range timeout            12 Ranging failure
  0 Unknown

MAC Address    MAC US       DS     US  DS US/DS  CHAN EXCLUDED
               id  Intf     Intf   SET SET
0025.08eb.74bc 63  12/0.0/0 2/0/31 256 257(3*23) 12/0.0w(3)
-output cut-

CASA#show cable modem bonding
Reason code: x/y/z(reason_code)
  1 MDD timeout               2 FEC lock failure
  3 Bad tcc                   4 Bad rcc
  5 Reg ack                   6 DBC rsp
  7 TR power bad              8 NCP profile failure
  9 Impaired channel         10 Channel unreachable
 11 Range timeout            12 Ranging failure
  0 Unknown

MAC Address   MAC US         DS      US  DS           US/DS CHAN EXCLUDED
               id Intf       Intf    SET SET
0024.d11e.4600  1 10/0.3/0  0/1/6   256 258(4*8)
-output cut-
c0cb.38d3.7c35  1 10/0.2/0  0/0/6   256 257(2*8)     10/0.0/0(5),
10/0.3/0(5)

CASA# show cable flap-list
MAC Address Us-Int   Ins Hit Miss(%)   CRC P-Adj ARP-TO Flap Time
0005.caa3.x 10/0.1/0 210 99  10(9.2 %) 0   18 0  228    2014-07-10,14:30:54
0013.f735.x 10/0.0/0 25  207 70(25.3%) 0   61 0  86     2014-07-10,14:06:49

CASA# show cable modem cm-status log
MAC Address Status_Event Msg Content Time
0022.68f2.d99c QAM_FEC_RECOVERY DS: 3 2014-09-09 13:47:28
0022.68f2.d99c QAM_FEC_RECOVERY DS: 2 2014-09-09 13:47:28
0022.68f2.d997 QAM_FEC_RECOVERY DS: 5 2014-09-09 13:47:28

CASA# clear cable modem partial-service
```

3.6. Troubleshooting Cable Modem Initialization

Troubleshooting cable modem initialization can be divided into three components: troubleshooting QAM lock, troubleshooting ranging, and troubleshooting CM provisioning and registration.

3.6.1. Overview: Cable Modem Initialization

Diagram: Docsis 3.0 Initialization Process



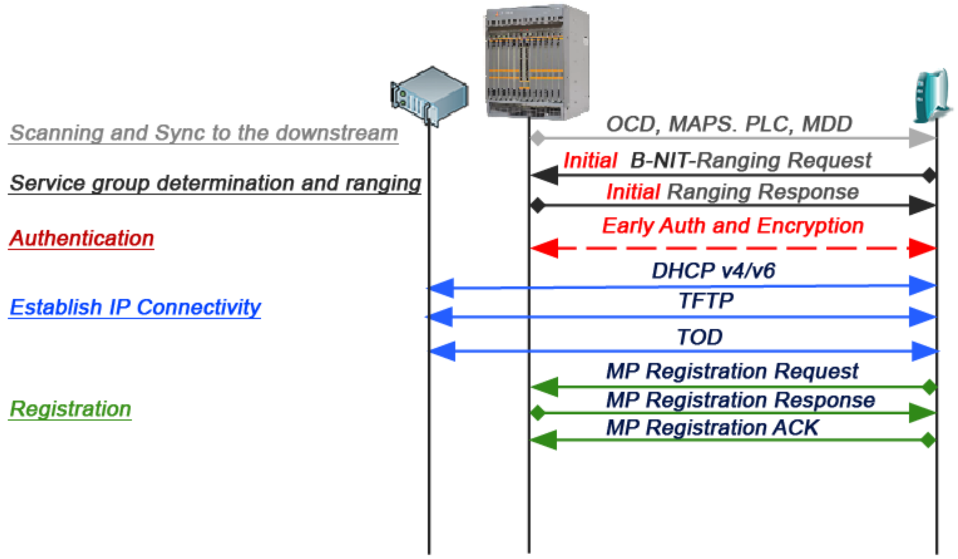
In the DOCSIS 3.0 initialization process, the CM must first find and lock to a downstream DOCSIS primary channel. Downstream acquisition consists of QAM lock, FEC lock, and synchronization of MPEG framing.

Once it has done so, the CM moves into the ranging process. This process initializes the DOCSIS layer and validates the communication path between the CM and CMTS over the HFC network. It then enables Early Authentication and Encryption, if configured, and obtains an IP address, its configuration file, and the Time Of Day.

Finally, the CM moves through the certificate validation process, enables BPI(+), and comes online.

The DOCSIS 3.0 MULPI describes the process in detail.

Diagram: Docsis 3.1 Initialization Process


Scanning and Sync to the downstream
Service group determination and ranging
Authentication
Establish IP Connectivity
Registration
OCD, MAPS. PLC, MDD
Initial B-NIT-Ranging Request
Initial Ranging Response
Early Auth and Encryption
DHCP v4/v6
TFTP
TOD
MP Registration Request
MP Registration Response
MP Registration ACK

The DOCSIS 3.1 cable modem initialization process follows the same architecture as the DOCSIS 3.0 process. It, too, can be divided into five phases: Scanning and Sync to the downstream, Service Group Determination and Ranging, Authentication, Establishing IP Connectivity, and Registration. However, DOCSIS 3.1 introduces a new series of MAC management messages in the initialization process.

The DOCSIS 3.1 MULPI describes the process in detail, including what happens when initialization fails. The link below opens a presentation describing a successful initialization.

3.6.1.1. Video Presentation on DOCSIS 3.1 Cable Modem Initialization

Click here for a video presentation on this topic.

3.6.2. Troubleshooting QAM Lock

If the CM cannot obtain QAM lock, it cannot range. Your troubleshooting options will be limited.

3.6.2.1. Video Flow Chart on Troubleshooting QAM Lock

Click here for a video troubleshooting flow chart on this topic.

The flow chart contains the commands below.

```
Verify the number of modems that are having QAM lock problems.

Confirm the state of the cable modem.

If the CM does not have QAM lock, verify the CCAP configuration. If the CM
does have QAM lock, move to the Troubleshoot Ranging process.

To verify the configuration of a single DOCSIS-MAC domain, type, show
interface docsis-mac <domain number> brief.

To verify the downstream channels in a DOCSIS-MAC domain, type show
downstream channel set mac-domain <domain number>.

To verify the parameters of a service group, type show service group
<service group name>.

To verify the downstream channels in a service group, type show md-ds-sg
service-group <service group name>.

To verify the configuration of the downstream channels, type show interface
qam <qam number>.

Ensure the modem is powered up and connected to the RF plant. Check the QAM
lock LED. If it is flashing, the modem is alive, but cannot acquire a
downstream channel. Proceed to RF Plant Diagnostics.

Check monitoring points.

Confirm nearby modems are online.
```

3.6.3. Troubleshooting Initial Ranging

The CMTS gives you multiple tools for troubleshooting ranging problems. Access information on those tools using the links below.

3.6.3.1. Video Presentation on Troubleshooting Initial Ranging

Click here for a video presentation on this topic.

During initialization, the CM goes through a number of steps before becoming fully operational on the DOCSIS network. The full initialization sequence is detailed in Section 10, but at a high level comprises four fundamental stages: 1) topology resolution and physical layer initialization, 2) authentication and encryption initialization, 3) IP initialization, and 4) registration (MAC layer initialization).

In the first stage, topology resolution and physical layer initialization, the CM acquires a single downstream channel (either via a stored last-known-good channel, or by scanning the downstream channel map) and receives broadcast information from the CMTS that provides it with enough information to identify what set of downstream channels are available to it, as well as what upstream channels might be available. The CM then attempts to initialize the upstream physical layer by "ranging" on a selected upstream channel. Via a series of attempts and alternative channel selections, the CM succeeds in contacting the CMTS and completing the ranging process. At this point, the CMTS has located the CM in the plant topology (i.e., is aware of what downstream channels and upstream channels physically reach the CM) and has established two way communication via a single downstream/upstream channel pair. While this section has referred to the first stage in terms of physical layer initialization, a provisional MAC layer initialization has been performed, with the full initialization of the MAC layer being deferred to the final stage.

3.6.3.2. Video Flow Chart on Troubleshooting Initial Ranging

Click here for a video troubleshooting flow chart on this topic.

The flow chart contains the commands below.

```
Configure the CCAP to gather T3 and T4 timeout information from the
configure DOCSIS MAC interface context, using the commands below.

CASA(conf-if-mac 1)#cable cm-status event 6 max-timer 30 max-number 30
CASA(conf-if-mac 1)#cable cm-status event 7 max-timer 30 max-number 30
CASA(conf-if-mac 1)#cm-status event report
```

3.6.4. Troubleshooting Cable Modem Provisioning and Registration

The provisioning and registration process is complex, but you have multiple tools for troubleshooting this part of the initialization process. The link below describes some of those tools.

3.6.4.1. Video Presentation on Troubleshooting Cable Modem Provisioning and Registration

Click here for a video presentation on this topic.

The second stage of provisioning, authentication and encryption initialization, involves the CM sending its X.509 digital certificate (including the CM's RSA public key) to the CMTS for validation. If the CM has sent a valid certificate, the CMTS will respond with a message that triggers the exchange of AES (or DES) encryption keys that are used to encrypt the upstream and downstream data transmissions from this point forward. This "Early Authentication and Encryption" can be disabled. If so, the CM will attempt authentication and encryption initialization after the registration stage. The details of the authentication and encryption initialization process are provided in [DOCSIS SECv3.0].

In the third stage, IP initialization, the CM acquires an IP address in the Cable Operator address space, as well as the current time-of-day, and a binary configuration file. DOCSIS 3.0 defines use of IP version 4 and IP version 6 and four provisioning modes: IPv4 Only, IPv6 Only, Alternate, and Dual-stack. For IPv4 Only provisioning, the CM uses DHCPv4 to acquire an IPv4 address and operational related parameters. To facilitate compatibility with existing provisioning systems, this process is identical to the DOCSIS 2.0 CM provisioning process. For IPv6 Only provisioning, the CM uses DHCPv6 to acquire an IPv6 address and operational parameters. The CM uses the IPv6 address to obtain the current time-of-day and a configuration file. For Alternate Provisioning Mode (APM) the CM combines the first two provisioning modes, IPv6 Only and IPv4 Only, in sequential order, attempting IPv6 provisioning first and, if this fails, attempting IPv4 provisioning next. In the first three provisioning modes, IPv6 Only, IPv4 Only, and APM, the CM operates with only one IP address type (v4 or v6) at any given time, and thus these modes are called single-stack modes. For Dual-stack Provisioning Mode (DPM), the CM acquires both IPv6 and IPv4 addresses and parameters through DHCPv6 and DHCPv4 almost simultaneously, prioritizing the use of the IPv6 address for time-of-day and configuration file acquisition. In this mode, the CM makes both the IPv4 and the IPv6 addresses available for management.

The fourth stage, registration, involves a three-way handshake between the CM and the CMTS in which the CM passes certain contents of the configuration file to the CMTS, the CMTS validates the contents, reserves or activates MAC layer resources based on the service provisioning information that it received, and communicates MAC layer identifiers back to the CM. Once the CM acknowledges receipt of the CMTS's response, the MAC layer initialization is complete.

After the CM completes initialization, it is a manageable network element in the operator's IP network. The CM supports SNMP (as mentioned above), and responds to queries directed to the IP (v4 or v6) address that it acquired during initialization. DOCSIS 3.0 also supports a dual-stack operational mode in which the CM is manageable via both IPv4 and IPv6 addresses simultaneously. This mode is initialized (i.e., the CM acquires a second IP address) after the CM is operational. This feature is also intended to help provide a streamlined migration from IPv4 to IPv6 in DOCSIS networks.

3.6.5. Troubleshooting Cable Modem Performance

The number of factors that can affect CM throughput can make your CM performance troubleshooting efforts both scattered and inefficient. A good approach is to work from the bottom up:

- Check that your RF power is OK, and troubleshoot RF power if it is not
- Check that your SNR is OK, and troubleshoot SNR if it is not
- Check that your FEC errors are OK, and troubleshoot your cable plant if it is not

3.6.5.1. Video Flow Chart on Troubleshooting Cable Modem Performance Issues

Click here for a video troubleshooting flow chart on this topic.

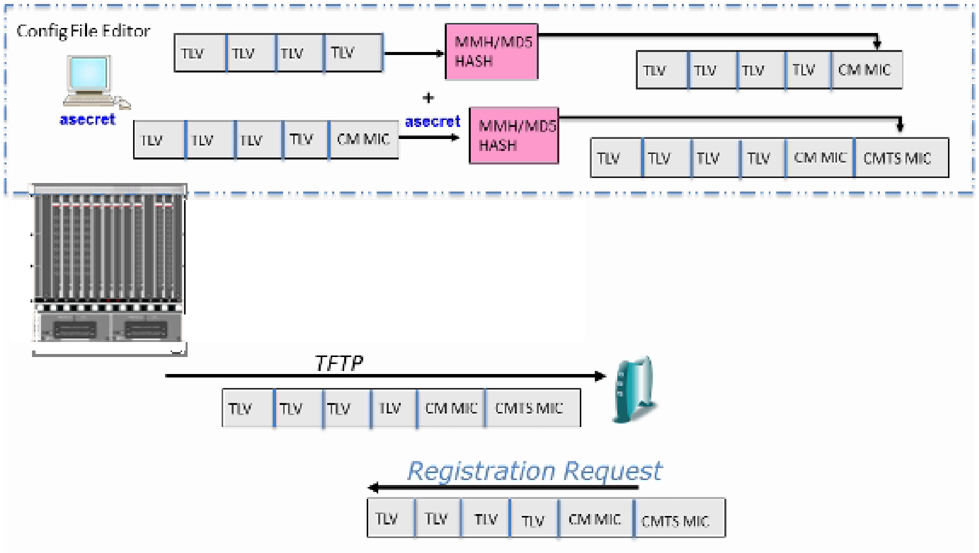
3.6.6. Verifying Baseline Privacy Interface Configuration

3.6.6.1. Overview: Cable Modem Security

DOCSIS 3.0 builds on the security built into previous versions of DOCSIS, namely, BPI and BPI+. Although DOCSIS 3.0 still uses BPI+ to protect customer traffic it has added an open peer reviewed encryption technique; the Advanced Encryption Standard, AES, to the algorithm suite.

Additionally, BPI+ has added Early Authentication and Encryption, or EAE. This security protocol if enabled will encrypt the traffic from the CM after initial ranging is complete.

Diagram: Message Integrity Check



The CMTS Message Integrity check (MIC) has been around since the DOCSIS 1.0 protocol. This Message Integrity Check feature is often referred to as the shared secret. Its primary purpose is to verify that the source of the configuration file downloaded to the cable modem is from an authorized tftp server.

When a configuration file is created on the provisioning server or a standalone configuration file editor, two MIC values are created, using either an MD5 or MMH hashing function. The first MIC, or the CM MIC, is a mandatory hash of the values in the configuration file; this hash value is inserted in the CM MIC field in the configuration file. The second MIC, or the CMTS MIC, is an optional hash of the values in the configuration file, including the CM MIC plus an operator configured ASCII string called the shared secret.

To enable this function in DOCSIS, the operator must configure the same shared secret on the CMTS. The Casa CMTS supports up to two shared secrets, and is configured with the shared-secret command in config mode.

Release 7.2 provides two security enhancements. A cable modem that registers with a mismatched DOCSIS shared secret now appears as offline with a MAC status of **offline(m)** in a **show cable modem** command output. The status indicates that the CM failed the message integrity check (MIC) and was put offline. The **show cable modem rogue** command indicates the configured shared secret of the rogue CM.

In addition, the **show cable modem [<mac-address>] privacy verbose** command output has been enhanced to display Baseline Privacy Interface (BPI) state information for both online and offline modems.

3.6.6.2. Video Use Case on Verifying Provisioning Security for DOCSIS 3.0 Cable Modems

Click here for a video use case on this topic.

The use case contains the commands below.

```
To view the cable security options on the CCAP, from config mode type, cable
sec ?

CASA(config)#cable sec ?
cert-revocation-list      Cert Revocation List
cert-revocation-method    Certificate Cert Revocation Method
config-file-learning      enable configuration file learning functionality
eae-exclusion             config EAE exclusion
encrypt_alg_priority      encryption algorithms for cable modem
modem-cert                cable modem certification
ocsp                      Online Cert Status Protocol
sav-auth-enable           enable sav auth for cable modem
sav-cfg-list              config sav rule
tftp-options              Server tftp options
CASA(config)#

To view the cable privacy options on the CCAP, from config mode type, cable
privacy ?

CASA(config)#cable privacy ?
40-bit-des                40-bit DES encryption
add-certificate           add a manufacturer or root CA certificate to the
list of trusted certificates
bpi-enforce               prohibits traffic for non-bpi-authenticated CM
bpi-plus-enforce          Enforce bpi-plus for DOCSIS1.1 or higher CM
test-edrca-certificate    EDRCA certificate for test purpose
CCAP1(config)#

To verify the cable security configurations on the CCAP, type show run | beg
“cable sec”.

CASA#show run | beg "cable sec"
cable sec encrypt-alg-priority des56CbcMode des40CbcMode aes128CbcMode

no cable sec modem-cert check

cable sec tftp-options net-addr

View your cable privacy configurations on the CCAP with the command, show
run | beg “cable privacy”.


CASA#show run | beg "cable privacy"
cable privacy bpi-enforce mandatory


cable privacy bpi-plus-enforce mandatory

 To verify that a shared secret is configured on the CCAP, type show run |
inc “shared-secret”.

CASA#show run | inc "shared-secret"
shared-secret 7
24392463393761623965353933386337396565246435396330636263373862 31
3634643963373766653661383233663732386666
CASA#
```

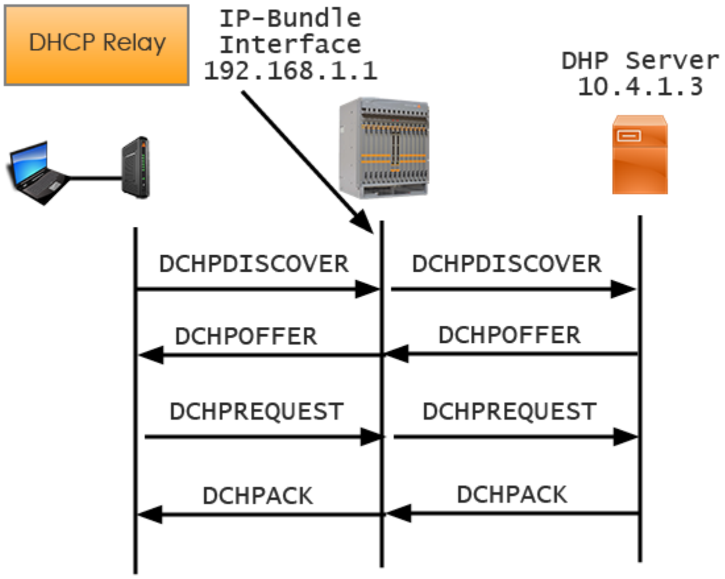
3.7. Verifying Cable Modem Operations Support System (OSS)

Overview

The Casa CMTS offers four IP-based functions on the RF interface: DHCP Relay, which is called "IP Bundle", CPE Host Management, DHCP Host Authorization, and TFTP Proxy/TFTP Enforce.

3.7.1. DHCP Relay for IPv4

Diagram: DHCP Relay for IPv4



The CMTS uses the Dynamic Host Configuration Protocol (DHCP) to request IP addresses from a DHCP server for CM and CPE devices that are registering with the CMTS. DHCP Discover, Offer, Request, and Acknowledgment messages are exchanged between the DHCP client and server. The DHCPACK message returns (broadcasts) the offered IP configuration to the DHCP client.

Cable helper addresses specify the IP destinations of one or more DHCP servers for UDP broadcasts from both CMs and CPE devices. These cable helper addresses are specified in the IP bundle configuration in a DOCSIS MAC domain.

To create or enter an IP-bundle interface, use the interface ip-bundle command in configuration mode.

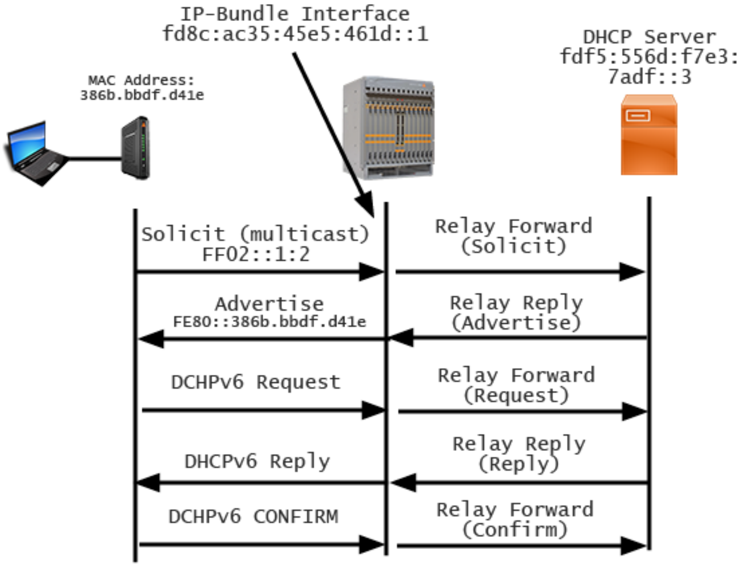
3.7.1.1. IP Bundles

The IP Bundle interface feature allows multiple cable interfaces to share a single IP subnet. Without the use of this feature, each interface must be configured with a separate IP subnet. For users with limited IP address space, assigning a separate IP subnet to each interface can consume limited IP address resources. It essentially configures the cable interface to function as a DHCP relay agent.

Cable bundling also allows for more scalable network designs by avoiding the need to reassign IP addresses as new service groups and mac domains are added to compensate for growth in the network.

Up to 16 IP bundles are supported and as of release 7.2 the CMTS/ CMTS now supports up to maximum of 2000 sub-interfaces system wide, in a single bundle or over multiple bundles. In addition, the IP sub bundle numbering has been expanded to 1023.

3.7.1.2. DHCP Leasequery for IPv6



The dhcp leasequery and the dhcpv6 leasequery commands configure the Casa CMTS to send DHCP leasequery requests to the DHCP server. The dhcp leasequery enforce or dhcpv6 leasequery enforce parameter must be set at the DOCSIS MAC interface, along with the dhcp-authorization enable on the IP bundle interface, for DHCP leasequery to work. Since leasequery uses the dhcp.conf file at the DHCP server, do not set an IP address on CPE/PC devices. The TCP/IP properties on these devices must be set so that IP addresses are obtained automatically from the dhcpd.conf host setting.

Two rules apply when setting leasequery for a device:

1. If the device's IP address is in the primary, secondary, or host range as set for the IP bundle, the leasequery request is sent to all cable helper-addresses (except those marked with the cable-modem keyword).
2. If the device's IP address matches a CPE class or multimedia terminal adapter (MTA) range, the leasequery request is sent to all the specific cable helper-addresses that are an exact match. Otherwise, Rule 1 applies.

3.7.2. CPE Host Management

The CMTS allows you to classify customer premises equipment (CPE) devices, such as IP phones, personal computers, and set-top boxes so that DHCP requests from those

CPEs for IP addresses are forwarded by the CMTS to specific DHCP servers. The maximum number of CPEs is 13,1072.

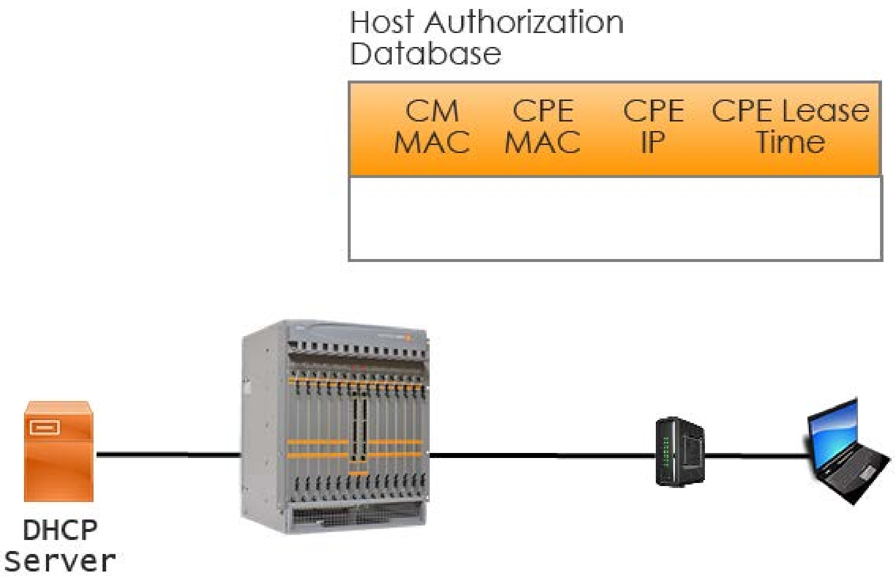
Using the cpe-class command, you can define a named CPE class grouping, and then specify any number of DHCP option 60 strings that the CMTS will match to configured DHCP server IPs. When the CMTS receives a DHCP option 60 string from a vendor CPE device, the CMTS checks the IP-bundle and cable helper addresses for a matching string. If the string matches, the CMTS forwards the request to the DHCP server IP address and awaits a DHCP response that the CMTS returns to the requesting CPE.

3.7.2.1. Video Presentation on Cable Modem IP Operations

Click here for a video presentation on this topic.

3.7.3. DHCP Host Authorization

Diagram: DHCP Host Authorization



Host Authorization Database

CM MAC	CPE MAC	CPE IP	CPE Lease Time

The CMTS implements DHCP host authorization as an anti-spoofing measure. It is designed to verify legal service, and block theft of service sourced by customers.

When you enable DHCP authorization, the DHCP Relay Agent on the CMTS snoops all DHCP traffic and keeps the information in a lease information database, called the “host authorization database”. The CMTS stores the CM MAC, CPE MAC, CPE IP, and CPE Lease Time for every authorized CPE device.

The implementation is the same for IPv4 and IPv6:

3.7.3.1. Video Presentation on DHCP Host Authorization

Click here for a video presentation on this topic.

3.7.4. TFTP Proxy and TFTP Enforce

Once a CM is assigned an IP address, the CM submits a request to a target TFTP server for the CM configuration file. This file provides operational information to the CM using parameters that are set by the cable service provider, including program identification to the MAC domain. The TFTP server, as programmed into each CM, responds to the request by forwarding and loading the configuration file to the CM at the DHCP-assigned address.

Use the tftp-proxy command on the DOCSIS-MAC interface to allow CMs to get the CM configuration file from a TFTP server.

The tftp-enforce command enables the CMTS to reject registration requests from CMs on the specific MAC domain. CMs must first download their configuration files from a TFTP server before the CMs are allowed to register with the CMTS.

3.7.4.1. Video Presentation on TFTP Proxy and TFTP Enforce

Click here for a video presentation on this topic.

3.8. Verifying QoS Configurations

Overview

The Casa CMTS supports quality of services (QoS) as defined by the DOCSIS 1.0, 1.1 specifications. Service classes can be configured to support the QoS profile number, traffic priority, maximum upstream bandwidth, guaranteed upstream bandwidth, maximum downstream bandwidth, maximum transmit burst length, baseline privacy enable/disable, and type of service (ToS) overwrite byte.

3.8.1. QoS support in DQM modules

The DOCSIS QAM Module (DQM) provides QoS support through a two-level hierarchical scheduler. The top level is priority based, and the second level is a fair scheduler based on round robin. Each packet destined for a downstream interface is assigned a service flow through classification by the DOCSIS forwarding engine. The scheduler in the DQM module supports a minimum guaranteed rate and a maximum transmitted rate. Packets are serviced in the order of priority specified by the service flow. A service flow that is within minimum guaranteed rate is served first. Within the same priority, round robin is used to schedule between different service flows, unless service flow weighted fair queuing (WFQ) is enabled.

If the service flow has a minimum guaranteed rate and the current rate is within the one specified, the packet is queued in the guaranteed class that has the highest priority. The packet is subsequently rate limited through a token bucket to conform to the maximum transmitted rate specified for the service flow. Packets that exceed the maximum transmitted rate are rate-shaped by deferring their transmission. Packets are dropped only if the buffer utilization is high and the buffer usage by the service flow is above the drop threshold.

The packet scheduler is driven by availability of transmission opportunities on the downstream channel. The scheduler can provide millisecond level latency guarantees for high priority traffic through the use of shallow transmit queues. Every time a channel transmit queue becomes available, the scheduler services the service flows in the order of priority until the transmit queue is full or all eligible packets are serviced. For downstream channel bonding operation, the service flow is serviced by each of the channels in the bonding channel set in parallel.

3.8.2. QoS support in DCU modules

In the DOCSIS Control and Upstream (DCU) module, the upstream scheduler handles modem transmission opportunities. In addition to providing minimum guaranteed rate and rate limiting support, it also provides jitter guarantees for jitter-sensitive services, such as unsolicited grant service (UGS). The hierarchical upstream scheduler serves upstream service flows based on priority. Jitter-sensitive service flows are serviced first, followed by service flows that are within its guaranteed rate. Best effort service flows are then serviced in the order of priority. Within each priority, the service flows are serviced by a round robin scheduler.

For best effort services, the minimum guaranteed rate is checked first. If the transmission rate of the service flow is within its specified guaranteed rate, the request is placed in the guaranteed queue, which is serviced before other best effort queues. A token bucket is used to rate-limit the service flow within its configured maximum transmission rate and maximum burst size. Requests that exceed the maximum transmission rate are deferred. Requests that conform to the maximum transmission rate are placed into the queue determined by the priority of the service flow.

Jitter-sensitive service flows are scheduled by the real-time scheduler. To provide jitter guarantees, the transmission opportunities are pre-allocated when the service flow is admitted to prevent overlap. At MAP generation time, the real-time scheduler aggregates jitter-sensitive grants into clusters. The best effort grants are then placed into the gaps between the real-time grant clusters. If the gap is not big enough, the cluster is allowed to move to increase the gap, as long as jitter guarantees can be met for the real-time grants in the cluster. If the gap is still not enough to place the best effort grant, the best effort grant is then fragmented. The scheduler keeps track of the remainder of the fragments and continues to serve the fragments until the request is fulfilled.

For service flows that are serviced by upstream channel bonding, the service flow is inserted into multiple queues, one for each of the upstream channels in the bonding channel set. The service flow is serviced by each of the upstream channels until all the outstanding bytes requested are served.

3.8.3. QoS support in switch fabric and Gigabit Ethernet interfaces

The switch fabric connects to the RF modules and Gigabit Ethernet interfaces. Each of the fabric ports supports eight classed-based queues. The scheduler in the switch fabric is straight priority. For packets entering the switch fabric from the DCU module, the priority is determined by the priority value in the upstream service flow. For packets entering the switch fabric from Gigabit Ethernet interfaces, the priority is from the 802.1p field if the packet is VLAN-tagged. For untagged packets, the DSCP value in the IP header is used to determine the priority. The filtering engine can be used to overwrite the DSCP value using access list. The priority value can also be modified based on access lists.

To prevent head-of-line blocking, the switch fabric keeps track of the outstanding buffer count and packet count for each of the ingress ports and each of the classes. When an egress port on the switch fabric becomes congested, a packet is discarded at ingress if the outstanding buffer count or packet count from the ingress port exceeds the discard threshold for the class it belongs to.

3.8.4. Video Use Case on Verifying QoS Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show cable modem qos
Sfid     Dir Curr  Sid  Sched  Prio MaxSusRate MaxBrst MinRsvRate
PeakTrafRate Throughput ServiceClassName
             State      Type        (kbps)             (kbps)     (kbps)
(kbps)
Mac Addr : 5c35.3b4a.a0f6
196645   US  act   285  BE     0    0          64000   0          0
0

196655   US  act   382  BE     1    0          64000   0          0
0

196656   US  act   383  BE     2    0          64000   0          0
0

196657   US  act   384  BE     3    0          64000   0          0
0

196658   US  act   385  BE     4    0          64000   0          0
0
-output cut-

CASA#show qos-profile
index = 10

CASA#show pcmm ps server
IP Address    Port  PSID Version
24.114.21.102 56275 null 5.0

CASA#show packetcable gate
GateID SubID        Type State  Dir  PDPIP          RKSIP
0xf    10.162.1.199 PCMM COMMIT down 192.168.57.145 192.168.55.49
```

3.9. Verification and Troubleshooting of DSG and PCMM

Overview

The Casa CMTS supports the latest PacketCable specification from CableLabs™. Those PacketCable features offer an end-to-end solution for traffic that originates or terminates on a cable network, simplifying the task of providing multimedia services over an infrastructure composed of disparate networks and media types. It also provides an integrated approach to end-to-end call signaling, provisioning, quality of service (QoS), security, billing, and network management.

3.9.1.1. Video Use Case on Verifying PacketCable Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show packetcable global
**********PacketCable Global***********
PacketCable: enable
Element ID: 9999
PEP ID: casa@packet.cable
MyIPaddr: 0.0.0.0
Gate ID Used: 0
Max Gate: 19660
COPS Server Listen Port: 2126
RKS_Receive_Port: 1813
PCMM Listen Port: 3918
PCMM version: 5.0

CASA#show packetcable log
697

CASA#show packetcable rks server
IP Address Port Timeout Retry Batch_file File_mode File_size File_max_msg

CASA#show packetcable gate
GateID SubID        Type State  Dir PDPIP           RKSIP
0xf    10.162.1.199 PCMM COMMIT down 192.168.57.145 192.168.55.49

CASA#show packetcable gateid 0 dspec
Packetcable gateid 0x0 downstream failed.

CASA#show packetcable commit gate
Packetcable committed gates count is 0

CASA#show packetcable cms server
IP Address Port

CASA#show packetcable mgpi
```

3.9.1.2. Video Flow Chart on Troubleshooting a Specific PCMM Issue

Click here for a video troubleshooting flow chart on this topic.

3.9.2. Verifying DOCSIS Set-Top Gateway Configuration

The CASA CMTS supports the latest DOCSIS Set-Top Gateway (DSG) specification from CableLabs. As a specification for transporting set-top box (STB) command and control information over DOCSIS, DSG offers substantial support for enhanced DOCSIS implementation in the Broadband Cable environment. It provides transparent unidirectional and bidirectional transport of out-of-band (OOB) service messaging over IP between the CMTS and STBs over hybrid fiber coaxial (HFC) networks.

Types of OOB messages include conditional access (CA), system information (SI), electronic program guide (EPG), emergency alert system (EAS), and other generic messages.

3.9.2.1. Video Use Cases on Verifying DSG Configurations

Click here for a video use case on this topic.

The use case on Verifying DSG Configurations contains the commands below.

```
CASA#show dsg running-config
dsg tunnel-group 1
dsg tunnel-group 2
dsg tunnel 1
classifier 1 255 192.168.8.8/24 224.0.0.100 indcd 6666 6667
dsg channel-list 1 channel 1 frequency 62500
dsg unicast-port 8888
```

```
CASA#show dsg channel-list
dsg channel-list 1 channel 0 frequency 62500

CASA#show dsg qam
interface qam 0/0
interface qam 0/1
interface qam 0/2
interface qam 0/3
interface qam 0/4
interface qam 0/5
interface qam 0/6
interface qam 0/7
interface qam 4/0
interface qam 4/1
interface qam 4/2
interface qam 4/3
interface qam 4/4
interface qam 4/5
interface qam 4/6
interface qam 4/7

CASA#show dsg timer

show dsg downstream [<slot>/<port>/<chan>] {dcd | decoded-dcd | tg
[<1:4294967295> channel <1:4294967295>] | tunnel [<1:4294967295>]}

CASA#show dsg downstream dcd
ds dcd  dcd       num of dcd num of dcd  num of
i/f     state Tx  sent       change cnt  fragment
0/1/0   dis   off 0          0           0
0/1/1   dis   off 0          0           0
0/1/2   dis   off 0          0           0
0/1/3   dis   off 0          0           0

CASA#show dsg client-list
dsg client-list 1 client 1 id-type broadcast id-value 2048
vendor-param-id 2

CASA#show dsg vendor-param
dsg vendor-param-id 1 vendor 1 oui 01:02:03 value abc
```

The use case on Verifying DSG Tunnel Configurations contains the commands below.

```
CASA#show dsg tunnel 1
group 1
dst-address 0100.5e40.100b
client-list 1
classifier 1 1 0.0.0.0/0 239.192.16.11 indcd
dst-address <mac_addr>

CASA#show dsg tunnel-group
channel 1 qam x/y/z rule-priority 20 vendor-param-id 1 ucid-list 1
channel 2 qam x/y/z rule-priority 30 vendor-param-id 500 ucid-list 2

CASA#show dsg tunnel
dsg tunnel 1
group 1
dst-address 0100.5e01.6401
service-class "video-DS"
classifier 1 2 0.0.0.0/0 224.11.11.1 indcd 3001 30011
classifier 11 2 0.0.0.0/0 224.22.22.1 indcd 3001 30011
dsg tunnel 2
```

```
group 2
dst-address 0100.5e01.6402
service-class "video-DS"
classifier 2 2 0.0.0.0/0 224.11.11.2 indcd 3001 30011
classifier 12 2 0.0.0.0/0 224.22.22.2 indcd 3001 30011

show cable dsg tunnel [<id> [cfrs | clients | interface | verbose]]

CASA#show cable dsg tunnel 1
tunnel TG cfr tunnel rule rule client service
id state mac-addr id id state IF id state listId class
1 en 0100.5e40.100b 1 1 en 11/0/0 1 en 1
CASA(config)# show cable dsg tunnel 1 cfrs
cfr cfr cfr destination ip source ip srcPre d_port d_port
id state pri address address length start end
1 en 1 192.168.0.1 000.000.000.000 0 0 65535

CASA#show cable dsg tunnel 1 verbose
Tunnel ID : 1
State : en
MAC Addr : 0100.5e40.100b
TG Id : 1
Cfr Id : 1
State : en
Priority : 1
Dest IP : 239.192.016.011
Src IP : 000.000.000.000
Src Prefix Length : 0
Dest Port Start : 0
Dest Port End : 65535
Client List Id : 1
Client Id : 1
Client Id Type : Application ID 0x1
Interface : 11/0/0
Rule ID : 1

show dsg statistics [dcd | traffic]

CASA#show dsg statistics
DS Channel DCD
2/0/0 0
2/0/1 0

CASA#show multicast replication
multicast group config 1
Multicast Session
Module ReplID DSID(hex) SFID Type Chan(s)
```

3.10. BFD Verification and Troubleshooting

Overview

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. BFD also provides a consistent failure detection method rather than the different rates for different routing protocol HELLO mechanisms.

3.10.1.1. Video Use Case on Verifying BFD Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
show bfd [session [<src_addr> <dst_addr] [<intf> <id>] [detail]]

CASA# show bfd
BFD ID: 00 Start Time:Thu Jan 1 00:01:21 1970
BFD Admin State: UP
Number of Sessions: 4
Slow Timer: 1000 Image type: MONOLITHIC
Echo Mode: Enabled BFD Notifications disabled
Next Session Discriminator: 6

CASA# show bfd session
BFD ID: 00 Start Time:Thu Jan 1 00:01:32 1970
Sess-Idx Remote-Disc Interface Lower-Layer Sess-Type Sess-State
1 0 eth6 IPv4 Single-Hop Down
UP-Time Remote-Addr
00:00:00 172.16.8.1/32
Number of Sessions: 1

CASA# show bfd session detail
======================================================
Session Interface : eth6/0 Session Index : 1
Lower Layer : IPv4 Version : 1
Session Type : Single Hop Session State : Down
Local Discriminator : 1 Local Address : 172.16.8.50/32
Remote Discriminator : 0 Remote Address : 172.16.8.1/32
Local Port : 49152 Remote Port : 3784
Options :
…
Number of Sessions: 1
```

3.11. NSI MAC Layer Verification and Troubleshooting

Overview

The Casa CMTS provides both a network side interface (NSI) and a radio frequency interface (RFI). On the NSI, the CMTS provides Ethernet 10/100 Mbps (for system management), GigE, and 10GigE (C10G) interfaces to routing gateways and servers.

On the NSI, the CMTS functions as a full participant in your network, supporting VLANs, trunking, and Layer 2 VPNs at Layer 2.

3.11.1. References

NSI Configuration Guide and Command Reference for Casa Software Releases to 7.2

Casa Systems NSI Configuration Guide and Command Reference

SNMP MIBs and Traps Reference

CM-SP-L2VPN-I15-150528 Data-Over-Cable Service Interface Specifications Business Services over DOCSIS: Layer 2 Virtual Private Networks

IEEE 802.1Q-2014

IEEE 802.1p

IEEE 802.1ad

IEEE 802.1Qay-2009

IEEE 802.1Q-2011 (Supersedes both of the above)

IEEE 802.3ad (Superseded by IEEE 802.1AX-2014)

RFC 44447 Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)

RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks

3.11.2. Verifying Rapid Spanning Tree Protocol Configurations

The Rapid Spanning Tree Protocol (RSTP) provides fault tolerance by automatically reconfiguring the spanning tree topology as a result of bridge failure, breakdowns in a data path within the confines of the available Bridge LAN components, and automatic accommodation of any bridge port added to the Bridge LAN without the formation of transient data loop.

RSTP runs on both IPv4 and IPv6. Introduced as IEEE standard 802.1w, it now is fully incorporated into the IEEE 802.1D-2004 standard.

3.11.2.1. Video Use Case on Verifying RSTP Configurations

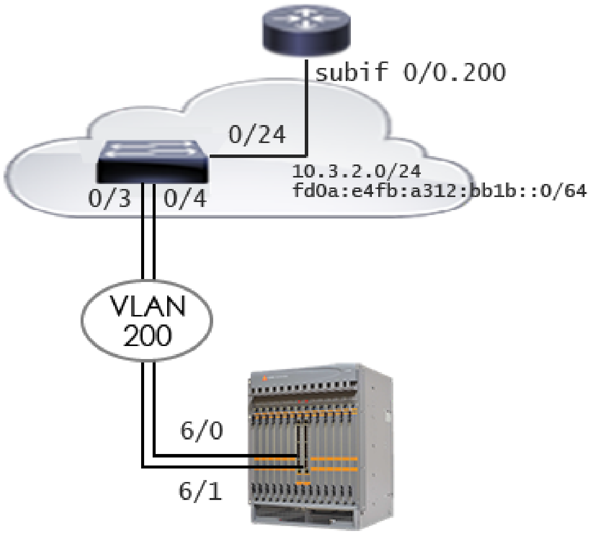
Click here for a video use case on this topic.

The use case contains the commands below.

```
show rstp bridge

CASA# show rstp bridge
---------------------------------------------
VLAN: 4095
BridgeId: F000-0050c2319902 Bridge Priority: 61440 (0xF000)
Designated Root: F000-0050c2319902
Root Port: none
Time Since Topology Change: 106512
Max Age: 20 Bridge Max Age: 20
Hello Time: 2 Bridge Hello Time: 2
Forward Delay: 15 Bridge Forward Delay: 15
Hold Time: 3

show rstp port

CASA# show rstp port
---------------------------------------------
trunk 1 : PortId: f015 in Bridge
Priority: 240
State: Forwarding Uptime: 106923
PortPathCost: admin: Auto oper: 20
Point2Point: admin: Auto oper: Yes
Edge: admin: Y oper: Y
Partner: oper: Rapid
PathCost: 20
Designated Root: F000-0050c2319902
Designated Cost: 0
Designated Bridge: F000-0050c2319902
Designated Port: f015
Role: Designated
TcAck: N TcWhile: 0
fdWhile: 0 rcvdInfoWhile: 0
rbWhile: 0 rrWhile: 0
RSTP BPDU rx: 0
CONFIG BPDU rx: 0
TCN BPDU rx: 0
L2VPN port Yes

show rstp stg

CASA# show rstp stg
------------------------------------------
Vlan List :
300 1308
------------------------------------------
Port List :
gige 6/1 trunk 1
```

3.11.3. Verifying L2 Configurations

Diagram: VLANs



The Casa CMTS supports 802.1q VLAN configuration for its SMM Ethernet interfaces and QAM ports. The software will support a maximum of 4094 VLANs.

From interface vlan <VLAN ID> configuration mode, you can assign an ACL to your VLAN. You can also associate your VLAN with a trunk interface with the trunk <trunk number> command.

If you have more than one configured trunk, you can add additional trunks to the VLAN as standby carriers with the trunk <trunk number> standby command.

3.11.3.1. Video Presentation on VLANs

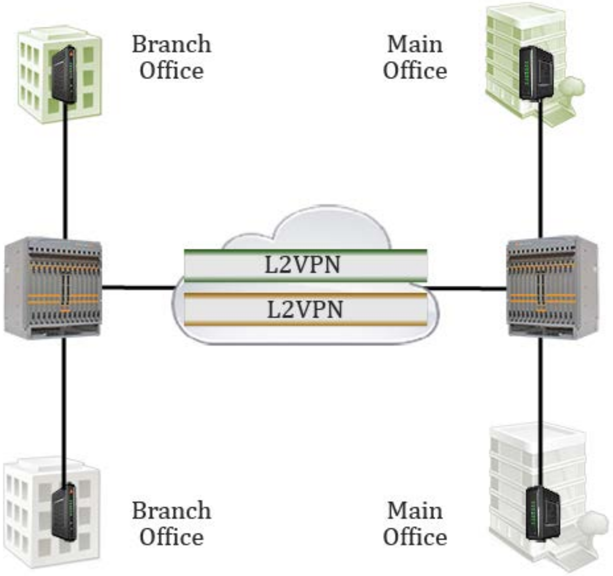
Click here for a video presentation on this topic.

3.11.4. Verifying Virtual Private Network Connections

Layer 2 Virtual Private Network (L2VPN) is a protocol that provides an end-to-end connection to an enterprise office over a Multi-Protocol Label Switching (MPLS) or IP core network.

L2VPN is primarily used by customers with multiple sites (like a business) who want all users to be on the same LAN by virtually connecting CMs and routers. The L2VPN is defined outside of the CMTS where the CM configuration file contains the information about the L2VPN. Because all L2VPN traffic is tagged before it reaches the CMTS, the CMTS knows which CMs are assigned to which L2VPN. When the CMTS receives the traffic tagged for a particular L2VPN, it strips off the tag and forwards the traffic to the CM. When the CM sends traffic to the CMTS, the CMTS adds the tag and forwards the traffic. The CMTS also recognizes local traffic and can send that traffic directly to another CM that is directly connected to it.

Diagram: QinQ Network



There are two types of VLAN tagging available. The first is IEEE 802.1q, the traditional method of VLAN tagging that adds a single tag to the frames. The second type adds a double tag, referred to as IEEE 802.1ad, or QinQ. The need for a second tag comes from the limited number of VLAN IDs available (only 4096) and the need from MSOs to create more unique VLANs. The number of VLAN IDs available in QinQ is over 16 million (4096*4096). Configuring the QinQ service requires the Tag Protocol Identifier (TPID) in the interface vlan, also referred to as the Ethertype, which sets the value for the outer tag when it is forwarded out the NSI port.

When planning an L2VPN implementation using VLAN tags, note that each L2VPN modem must be configured to receive its L2VPN configuration during registration. Multiple modems can share the same VLAN ID, but each VLAN must be configured on the CMTS and must be assigned a GigE port. When an L2VPN modem registers on the CMTS, some or all of its service flows are assigned to a VLAN. CPEs behind the modem do not use the IP bundle for DHCP provisioning, are not be visible in show cable modem <mac_addr> cpe output, and cannot reach IP addresses on the CMTS.

3.11.4.1. Video Presentation on L2VPNs

Click here for a video use case on this topic.

3.11.4.2. Business Services over DOCSIS

Casa also provides a Business Services over DOCSIS (BSoD) solution using L2VPN, allowing all CPEs that belong to an Alternative Operator (AO) to forward their traffic in L2VPNs via the CMTS.

As part of that support, as of the 7.2 release, you can now configure the CMTS to disable L2 broadcast traffic between two cable modems on the same VLAN. With this configuration, all L2 traffic will be forwarded to the upstream router. The upstream router will then redirect the traffic back to the CMTS. Use the no l2vpn mac-address-movable and no l2vpn local-traffic-forwarding commands to accomplish this.

In addition, you can now configure the CMTS to add DHCP Option 82 into cable modem L2VPN packets to allow the modem MAC address to be carried in the DHCP Request message from the modem and forwarded to the DHCP server. Use the l2vpn dhcp-insert option 82 command on a per-VLAN basis to enable this behavior.

The CMTS supports VLAN IP spoofing prevention for L2VPNs. This feature blocks packets coming from a CPE coming online that has an IPv4 or IPv6 address already associated with a different CPE MAC address. This feature is non-configurable.

Finally, you can now configure the CMTS to register a trap whenever BSoD/L2VPN modems deregister and go offline. Use either the l2vpn-cm-offline-only or the l2vpn-cm-on-offline-only command to implement this function.

3.11.4.3. Video Use Case on Verifying L2VPN Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show l2vpn mpls
l2vpn vlan table: vlan_id=4095

CASA# show l2vpn qam 1 mpls
lc: logical=1 phy=1
L2VPN US: ttl=0 drop=0 DS: ttl=0 drop=0 NotDefined pkt=0 id=0 bc_src=0
local: mac_addr_movable 0 traffic_fwd 0
l2vpn_vlan_tbl_prt():
l2vpn_addr_hs_tbl_prt():

CASA#show l2vpn vlan
l2vpn vlan table: vlan_id=0
vid in=300 out=2000 cm=43 lc=1 c0cb.38d3.7101 US 10/5.1/0* DS 1/1/1*
vid in=300 out=2000 cm=47 lc=1 e448.c714.c4f0 US 10/5.0/0 DS 1/1/0

CASA#show l2vpn vpnid
l2vpn vpnid 0123
nsi encapsulation 802dot1q 124
```

3.11.5. Verifying Label Switch Protocol Configurations

Overview

The *Label Distribution Protocol* (LDP) is used to support *Multi-Protocol Label Switching* (MPLS) forwarding along normally routed paths. It is a protocol defined for distributing labels. The routed path through the network is determined by the existing interior routing protocols (IGPs), such as RIP, OSPF, IS-IS and iBGP. LDP is based on RFC 3036, which was obsoleted by RFC 5036, *LDP Specification.*

LDP enables *label-switched routers* (LSRs) to request, distribute and release MPLS label prefix binding information to peer LSRs in a network. LDP also enables LSRs to discover potential peers and establish LDP sessions with those peers to learn the others’ label mappings. Each LSR in the network makes an independent, local decision to assign a label value to represent a *forwarding equivalence class* (FEC). When a labeled packet is being sent from LSR A to the neighboring LSR B, the label value carried by the IP packet is the label value that LSR B assigned to represent the FEC of the packet. The label value changes as the IP packet traverses the network.

Virtual Private LAN Service (VPLS) is a virtual private network (VPN) service to emulate Ethernet LANs on top of service provider IP or MPLS networks. It enables an enterprise to auto-discover and link its individual LANs in geographically dispersed sites through virtual circuits called *pseudowires* (PWs) to function as a single corporate LAN. A PW emulates a point-to-point connection on top of service provider IP or MPLS networks to carry the native traffic (such as Ethernet and other protocol traffic). VPLS is based on RFCs 4761 and 4762.

A VPLS instance is implemented by the *virtual forwarding instance* (VFI) that provides MAC address learning and aging, flooding, split-horizon forwarding, MPLS label processing capabilities, and forwarding over the upstream and downstream interfaces. Each VFI has *virtual ports* (VPs) that are dynamically added or deleted on the VFI. On the CMTS network side interface (NSI), a VP is added to the VFI when a PW is established by the signaling protocol for that VFI. Similarly, the VP is deleted from the VFI when a PW is removed by the signaling protocol. On the radio frequency (RF) side of the CMTS, a VP is added to the VFI when a participating CM is registered and in the online state. A VP is deleted from the VFI when the CM is offline and no longer registered at the CMTS.

Ethernet over MPLS (EoMPLS) is a *virtual private wire service* (VPWS) to encapsulate Ethernet frames in MPLS packets and forward them across the service provider MPLS network through virtual circuits (VCs) or *pseudowires* (PWs). A PW emulates a point-to-point connection on top of service provider IP or MPLS networks to carry the native traffic (such as Ethernet and other protocol traffic). EoMPLS is based on RFCs 4447 and 4448.

EoMPLS is implemented using *pseudowire emulation* (PWE) to provide *virtual port* (VP) cross-connecting, VLAN rewriting and stripping, priority mapping, label processing, and hardware forwarding over upstream and downstream interfaces. Unlike VPLS, each PWE has only two virtual ports that are dynamically added to the PWE. On the CMTS NSI side, the VP is added to the PWE when a PW is established by the signaling protocol for that PWE. The VP is removed when the PW is removed by the signaling protocol. On the RF side, a VP is added to the PWE when a participating CM is registered with the CMTS and is in the online state. The VP is removed when the CM is offline and no longer registered.

3.11.5.1. Video Use Cases on Verifying LDP and MPLS Configurations

Click here for a video use case on this topic.

The use case on Verifying LDP Configurations contains the commands below.

```
show mpls ldp fec
Shows the LDP forwarding equivalence classes (FECs) of the LDP
configuration.

show ldp targeted-peers
Shows the list of defined LDP targeted peers.
CASA(config)# show ldp targeted-peers
70.1.1.1 gige2/0
72.1.1.1 N/A

show mpls running-config

show mpls static binding ipv4

show mpls interfaces
CASA(config)# show mpls interfaces
Interface IP Tunnel Operational

show mpls label range
CASA(config)# show mpls label range
Range for dynamic labels (Min/Max): 16/1048575

show mpls vpls [<id> [detail]]
CASA(config)# show mpls vpls detail
VPLS Name: VPLS-Net1 ID: 100
Signaling Protocol: LDP
Local CMs (attachment circuits)
CM MAC Address US Intf DS Intf SID
D4:BE:D9:A8:A5:5C 0/1/2 4/3/2 8
00:17:10:03:60:C0 1/5/5 6/4/2 6
Neighbors Connected via PWs
Peer Address Network-Intf In-Label Out-Label Tunnel-label Status
1.1.1.1 gige 6/6 12 123 52310 Up
2.2.2.2 gige 7/2 13 63545 6302 Up
3.3.3.3 N/A N/A N/A N/A Dn

show mpls vpws xconnect [<id> [mpls-vc-map]]
CASA(config)# show mpls vpws xconnect
MAC Address Peer IP Address VC_ID US_Intf DS_Intf PSID State VPWSID
0000.1234.5678 1.2.3.4 22 3/2/0 6/2/1 8 Active vpws-A(s)
```

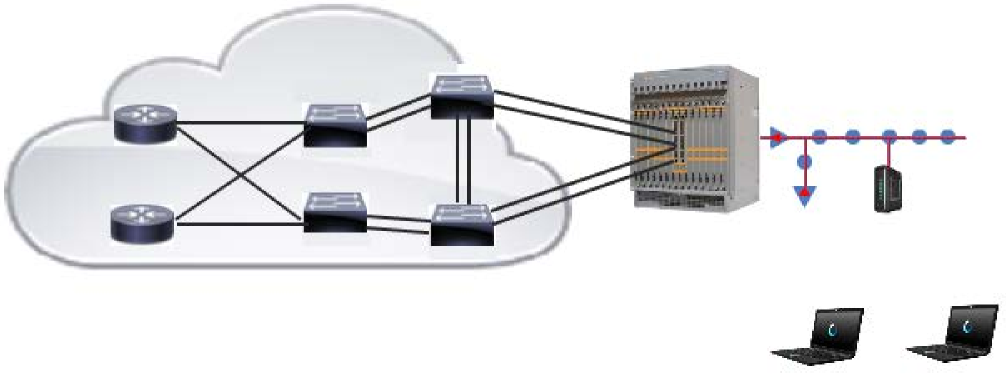
The use case on Verifying MPLS Configurations contains the commands below.

```
show mpls ldp discovery <interface>

show mpls ldp neighbor

show mpls ldp session [<addr>]

show mpls forwarding-table [<net_addr>/<mask> | labels | vrf <name>]
CASA(config)# show mpls forwarding-table
Codes: > - selected FTN, p - stale FTN, B - BGP FTN, K - CLI FTN,
L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
U - unknown FTN
Code FEC Tunnel-id FTN-ID Pri Nexthop Out-Label Out-Intf
R> 33.33.33.33/32 101 2 Yes 13.13.13.2 16044 xgige6/2
time
23:45:14

show mpls ftn-table

show mpls ilm-table

show mpls vc-table

CASA(config)# show mpls vpws xconnect mpls-vc-map
Peer Address PSID VC-ID In-Label Out Label Tunnel-Label
Network-Intf Control-Word
114.1.1.1 114 87042 25551 3
vlan471 enabled
199.1.1.1 199 87044 11424 0
vlan461 enabled
72.1.1.1 7 87043 87042 567
gige7/0 disabled

show ldp mpls-l2-circuit

CASA(diag)# show ldp mpls-l2-circuit
Code Transport Client VC VC Local Remote Destination
VC ID Binding State Type VC Label VC Label Address
101 vc-101 UP Ethernet 87042 27065 114.1.1.1
102 vc-102 UP Ethernet 87047 27066 114.1.1.1
…


show mpls ldp graceful-restart

CASA(config)# show mpls ldp graceful-restart
% No LDP instance configured. Enable with "router ldp" first.
```

3.11.6. Verifying LACP Configuration

Overview

Diagram: Trunks



Trunking is the use of multiple concurrent network connections to aggregate the link speed of each participating port and cable. In Ethernet networks, trunks can be created either statically, or dynamically using LACP.

The Casa CMTS supports the IEEE Link Aggregation Control Protocol (LACP) for controlling the bundling of several SMM physical ports together to form a trunk, which functions as a single logical connection to another router or switch.

The CMTS allows you to configure link aggregation groups (LAGs) both on a single SMM and across SMMs. LACP allows the exchange of information with regard to the link aggregation between the two members of the aggregated ports, regardless of the SMM the ports are on.

3.11.6.1. Video Presentation on Trunking and LACP

Click here for a video presentation on this topic.

3.11.6.2. Verifying LACP Activity

To verify LACP activity on a trunk, use the **show lacp summary** command, and examine the flags set on your interface.

```
CASA(config)# show lacp summary
Flag: A--LACP Activity, B--LACP Timeout, C--Aggregation,
D--Synchronization E--Collecting, F--Distributing, G--Defaulted,
H--Expired
Trunk  Port      Mode   State  Priority  Flag      Receive  Send
20     gige6/1 active  indep 32768    ACDEFG  0          41
20     gige7/1 active  bind   32768    ACDEF    42          38
```

Each flag gives you specific information about the LACP state of the interface.

Flag	Description
A--LACP Activity	The LACP_Activity flag indicates a participant's intent to transmit periodically to detect and maintain aggregates. If set the flag communicates Active LACP, if reset Passive LACP. A passive participant will participate in the protocol if it has an active partner.
B--LACP Timeout	The LACP_Timeout flag indicates that the participant wishes to receive frequent periodic transmissions , and will aggressively times out received information. If set, the flag communicates Short Timeout, if reset Long Timeout.
C--Aggregation	The Aggregation flag indicates that the participant will allow the link to be used as part of an aggregate. Otherwise the link is to be used as an individual link, i.e. not aggregated with any other. This flag is set or reset as a consequence of local key management : the participant may know that the link has a unique key and hence will not be aggregated. Signaling this information allows the receiving actor to skip protocol delays that are otherwise invoked to allow all links with the same system id and key combinations to be collected into one aggregate port without successive rapid changes to aggregate ports and accompanying higher layer protocol disruption. If set the flag communicates Aggregatable, if reset Individual.
D--Synchronization	The Synchronization flag indicates that the transmitting participant's mux component is in sync with the system id and key information transmitted. This accommodates multiplexing hardware that takes time to set up or reconfigure. If set the flag communicate In Sync, if reset Out of Sync.

E--Collecting	The Collecting flag indicates that the participant’s collector, i.e. the reception component of the mux, is definitely on. If set the flag communicates collecting.
F--Distributing	The Distributing flag indicates that the participant’s distributor is not definitely off. If reset the flag indicates not distributing.
G--Defaulted	This port has reset to its default state.
H--Expired	

3.11.6.3. Video Use Case on Verifying LACP Activity

Click here for a video use case on this topic.

The use case contains the commands below.

```
show lacp summary

CASA(config)# show lacp summary
Flag: A--LACP Activity, B--LACP Timeout, C--Aggregation,
D--Synchronization E--Collecting, F--Distributing, G--Defaulted,
H--Expired
Trunk Port Mode State Priority Flag Receive Send
20 gige6/1 active indep 32768 ACDEFG 0 41
20 gige7/1 active bind 32768 ACDEF 42 38

show lacp system-id

CASA(config)# show lacp system-id
System ID: 32768,00:17:10:02:cb:c1
```

3.12. NSI Network Layer Verification and Troubleshooting

Overview

On the Network Side Interface, the Casa CMTS functions as an IP device in your IP network, supporting both IPv4 and IPv6. As such, the verification and troubleshooting options available to you for observing and diagnosing the CMTS's IP functions are both broad and deep. This section provides only a brief overvew of those options; for further details please consult the Casa technical publications.

The "show ip" command is your path into beginning to verify your IP configurations. The table below displays your initial options for both the show ip and the show ipv6 commands.

show ip	show ipv6	Displays:
access-list		Access list configuration
bgp	bgp	BGP information
bundle		DOCSIS ip-bundle information
community-list		Lists community list
domain-name		Default domain name configuration
extcommunity-list		Lists extended community list
interface	interface	Interface status and configuration
isis	isis	IS-IS information
mroute		IP multicast routing table
multicast	multicast	Multicast information
	neighbor	IPv6 neighbors
ospf	ospf	OSPF/OSPFv6 information
pim		PIM information
prefix-list	prefix-list	Lists IP prefix lists
rip	rip	RIP/RIPng information
route	route	IPv4/IPv6 routes
vrf		Virtual route forwarding instance

3.12.1.1. Video Use Case on Verifying IP Configurations

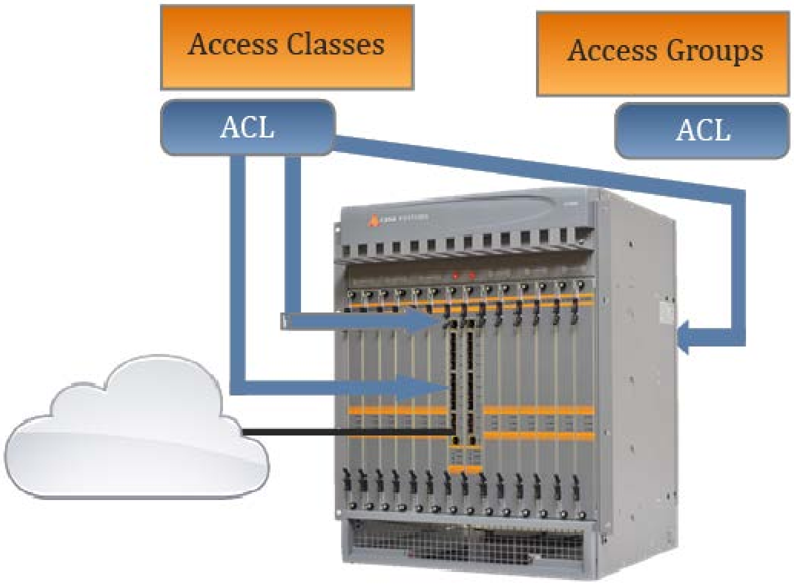
Click here for a video use case on this topic.

The use case contains the commands below:

```
CASA#show ip
access-list         Access List Configuration
bgp                 BGP information
bundle              docsis ip bundle info
community-list      List community-list
domain-name         default domain name configuration
extcommunity-list   List extcommunity-list
interface           ip interface
isis                IS-IS information
mroute              ip multicast routing table
multicast           ip multicast
ospf                ospf
pim                 pim
prefix-list         List IP prefix lists
rip                 rip
route               ipv4 route
vrf                 vrf

CASA#show ipv6
bgp                  BGP information
interface            ipv6 interface status and configuration
isis                 IS-IS information
link-local-address   link local address
multicast            ipv6 multicast
neighbor             IPv6 neighbor
ospf                 Open Shortest Path First (OSPF) for IPv6
prefix-list          List IP prefix lists
rip                  Show RIPng routes
route                ipv6 route
```

3.12.2. Verifying Access Control Configurations Overview

Diagram: Access Controls



Access controls manage IP access to the system via certain interfaces, access groups, and access classes, incoming and outgoing. The access controls deny or permit the flow of data traffic to or from user-defined IP addresses and upper layer protocols specified in the IP protocol (TCP, UDP) field, such as tcp, udp, tftp, telnet, etc. To implement IP access control, you need to create an Access Control List (ACL) and apply the ACL to specified system interfaces, access groups, or access classes.

An ACL is an ordered sequence of rules that control the flow of data packets through the system. These rules may be used to permit or deny the flow of data traffic. ACLs help in restricting the use of the system as desired based on the data traffic.

3.12.2.1. Video Presentation on Access Controls

Click here for a video presentation on this topic.

Access Classes

The access-class command sets CPU-level access conditions for an ip access-list. An access class applies to line access, such as Telnet and SSH, as differentiated from an ip access-group that is set on each separate interface. Incoming access classes control the line traffic arriving at the CMTS. Outgoing access classes control the line traffic originating from and leaving the CMTS. You can also base an outgoing access class on a service policy.

With release 7.2, the CMTS now supports access control for specific access-class services. Use the <service-name> access-group <ACL-name> command, and specify either ntp, snmp, telnet, telnets, ssh, ipdr, ftp sntp, rtsp, or http for your <service-name> value.

Access Groups

The ip access-group command configures an access group that applies a specific ip access-list to a CMTS interface. An interface can have only one access group applied, although the same access group can be used for more than one interface. If an ACL is applied to an IP-bundle, the ACL also applies to all IP-bundle subinterfaces (unless the subinterfaces are overridden by another ACL). You can apply an access group to each of the following interfaces:

- eth0
- gige
- ip-bundle
- loopback
- trunk
- vlan

Access Lists

The ip access-list command configures an access list. An access list, or Access Control List (ACL), is an ordered sequence of rules that control the flow of data packets through the system. These rules may be used to permit or deny the flow of data traffic. Access lists help in restricting the use of the system as desired based on the data traffic. An access list needs to be applied to specified system interfaces or access classes. A maximum of 32 access lists are allowed, with up to 256 rules per ACL.

Access List Management

Release 7.2 included several enhancements to help you manage your ACLs.

- The **show ip access-list route status** command has been implemented in the CLI to the display the number of times an ACL rule has been matched. The number of rule matches is displayed in parentheses.

- The **show this** command now operates within the **ip access-list** configuration context.

Management of access control lists (ACLs) has been revised for improved optimization when ACLs are shared across IP bundle and sub-bundle interfaces. The following CLI commands have been removed with this enhancement:

- show interface ip-bundle <num=1:16> acl-count [details]
- show interface ip-bundle <sub_interface> acl-count [details]

Use the **show ip access-list <ACL name> details** command to display the ACL counters.

3.12.2.2. Video Use Case on Verifying Access Control Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show ip access-list
ip access-list ACL1
ip access-list test

CASA#show ip access-list ACL1
10 permit telnet 192.168.2.238 255.255.255.255 any
20 deny telnet any any
30 deny icmp 192.168.2.19 255.255.255.255 any

CASA#show run | inc access-class
access-class out COPS_DSCP_ACL
access-class service-policy out COPS_DSCP_REWRITE

CASA#show interface access-class in acl-count
packet hit count by access-class in:
total count: 0

CASA#show interface access-class out service-policy-count details
10 permit udp 192.0.0.0 255.0.0.0 any 2126 any (0 matches)
20 permit tcp 192.0.0.0 255.0.0.0 any 2126 any (0 matches)
30 permit udp 15.0.0.0 255.0.0.0 any any 2126 (0 matches)
40 permit tcp 15.0.0.0 255.0.0.0 any 2126 any (0 matches)
50 permit udp 15.0.0.0 255.0.0.0 any 2126 any (0 matches)
60 permit udp 15.0.0.0 255.0.0.0 any any any (0 matches)
```

```
CASA#show interface gige 6/0
mac address 00:17:10:02:cb:c2
no ip igmp
no ipv6 mld
no auto negotiate
no shutdown
ip access-group ACL1 out
```

3.12.2.3. Prefix Lists

The ip prefix-list command configures a prefix list. IP prefix lists work like access control lists (ACLs) for route advertisements (prefixes) in that one or more ordered entries are processed sequentially. While extended (and to a limited extent, standard) ACLs can be employed to match network prefix announcements, prefix lists are generally more graceful. As with ACLs, evaluating a prefix against a prefix list ends as soon as a match occurs. There can be up to 200 entries in a prefix list.

The Casa CMTS uses IP prefix lists with the Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Router Information Protocol (RIP) routing protocols, and with route-maps.

IPv6 Prefix Lists

The ipv6 prefix-list command is the IPv6 version of the ip prefix-list command. There can be up to 200 entries in a prefix list.

3.12.2.4. Video Use Case on Verifying IP Prefix-list Configurations

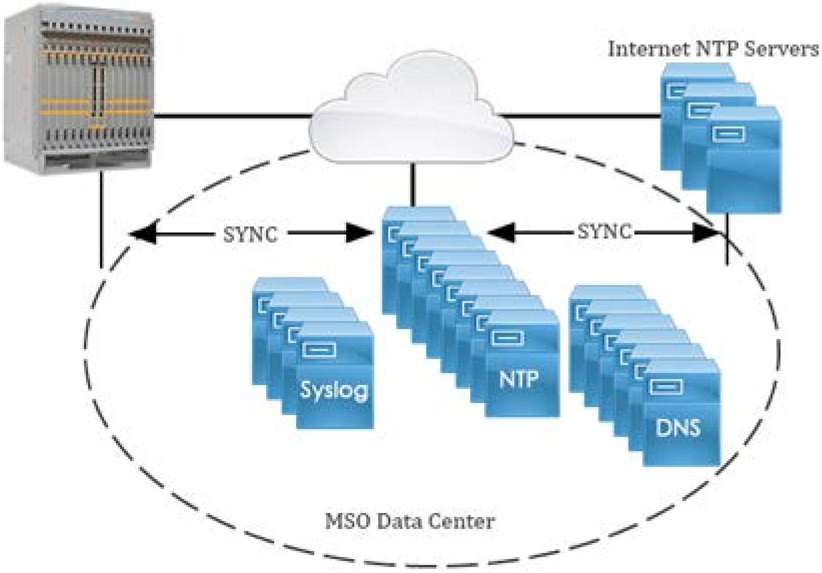
Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show ip prefix-list
ip prefix-list PRE1: 2 entries
seq 5 permit any
seq 30 deny 205.1.1.5/32
ip prefix-list PRE2: 1 entries
seq 10 deny 192.168.8.8/24 le 32

CASA#show ip prefix-list summary
ip prefix-list PRE1:
count: 2, range entries: 0, sequences: 5 - 30
```

```
ip prefix-list PRE2:
count: 1, range entries: 0, sequences: 10 - 10

CASA#show ip prefix-list detail
ip prefix-list PRE1:
count: 2, range entries: 0, sequences: 5 - 30
seq 5 permit any
seq 30 deny 205.1.1.5/32
ip prefix-list PRE2:
count: 1, range entries: 0, sequences: 10 - 10
seq 10 deny 192.168.8.8/24 le 32

CASA#show ip access-list route status
ip access-list c1
10 permit all 13.237.1.0 255.255.255.0 any any any
(4 matches)
```

3.13. Verifying OSSI



3.13.1. Syslog

The logging command in the Casa enable mode sets the type of logging, such as alerts, critical, errors, and warnings, for the current session. The logging command in the Casa configuration mode sets the logging levels for various logging types. You can direct messages to a specified target destination, which can be a remote SYSLOG host, the system console display, volatile or non-volatile memory, or a loopback interface. For each logging target, you need to specify the type of message based on a severity level. The system log file capacity is 1 MB. Use the show log command to show the current SYSLOG messages.

3.13.1.1. Video Presentation on SYSLOG Implementations

Click here for a video presentation on this topic.

3.13.2. Verifying DNS

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. DNS is an essential component of the functionality of the Internet.

In most cases, because the GigE CMTS interfaces are in the private network, the source interface for DNS responses over the public network will be a previously configured loopback interface.

3.13.2.1. Video Flow Chart on Troubleshooting DNS

Click here for a video troubleshooting flow chart on this topic.

3.13.3. Verifying NTP

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. The Time protocol is a network protocol defined in the earlier RFC 868.

The output of the “show ntp status” command includes symbols before each peer address. The symbols have the following meanings:

* Selected for synchronization
# Selected for synchronization, but distance exceeds maximum
+ Included in the final selection set
x Designated falsticker by the intersection algorithm
- Discarded by the clustering algorithm
<space> Discarded due to a high stratum (“st” at e.g. 16) or failed sanity check

A positive offset means that the system clock is behind the reference time, and should be less than 150 milliseconds. Jitter is measured in microseconds and should not be more than a few milliseconds.

3.13.3.1. Video Use Case on Verifying DNS, NTP, and SYSLOG Configurations

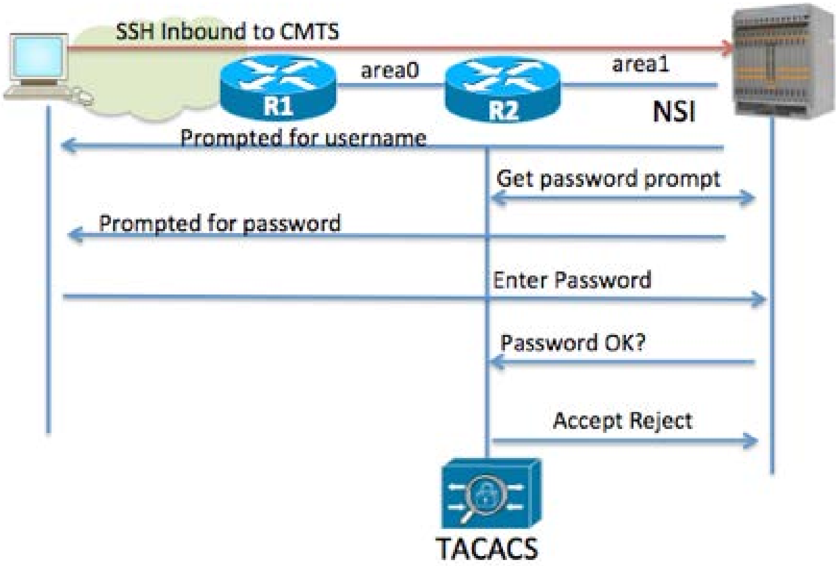
Click here for a video use case on this topic.

The use case contains the commands below.

```
show run | inc nameserver

CASA#show run | inc nameserver
nameserver source-interface loopback 1
nameserver 192.168.1.1

show ntp status

CASA#show ntp status
remote refid st t when poll reach delay offset jitter
======================================================================
+10.3.92.32 208.75.89.4 3 u 42 64 37 0.253 0.741 0.103
+32.32.32.32 208.75.89.4 3 u 40 64 37 0.562 0.644 0.143
*16.62.101.1 192.15.90.1 3 u 42 64 37 0.332 0.812 0.089
-10.3.97.58 104.233.3.3 3 u 40 64 37 0.268 0.110 0.038

show ntp-server

CASA#show ntp-server
no ntp scheck

CASA#ntp sync 10.4.1.3
Stopping NTP server: ntpd.
29 Sep 19:33:24 ntpdate[8609]: step time server 10.4.1.3 offset 0.000636 sec

CASA#show run | in logging
!casa logging control configuration:
no logging system
```

```
logging source-interface loopback 0
logging host 10.4.1.3
<<Output Cut>>
```

3.14. Verifying TACACS+ and RADIUS Configuration



Authentication, Authorization, and Accounting (AAA) encompasses two protocols used in the Casa CMTS:

- Remote Authentication Dial In User Service (RADIUS)
- Terminal Access Controller Access Control System Plus (TACACS+)

RADIUS provides centralized AAA management for users that connect and use a network service. TACACS+ provides separate authentication, authorization and accounting services. TACACS+ uses the TCP protocol and encrypts the entire packet (except the header). RADIUS, TACACS, XTACACS, and TACACS+ are open, publicly documented protocols.

The CMTS supports five methods of authentication and authorization:

1. TACACS authentication and TACACS authorization
2. TACACS authentication and local authorization
3. RADIUS authentication and TACACS authorization
4. RADIUS authentication and local authorization
5. Local authentication and local authorization

RADIUS is set up for authentication only and cannot do authorization. TACACS can do authentication and authorization. Note that, for RADIUS authentication and TACACS+ authentication, the two databases must be in sync in terms of usernames and privileges.

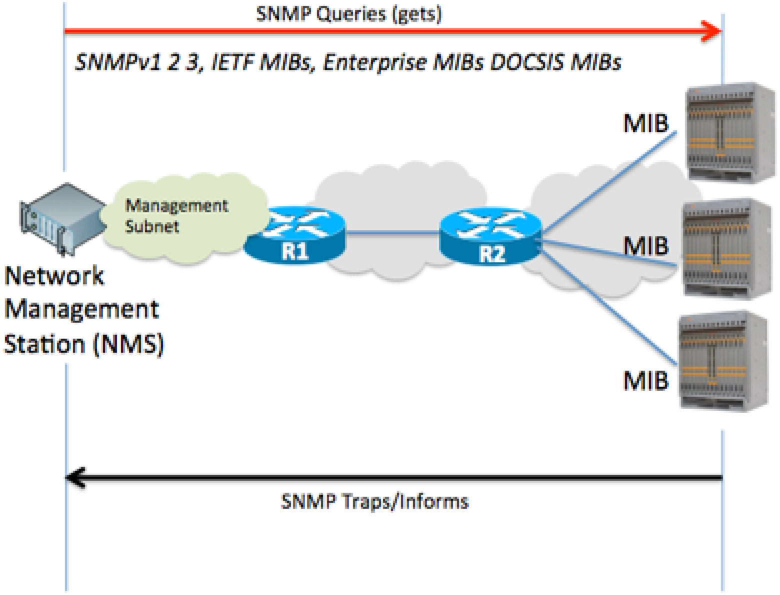
3.14.1. Video Use Case on Verifying TACACS/RADIUS Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show run | inc "aaa authorization"
aaa authorization command 0 default if-authenticated
aaa authorization command 15 default if-authenticated
CASA#

CASA#show run | inc tacacs
tacacs-server host 10.4.1.4
tacacs-server key
$9$5d8378a342100b8d$de497aef17461a775c2b70c2ec2a702409fa17a240
34092fff7d1eb63e3b05cf 7
aaa authentication login default group tacacsplus
aaa authentication enable default group tacacsplus enable
aaa authentication login tacacsplus-local
aaa accounting default group tacacsplus
aaa tacacs-source loopback 0
CASA#

CASA#show running-config | inc radius|aaa
radius-server host 10.4.1.4
radius-server key $9$9d7d2f7c29befcbb$715e0756cd6c72b8e67bdd160c01215b 7
aaa authentication login default group radius
aaa authentication login radius-local
aaa accounting
aaa accounting commands 1 default start-stop
aaa accounting commands 15 default start-stop
aaa accounting exec default start-stop group radius

CASA#show aaa
------------------------------AAA Configurations----------------------
TACACS Server IP Address : 192.168.3.63 (KEY: $xxxxxx) Status: Up
TACACS timeout : 3
TACACS Server Encryption Key : $xxxxxx
TACACS Password-aging : NOT ENABLED
<<output cut>>
```

3.15. Verifying SNMP Configuration


SNMP Queries (gets)
SNMPv1 2 3, IETF MIBs, Enterprise MIBs DOCSIS MIBs
MIB
Management Subnet
R1
R2
MIB
Network Management Station (NMS)
MIB
SNMP Traps/Informs

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more. SNMP is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMP is comprised of an *agent* and a *manager*, where the agent functions as a server for the manager client, also known as a client-server model.

Once SNMP is configured at the CMTS using the command line interface, the CMTS becomes the SNMP agent. Similarly, the remote workstation or PC running the SMNP management software assumes the role of SNMP manager. Communication between the CMTS SNMP agent and the SNMP management software takes place over a Telnet or SSH connection that is initiated by the management software.

3.15.1. Video Use Case on Verifying SNMP Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show snmp brief
snmp engineid 8000517a0300171008ad8000
snmp notify InformV2cSNMPv2cNotifyTagList InformV2cSNMPv2cNotifyTagList
inform non-volatile active
snmp notify InformV3SNMPv3NotifyTagList InformV3SNMPv3NotifyTagList inform
non-volatile active
snmp notify TrapV1SNMPv1TrapsTagList TrapV1SNMPv1TrapsTagList trap non-
volatile active
<<Output Cut>>


CASA#snmp default
This will remove any SNMP configuration and will set public/private
communities, are you sure you want to continue? (YES/NO):

CASA#show snmp access-list user-name burns
10 permit snmp 192.168.8.0 255.255.255.0 any (0 matches)
20 permit snmp 10.10.10.0 255.255.255.0 any (0 matches)
30 permit snmp 172.30.58.78 255.255.255.255 any (26 matches)

CASA#show snmp statistics
SNMP agent statistics
snmpInPkts: 206798
snmpOutPkts: 206896
snmpInBadVersions: 0
snmpInBadCommunityNames: 5
snmpInBadCommunityUses: 95
<<Output Cut>>

CASA(config)#show snmp
    SNMP packet size
snmp packet size :        4096

    SNMP community information
Community name:          casaadmin
Community Index:         casaadmin
Community SecurityName:  rwtesting
<<Output Cut>>

CASA#diag
Password:
CCAP1(diag)# snmp shutdown
CCAP1(diag)# snmp start
```

3.16. Verifying IPDR Configuration

In the Internet Protocol Detail Record (IPDR) architecture, the CMTS functions as the IPDR Recorder. It exports IPDR records to the IPDR Collector over TCP port 4737. In a large network, with hundreds of thousands of devices including Customer Premise Equipment, the IPDR collector will end up processing a very high volume of IPDR records.The CMTS can report to one or two IPDR collectors.

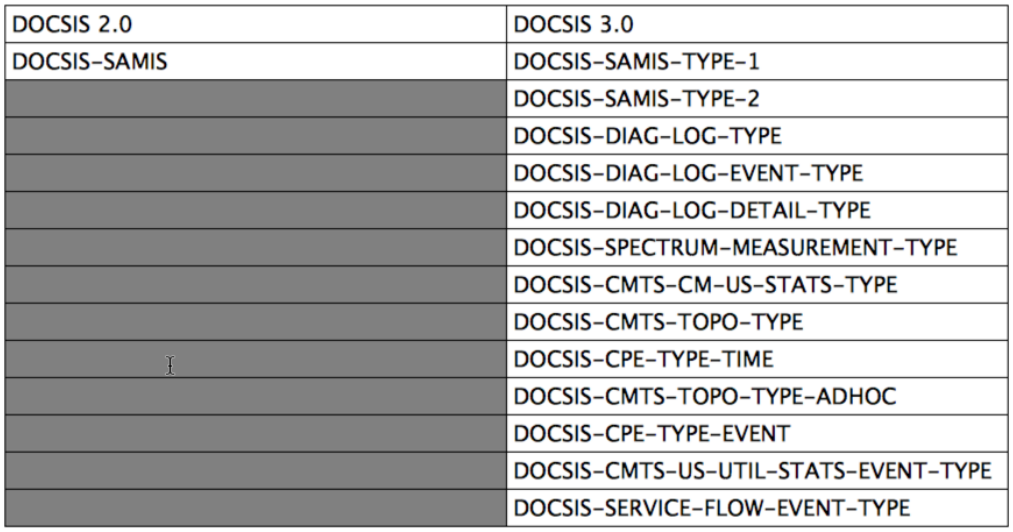
DOCSIS 2.0 defines the Subscriber Account Management Interface Specification (SAMIS) schema for collecting subscriber usage data via IPDR. DOCSIS 3.0 breaks the SAMIS schema into SAMIS Type 1 and SAMIS Type 2, and defines 11 additional schema for collecting network and RF/HFC instrumentation data.

The Casa CMTS supports the entire DOCSIS 2.0 and 3.0 IPDR schemas.

3.16.1. Video Presentation on IPDR Implementations

Click here for a video presentation on this topic.

Casa IPDR Schema Support



DOCSIS 2.0	DOCSIS 3.0
DOCSIS-SAMIS	DOCSIS-SAMIS-TYPE-1
	DOCSIS-SAMIS-TYPE-2
	DOCSIS-DIAG-LOG-TYPE
	DOCSIS-DIAG-LOG-EVENT-TYPE
	DOCSIS-DIAG-LOG-DETAIL-TYPE
	DOCSIS-SPECTRUM-MEASUREMENT-TYPE
	DOCSIS-CMTS-CM-US-STATS-TYPE
	DOCSIS-CMTS-TOPO-TYPE
	DOCSIS-CPE-TYPE-TIME
	DOCSIS-CMTS-TOPO-TYPE-ADHOC
	DOCSIS-CPE-TYPE-EVENT
	DOCSIS-CMTS-US-UTIL-STATS-EVENT-TYPE
	DOCSIS-SERVICE-FLOW-EVENT-TYPE

3.16.2. Video Use Case on Verifying IPDR Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show ipdr connection
DISPLAYING CONNECTION INFORMATION OF THE IPDR COLLECTORS
Connection 0
connection index: 0
collector ip address: 192.168.16.171

CASA#show ipdr diaglog
DISPLAYING IPDR DIAGLOG TRIGGERS INFORMATION
Include Triggers : C0
Aging Triggers : 00
Registration Detail : 0000

CASA#show ipdr session all
Session: 1
Session Name : DOCSIS-SAMIS-TYPE-1
Schema Name : DOCSIS-SAMIS-TYPE-1_3.5.1-A.1.xsd
Schema version : 3.5.1-A.1
Collection Interval: 900 (seconds)
<<output cut>>
Session: 27
Session Name : DOCSIS-US-OFDMA-PROFILE-STATS-TYPE
Schema Name :
DOCSIS-US-OFDMA-PROFILE-STATS-TYPE_3.5.1-B.1.xsd
Schema version : 3.5.1-B.1
Collection Interval: 900 (seconds)
<<output cut>>

CASA#show ipdr session id-map
nameserver source-interface loopback 0
ip domain-name sdclasslab.local
nameserver 10.4.1.3

CASA#show ipdr template samis-1
Template: DOCSIS-SAMIS-TYPE-1_3.5.1-A.1.xsd
FIELD-NAME FIELD-ID TYPE ENABLE NEGOTIATED NEG-VALUE
---------- -------- ---- ------ ---------- ---------
CmtsHostName 1 String Yes No N/A
CmtsSysUpTime 2 UInteger Yes No N/A
<<output cut>>
```

3.17. Verifying NetFlow Configuration

NetFlow provides the ability to collect IP network traffic as it enters or exits an interface. By analyzing the data provided by NetFlow, a network administrator can determine such things as the source and destination of traffic, class of service, and the causes of congestion. A network flow is a unidirectional stream of packets identified as the combination of factors. Any one of the following factors being different defines the flow as unique:

- Source IP address
- Destination IP address
- IP protocol
- Source port number
- Destination port number
- Type of service (ToS)

- Ingress interface (SNMP IfIndex).

The Casa NetFlow implementation is based on NetFlow version 9, described in RFCs 7011 and 7012. Version 9 is template-based and complies with IPv6 as well as IPv4 addressing. NetFlow information collection is turned on and off on individual IP bundle interfaces only. One sampler MAP and one exporter map are supported per CMTS, with one data template each for IPv4 and IPv6. Each line card is both an observation domain and an export device. Only UDP transport is supported.

NetFlow depends on a sampling rate. The Casa minimum sampling rate is defined as one packet out of one thousand packets.

3.17.1. Video Use Case on Verifying NetFlow Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
show flow exporter-map [<name>]

CASA#show flow exporter-map
flow exporter-map EXMAP1
options interface-table timeout 300
options sampler-table timeout 300
template data timeout 300
template options timeout 300
transport udp dst-port 2025
transport udp src-port 1025
destination 192.168.8.8
source loopback 0
index id 0
…
show flow exporter stat
UPS 9/ 9: nobuf 0
UPS 12/12: nobuf 0
QAM 1/ 5: nobuf 0
QAM 5/ 5: nobuf 0
QAM 10/10: nobuf 0
TTL 0/ 0: nobuf 0

show flow monitor-map [<name>]

CASA#show flow exporter-map
flow monitor-map MONMAP1
record ipv4
```

```
exporter EXNAME1
cache timeout update 300

show flow sampler-map [<name>]

CASA#show flow sampler-map
flow sampler-map SAMP1
random 1-out-of 1024
```

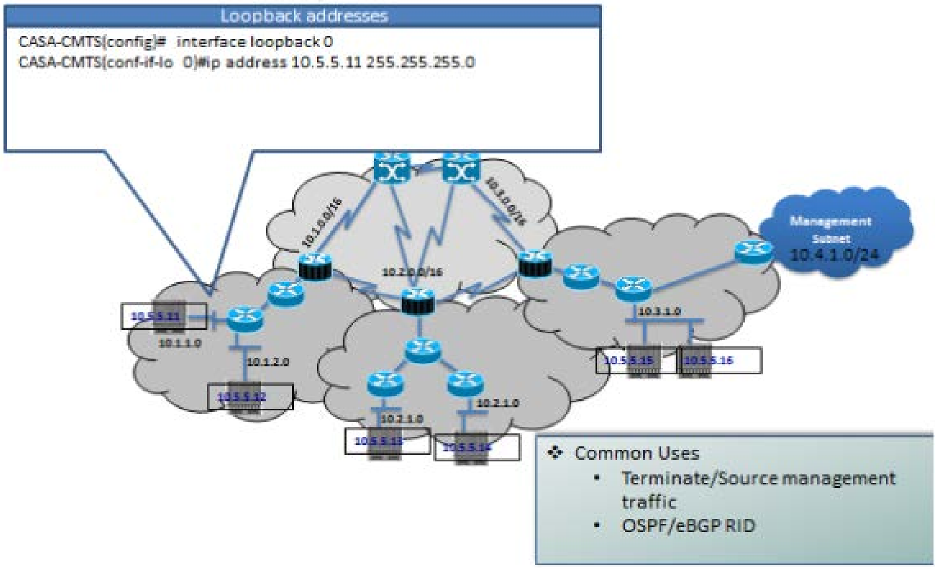
3.18. Verifying Routing Configurations

3.18.1. Overview

The Casa CMTS operates in your network as a fully functional Layer 3 router, supporting static routing, RIP, OSPFv2 and v3, ISIS,iBGP and BGP, policy-based routing, and Virtual Routing and Forwarding. This module covers the operation and configuration of each of these functions.

3.18.2. Loopback Interfaces

Diagram: Loopback Addressing



Loopback addresses

```
CASA-CMTS(config)#  interface loopback 0
CASA-CMTS(conf-if-lo  0)#ip address 10.5.5.11 255.255.255.0
```

❖ Common Uses
- Terminate/Source management traffic
- OSPF/eBGP RID

A loopback interface is a virtualized interface not tied to any physical interface. Just like a physical interface it can be assigned a v4 or v6 IP address.

It is common practice to use loopback addresses for terminating management connections, for example SSH, or SNMP. It is also common to identify the loopback as the source address for management traffic leaving the CMTS. Because the loopback address is a virtualized address, these services remain up and operational as long as at least one physical interface is up and active.

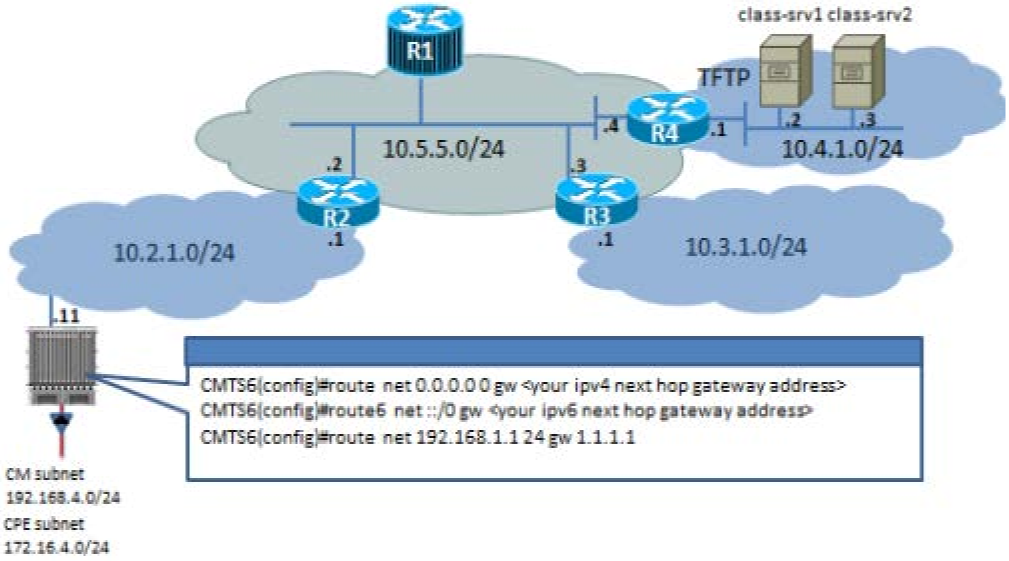
Additionally, the use of the loopback in this manner allows identification, segmentation, and control of management traffic. This facilitates internal documentation, and other system administration purposes.

As of Release 7.2, the Casa CMTS will support up to 64 loopback interfaces, with a loopback port ID range of 0-255.

3.18.3. Verifying Static/Default Routing Configurations

Overview

Diagram: Default Route



```
CMTS6(config)#route  net 0.0.0.0 0 gw <your ipv4 next hop gateway address>
CMTS6(config)#route6  net ::/0 gw <your ipv6 next hop gateway address>
CMTS6(config)#route  net 192.168.1.1 24 gw 1.1.1.1
```

Static routing algorithms are basically route table mappings created manually by a network administrator. These mappings do not change unless the network administrator alters them.

Static routes are simple to design and work well in environments where network traffic is relatively predictable and where network design is relatively simple.

There are basically two types of static routes:

- Default routes
- Static routes

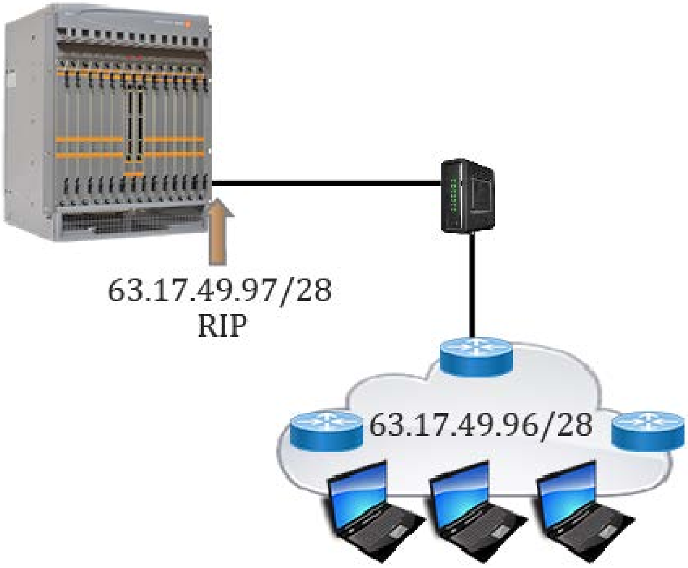
These configurations are similar, however static routes point to a specific subnet while default routes are a “route of last resort.” That is to say that the route will be used if there is no match in the routing table for the destination network.

3.18.3.1. Video Presentation on Loopback Interfaces and Static Routing

Click here for a video presentation on this topic.

3.18.4. Verifying RIP Configurations

Diagram: RIP Network



The Routing Information Protocol (RIP) is an internal gateway protocol (IGP) based on the Bellman-Ford (or distance vector) algorithm. RIP uses UDP to exchange routing information. Casa RIP supports RIPv1, RIPv2, and RIPng, along with plain text and MD5 authentication and route summarization. RIP version 1 (RIPv1) broadcasts routing updates over the broadcast IP address 255.255.255.255, while RIP version 2 (RIPv2) broadcasts routing updates over the multicast address 224.0.0.9. RIPv1 is based on RFC 1058 and RIPv2 is based on RFC 2453. MD5 authentication is based on RFC 2082.

RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance, which renders the route unreachable. Among the stability features of RIP is that it implements the split horizon, route poisoning and holddown mechanisms to prevent incorrect routing information from being propagated.

RIP Next Generation (RIPng) functions the same and offers the same benefits for IPv6 as RIP in IPv4. RIPng includes support for IPv6 addresses and prefixes, and the use of the all-RIP-routers multicast group address FF02::9 as the destination address for RIP update messages. RIPng is based on RFC 2080.

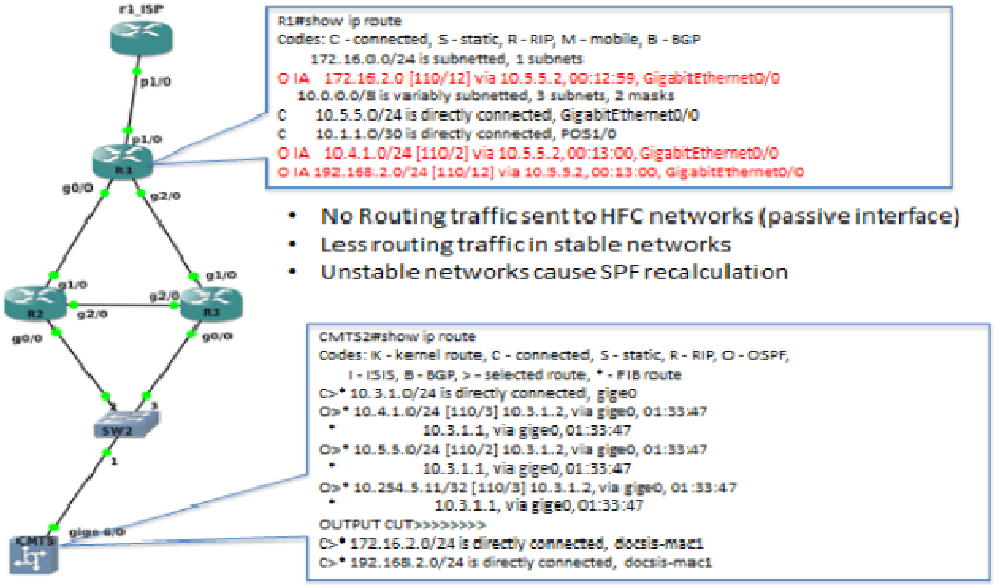
The most common use for RIP is to provide routing support to small business customers. The MSO assigns a subnet of publicly valid IP addresses to the customer, and configures the IP Bundle interface on the CMTS to be the gateway for the customer’s devices.

The MSO also configures the IP Bundle interface to run RIP, and configures its Interior Gateway Protocol to redistribute the RIP route.

3.18.5. Verifying OSPF Configurations

Overview

Diagram: OSPF Network



```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M – mobile, B - BGP
     172.16.0.0/24 is subnetted, 1 subnets
O IA   172.16.2.0 [110/12] via 10.5.5.2, 00:12:59, GigabitEthernet0/0
   10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C      10.5.5.0/24 is directly connected, GigabitEthernet0/0
C      10.1.1.0/30 is directly connected, POS1/0
O IA   10.4.1.0/24 [110/2] via 10.5.5.2, 00:13:00, GigabitEthernet0/0
O IA 192.168.2.0/24 [110/12] via 10.5.5.2, 00:13:00, GigabitEthernet0/0
```

- No Routing traffic sent to HFC networks (passive interface)
- Less routing traffic in stable networks
- Unstable networks cause SPF recalculation

```
CMTS2#show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
     I - ISIS, B - BGP, > - selected route, * - FIB route
C>* 10.3.1.0/24 is directly connected, gige0
O>* 10.4.1.0/24 [110/3] 10.3.1.2, via gige0, 01:33:47
 *                 10.3.1.1, via gige0, 01:33:47
O>* 10.5.5.0/24 [110/2] 10.3.1.2, via gige0, 01:33:47
 *                 10.3.1.1, via gige0, 01:33:47
O>* 10.254.5.11/32 [110/3] 10.3.1.2, via gige0, 01 :33:47
 *                  10.3.1.1, via gige0, 01:33:47
OUTPUT CUT>>>>>>>>
C>* 172.16.2.0/24 is directly connected, docsis-mac1
C>* 192.168.2.0/24 is directly connected,  docsis-mac1
```

The Open Shortest Path First (OSPF) routing protocol, defined by RFC 2328, OSPF Version 2 and RFC 5340, OSPF for IPv6, is a link-state routing protocol used for interior routing. Like the Border Gateway Protocol (BGP), OSPF uses an autonomous system (AS) as the routing domain, but, unlike BGP, it remains within a single AS. It is probably the most widely used interior gateway protocol (IGP). OSPF was designed to support variable-length subnet masking (VLSM) and classless inter-domain routing (CIDR) in defining participating networks. OSPF detects and converges on a loop-free routing topology using the Dijkstra algorithm. OSPF uses link cost factors (external metrics) associated with each routing interface. The cost factors can be the round-trip time distance of a router, network throughput of a link, or link availability and reliability, expressed as simple unitless numbers.

3.18.5.1. Video Presentation on OSPF

Click here for a video presentation on this topic.

The OSPF AS is subdivided into areas identified by 32-bit numbers that commonly correspond to the area’s main router IP address. Area 0.0.0.0 normally represents the backbone region of the OSPF network. A border router between areas is called an area border router (ABR) that maintains separate link state databases for each area it serves and maintains summarized routes for all areas in the network. An interface is generally configured in a single OSPF area. An OSPF instance is identified by an integer process identifier (process ID) that is often the same as the defined area number.

OSPF uses multicast addressing for route flooding on a broadcast domain, and provides neighbor discovery based on detected adjacencies, for which OSPF maintains an adjacency database. Routers on the network select a designated router (DR) and a backup designated router (BDR) to act as hubs to reduce traffic.

3.18.5.2. Video Use Cases on Verifying OSPFv2 and v3 Configurations

Click here for a video use case on this topic.

The use cases on Verifying OSPFv2 Configurations contains the commands below.

```
CASA#show run | begin “router ospf”
router ospf 105
router-id 105.105.105.1
redistribute connected
-output cut-

CASA#show ip ospf
Routing Process "ospf 105" with ID 105.105.105.1
Process uptime is 32 minutes
Process bound to VRF default
Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
-output cut-

CASA#show ip ospf interface
gige6/0 is up, line protocol is up
Internet Address 172.16.200.200/24, Area 0.0.0.0, MTU 1500
Process ID 1, Router ID 11.1.1.200, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DROther, Priority 1
Designated Router (ID) 11.1.1.204, Interface Address 172.16.200.204
-output cut-

CASA#show ip route ospf
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - ISIS L1 - LEVEL-1 L2 - LEVEL-2 IA - inter area, B - BGP, >
- selected route, * - FIB route.
O *> 3.3.3.3/32 [110/13] via 172.16.200.1, gige6/0, 00:02:38
O *> 7.7.7.7/32 [110/20] via 172.16.200.1, gige6/0, 1d19h58m
O *> 9.105.1.0/24 [110/20] via 172.16.200.1, gige6/0, 1d19h58m
-output cut-

CASA#show ip ospf database

            OSPF Router with ID (10.254.1.1) (Process ID 1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.254.1.1      10.254.1.1       292 0x800000e1 0xec7a 5
10.254.2.1      10.254.2.1       306 0x800000e1 0xe1fb 4
10.254.5.1      10.254.5.1       290 0x800000e1 0x8d9d 5
-output cut-
```

```
CASA#show ip ospf neighbor
OSPF process 1:
Neighbor ID Pri State Dead Time Address Interface
11.1.1.12 1 Full/DR 38.615s 172.16.200.1 gige6/0
11.1.1.202 1 Full/DROther 31.254s 172.16.200.202 gige6/0
11.1.1.204 1 Full/DROther 31.757s 172.16.200.204 gige60
-output cut-

CASA#show ip ospf traffic
OSPF Routing Process ID 1
Interface statistics
Interface gige6/0:172.16.200.200 (line protocol is UP)
OSPF packets received/sent
Invalid Hellos DB-des LS-req LS-upd LS-ack Total
Rx: 5 540 14 0 329 8 891
Tx: N/A 134 16 6 86 261 503
-output cut-

CASA#show ip ospf border-routers
OSPF process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 10.254.5.14 [11] via 10.3.11.5, vlan100, ABR, Area 0.0.0.0
i 10.254.5.12 [10] via 10.3.11.5, vlan100, ASBR, Area 0.0.0.0
```

The use case on Verifying OSPFv6 Configurations contains the commands below.

```
CASA#show run | beg "router ospf"
ipv6 router ospf 1 area 0.0.0.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 are2@casa
ip ospf network point-to-point
enable-ldp ipv4
no shutdown

CASA#show ipv6 ospf
Routing Process "OSPFv3 (1)" with ID 10.10.10.10
Process uptime is 4 days 15 hours 8 minutes
SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0 secs
Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
Number of incomming current DD exchange neighbors 0/5
-output cut-

CASA#show ipv6 ospf interface
vlan100 is up, line protocol is up
  Interface ID 252
  IPv6 Prefixes
    fe80::217:10ff:fe08:ad80/64 (Link-Local Address)
    fd25:5899:2cba:b390::2/64
  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 0
-output cut-

CASA#show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                  Metric
     Next-hop
O  fd0a:e4fb:a312:bb1b::/64                        11
     via fe80::21a:e2ff:fe19:5360, vlan100, Area 0.0.0.0
-output cut-
```

```
CASA#show ipv6 route ospf
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS L1 - LEVEL-1  L2 - LEVEL-2  IA - inter area, B - BGP, > -
select
ed route, * - FIB route.

O   *> fd0a:e4fb:a312:bb1b::/64 [110/11] via fe80::21a:e2ff:fe19:5360,
vlan100, 4d15h24m

-output cut-

CASA#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.10) (Process 1)

                Link-LSA (Interface vlan100)

Link State ID   ADV Router      Age  Seq#       CkSum  Prefix
0.0.0.8         2.2.2.2         1966 0x800000c9 0x2e37      1
0.0.0.252       10.10.10.10      570 0x800000df 0x6561      1
-output cut-

CASA#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State     Dead Time   Interface  Instance ID
2.2.2.2           1   Full/ -   00:00:32    vlan100    0


CASA#show ipv6 ospf neighbor detail
 Neighbor 2.2.2.2, interface address fe80::21a:e2ff:fe19:5360
    In the area 0.0.0.0 via interface vlan100
    Neighbor priority is 1, State is Full, 5 state changes
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x000013 (-|R|-|-|E|V6|-)
    Dead timer due in 00:00:32
    Neighbor is up for 112:20:3
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0

CASA#show ipv6 ospf topology

OSPFv3 Process (1)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop Interface
1.1.1.1                11         2.2.2.2  vlan100
2.2.2.2                10         2.2.2.2  vlan100
3.3.3.3                11         2.2.2.2  vlan100
4.4.4.4                11         2.2.2.2  vlan100
10.10.10.10        E   --
-output cut-
```

An OSPF network will only converge if your OSPF routers enter the appropriate neighbor states. If you are experiencing route unreachability, and suspect that a lack of OSPF convergence may be the cause, troubleshoot your OSPF neighbor states.

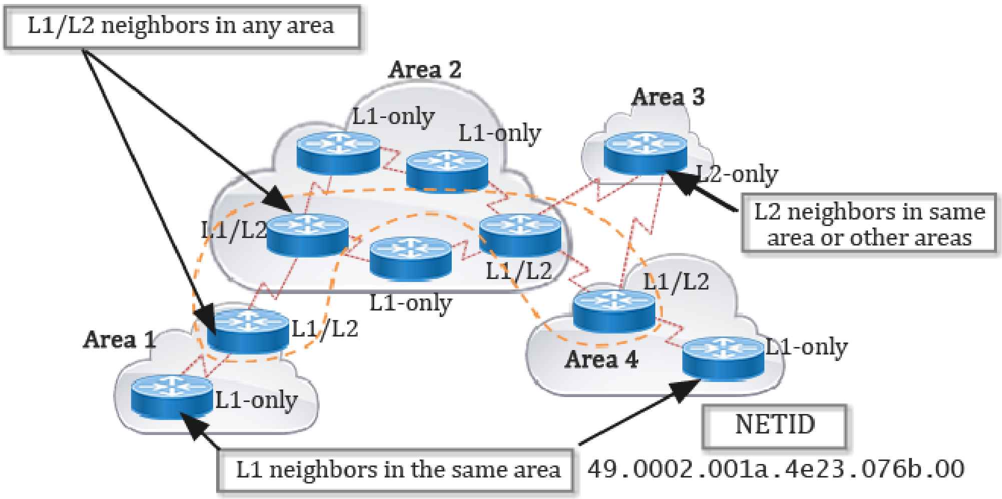
3.18.5.3. Video Flow Chart on Troubleshooting OSPF Neighbor States

Click here for a video troubleshooting flow chart on this topic.

3.18.6. Verifying IS-IS Configurations

3.18.6.1. Overview

Diagram: IS-IS Network



L1/L2 neighbors in any area
Area 2
L1-only
L1-only
Area 3
L2-only
L2 neighbors in same area or other areas
L1/L2
L1/L2
L1-only
L1/L2
Area 1
L1/L2
L1-only
Area 4
L1-only
NETID
L1 neighbors in the same area
49.0002.001a.4e23.076b.00

The Intermediate System to Intermediate System (IS-IS) routing protocol, defined by RFC 1142, OSI IS-IS Intra-domain Routing Protocol, in 1990 (reclassified to historic by RFC 7142) and updated by RFCs 1195, 1309, 5302, 5304, 5305, and others. IS-IS is an interior gateway, link-state routing protocol often described as the de facto standard for large service provider network backbones, developed around the same time as Open Shortest Path First (OSPF). Like OSPF, IS-IS uses the Dijkstra algorithm for determining the best path, supports VLSM, uses multicast to discover neighboring routers, and does summary routing. Unlike OSPF, IS-IS is network-type agnostic as far as IPv4 and IPv6. The lowest-cost (shortest) path metric to a subnet is used to forward traffic.

Like OSPF, IS-IS uses areas, but defines them differently. IS-IS routers are designated as Level 1 (intra-area), Level 2 (inter-area), or Level 1-2 (both). Level 2 routers can form relationships only with other Level 2 routers, while routing information is exchanged among all Level 1 routers. Level 1-2 routers exchange information with both levels and connect inter-area routers. IS-IS also does not require the backbone area 0 that OSPF requires.

3.18.6.2. Video Presentation on IS-IS

Click here for a video presentation on this topic.

Release 7.2 provided two enhancements to the CMTS IS-IS functionality. The **distance** parameter has been added to the **router isis** configuration to allow setting of the administrative distance metric of ISIS routing protocol. Lower values indicate preferred routes over other ISIS routers have higher distance settings. In addition, the **attached-bit receive ignore** command has been introduced in the **router-isis** configuration to configure the IS-IS router or IPv6 address-family to ignore the attached-bit in received Level 1 link-state packets (LSPs). The **attached-bit** can also be set using the **set-attached-bit {always | never}** command. The default setting (**no attached-bit receive ignore)** allows the router to install the default route when the attached-bit is set in the LSP receive. The command can also be set at the IPv6 address-family level.

3.18.6.3. Video Use Case on Verifying IS-IS Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show run | inc isis
  ip router isis ccap1
  ipv6 router isis ccap1
  isis network point-to-point
router isis ccap1

CASA#show run verbose | inc isis
  ip router isis ccap1
  ipv6 router isis ccap1
  isis network point-to-point
  isis hello padding
  isis priority 64
router isis ccap1

CASA#show ip route isis
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS L1 - LEVEL-1  L2 - LEVEL-2  IA - inter area, B - BGP, > -
selected route, * - FIB route.

I L2 *> 10.3.12.8/30 [115/20] via 10.3.11.5, vlan100, 01:17:32
I L2 *> 10.3.13.12/30 [115/20] via 10.3.11.5, vlan100, 01:17:32
-output cut-

CASA#show isis database
Area CASA:
IS-IS Level-1 Link State Database:
LSPID           LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
CASA.00-00      * 0x00000003   0x4C22        1111              0/0/0

IS-IS Level-2 Link State Database:
LSPID           LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
CASA.00-00      * 0x00000003   0xD003        1111              0/0/0
CCAP2.00-00       0x00000002   0xBF4C        475               0/0/0
R1.00-00          0x00000214   0x8E3B        968               0/0/0
R1.01-00          0x00000211   0x6711        561               0/0/0
R2.00-00          0x00000217   0x59D0        458               0/0/0
R3.00-00          0x00000214   0x9326        898               0/0/0
R4.00-00          0x00000214   0x4F17        673               0/0/0

CASA#show isis interface vlan 100
vlan100 is up, line protocol is up
  Routing Protocol: IS-IS (CASA)
    Network Type: Point-to-Point
    Circuit Type: level-1-2 , MTU: 1500
    Local circuit ID: 0x01
    Extended Local circuit ID: 0x00000001
 -output cut-

CASA#show isis neighbors
Area CASA:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R2             vlan100     001a.e219.5360  Up     29        L2   IS-IS

CASA#show isis neighbors detail
Area CASA:
System Id      Interface   SNPA            State  Holdtime  Type Protocol
R2             vlan100     001a.e219.5360  Up     22        L2   IS-IS
  Uptime: 00:20:49
  Area Address(es): 49.0001
  IP Address(es): 10.3.11.5
  IPv6 Address(es): fe80::21a:e2ff:fe19:5360
  Topology: IPv4
  Level-2 Protocols Supported: IPv4, IPv6
  Adjacency advertisement: Advertise

CASA#show isis topology
|                  Output  modifiers
<cr>
level-1            Paths to all level-1 routers in the area
level-2            Paths to all level-2 routers in the domain
CASA#show isis topology

Area CASA:
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop       Interface   SNPA
CASA                --

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop       Interface   SNPA
CASA                --
CCAP2                20         R2             vlan100     001a.e219.5360
R1                   20         R2             vlan100     001a.e219.5360
-output cut-
```

An IS-IS network will only converge if your IS-IS routers form the appropriate adjacencies. If you are experiencing network unreachability, and suspect that a lack of IS-IS convergence could be the cause, troubleshoot your IS-IS adjacencies.

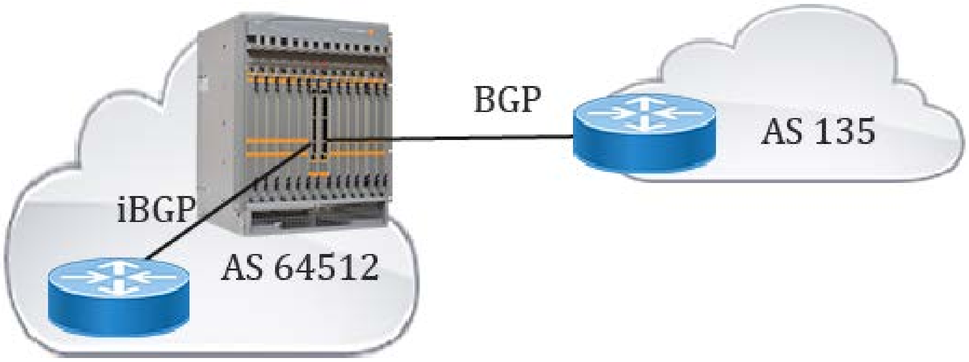
3.18.6.4. Video Flow Chart on Troubleshooting IS-IS Adjacencies

Click here for a video troubleshooting flow chart on this topic.

3.18.7. Verifying BGP and iBGP Configurations

Overview

Diagram: BGP Network



3.18.7.1. Video Presentation on BGP

Click here for a video presentation on this topic.

The Border Gateway Protocol (BGP), defined by RFC 4271, provides policy-based connectivity, routing, and route exchanges among internal and external BGP peers. Internal BGP peers share routes with each other under one administrative authority or domain called an autonomous system (AS), which is identified by a unique number at the CMTS. Autonomous systems share their routes with other autonomous systems called external BGP peers (or neighbors) using a border router, or edge router. This router advertises the routes from its own autonomous system to other BGP border routers in other autonomous systems. BGP protocol uses the AS number for detecting whether a BGP connection to a BGP peer is an internal or external connection. BGP connections at the CMTS are established with BGP peers over SMM GigE and XGigE network-side interfaces. The absolute minimum requirement for configuring a BGP route is setting up local network addresses and establishing neighbor relationships.

3.18.7.2. Video Use Case on Verifying BGP Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show run | begin “router bgp”
router bgp 64511
no synchronization
bgp router-id 105.105.105.1
neighbor 192.105.1.3 remote-as 100
neighbor 192.105.1.3 update-source loopback 0
-output cut-

CASA# show ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - ISIS L1 - LEVEL-1 L2 - LEVEL-2 IA - inter area, B - BGP, >
- selected route, * - FIB route.
B *> 105.0.0.0/24 [20/0] via 192.105.1.3, gige6/5, 22:41:23
B *> 105.0.1.0/24 [20/0] via 192.105.1.3, gige6/5, 22:41:23
-output cut-

CASA#show ip bgp
BGP table version is 2, local router ID is 105.105.105.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*> 11.105.0.0/16 0.0.0.0 0 100 32768 i
*> 105.0.0.0/24 192.105.1.3 0 0 100 25 i
-output cut-

show ip bgp {vpnv4 | vpnv6} ?
all
all <ip6_addr>
all neighbors [<addr>] [advertised-routes]
all summary
all tags
rd <id> [label | neighbors <ip6_addr>]
vrf <id> [<ip6_net> | label | summary]

CASA#show ip bgp vpnv4 all neighbors 192.168.8.8 advertised-routes
BGP table version is 1, local router ID is 175.12.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i
- internal, l - labeled S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 10:4
```

```
*>i10.175.59.0/24 175.12.1.1 0 100 32768 ?
-output cut-

CASA#show ip bgp summary
BGP router identifier 105.105.105.1, local AS number 1001
BGP table version is 1863
2 BGP AS-PATH entries
0 BGP community entries
4 Configured ebgp ECMP multipath: Currently set at 4
4 Configured ibgp ECMP multipath: Currently set at 4
Neighbor     V AS  MsgRcvd MsgSent TblVer InQ OutQ Up/Down  State/PfxRcd
192.85.2.10  4 100 0       0       0      0   0    Active
192.85.2.100 4 100 7497    8796    1863   0   0    2d14h26m 10
Total number of neighbors 2

CASA#show ip bgp neighbors
BGP neighbor is 192.105.1.3, remote AS 100, local AS 1001, external link
BGP version 4, remote router ID 192.105.1.3
BGP state = Established, up for 1d01h17m
Last read 00:00:03, hold time is 90, keepalive interval is 30 seconds
Neighbor capabilities:
     Route refresh: advertised
     4-Octet ASN Capability: advertised
     Address family IPv4 Unicast: advertised and received
```

A BGP network will only converge if your BGP routers correctly establish neighbors. If you are experiencing route unreachability, and suspect that a lack of BGP convergence may be the cause, troubleshoot your BGP neighbor establishment.

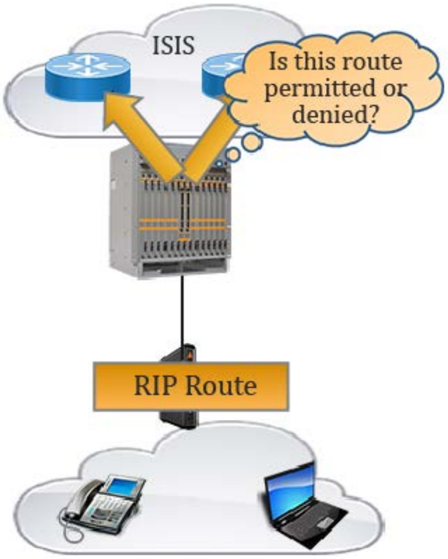
3.18.7.3. Video Flow Chart on Troubleshooting BGP Neighbor Establishment

Click here for a video troubleshooting flow chart on this topic.

3.18.8. Verifying Policy Based Routing Configurations

3.18.8.1. Overview

Diagram: Policy Based Routing



An MSO commonly needs to redistribute customer-facing routes, such as subnets set up to provide Residential or VoIP service, into its routing backbone. You can configure the CMTS to simply redistribute everything; however, MSOs typically want to control what subnets are advertised.

Route maps provide a mechanism for permitting or denying route announcements that are redistributed by dynamic routing protocols such as Border Gateway Protocol (BGP) and Open Shortest Path First protocol (OSPF). Route maps are similar in function to Access Controls (ACLs) when permitting or denying IP traffic. However, a route-map applies only to matched inbound IP routes; route information can then be modified before it is redistributed by the intended protocol.

You create named route maps using match and set criteria at the CMTS. The match command configures the criteria for selecting the routes to which a route map applies, while the set command modifies route information prior to redistribution. When an inbound route is received at a CMTS interface, the CMTS evaluates the route against configured route maps in numbered sequence for matching criteria, as follows:

- If matched, the route is then redistributed using the newly modified settings.
- If the route map does not contain at least one match command, then all routes match.
- If the route map is matched, but does not contain at least one set command instance, then the unmodified route is redistributed.

When configuring BGP or OSPF, specify a named route map with the redistribute command for the targeted routing protocol.

3.18.8.2. Video Presentation on Policy Based Routing

Click here for a video presentation on this topic.

Policy Based Routing uses IP Prefix Lists to identify the routes for redistribution. IP prefix lists work like access control lists (ACLs) for route advertisements (prefixes) in that one or more ordered entries are processed sequentially. While extended (and to a limited extent, standard) ACLs can be employed to match network prefix announcements, prefix lists are generally more graceful. As with ACLs, evaluating a prefix against a prefix list ends as soon as a match occurs. There can be up to 200 entries in a prefix list.

The Casa CMTS uses IP prefix lists with the Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Router Information Protocol (RIP) routing protocols.

3.18.8.3. Video Use Case on Verifying IP Prefix List and Policy Based Routing Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show ip prefix-list
ip prefix-list PRE1: 2 entries
  seq 5 permit any
  seq 30 deny 205.1.1.5/32
ip prefix-list PRE2: 1 entries
  seq 10 deny 192.168.8.8/24 le 32
```

```
CASA#show ip prefix-list detail
ip prefix-list redistribute_rip:
  count: 1, range entries: 0, sequences: 5 - 5
  seq 5 permit 172.16.11.1/24

CASA(config)# show ip prefix-list summary
ip prefix-list PRE1:
  count: 2, range entries: 0, sequences: 5 - 30
ip prefix-list PRE2:
  count: 1, range entries: 0, sequences: 10 - 10

CASA#show route-map
route-map connect_rip_to_ospf, permit, sequence 10
  Match clauses:
    ip address prefix-list: redistribute_rip
  Set clauses:

  Policy routing matches: IPv4 0 packets, 0 bytes  IPv6 0 packets, 0 bytes

CASA(config-router-ospf)#show this
router ospf 1
 redistribute connected route-map connect_rip_to_ospf
 passive-interface ip-bundle 1
 area 0 authentication message-digest
 network 10.3.11.4/30 area 0
 network 10.254.1.1/32 area 0
 network 172.16.1.0/24 area 0
 network 192.168.1.0/24 area 0

CASA#show ip ospf database

            OSPF Router with ID (10.254.1.1) (Process ID 1)

                Router Link States (Area 0.0.0.0)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.254.1.1      10.254.1.1       475 0x80000118 0x83aa 5
-output cut-

                AS External Link States
Link ID         ADV Router      Age  Seq#       CkSum  Route
Tag
172.16.11.0     10.254.1.1       505 0x80000116 0x20b5 E2 172.16.11.0/24  0

CASA#show ip ospf
 Routing Process "ospf 1" with ID 10.254.1.1
 Process uptime is 5 days 15 hours 38 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Graceful Restart
 This router is an ASBR (injecting external routing information)
-output cut-

Use the commands shown below to verify your RIP configurations.

CASA#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

   Network            Next Hop         Metric From            If
Time
Rc 172.16.11.0/24       0.0.0.0             1     self        ip-bundle1.2
```

```
CASA#show ip rip status
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 12 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
-output cut-
```

3.18.9. Verifying VRF Configurations

Overview

Virtual Routing and Forwarding (VRF) allows the Casa CMTS to participate as a provider edge (PE) or customer edge (CE) device in virtual private networks (VPNs) using protocols such as Border Gateway Protocol (BGP) and Multi-Protocol Label Switching (MPLS). IP routes can also include VRF instances in the instance of static routes.

3.18.9.1. Video Presentation on Virtual Routing and Forwarding

Click here for a video presentation on this topic.

VRF forwarding can be set for interfaces. VRF allows multiple independent instances of a routing table (up to 16) to exist on a single CMTS without the problem of overlapping IP addresses over a shared WAN backbone. Data is transmitted over the wide-area core backbone between VRF instances at each customer or provider edge location for forwarding to a destination.

A C100G with SMM 8x10G can support 128 virtual routing and forwarding (VRF) instances. A passive ARP (PARP) update has also been applied to ensure the additional VRFs are supported in policy-based routing (PBR) where a VRF next-hop instance is applied in a route-map.

A C10G with SMM 2x10G or SMM 8x1G, or a C40G, supports only 32 named VRFs.

3.18.9.2. Video Use Case on Verifying VRF Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
CASA#show ip vrf detail
VRF casalabs; default RD 1:1
  Interfaces:
    ip-bundle1.1

CASA#show ip vrf running-config
!
vrf definition casalabs
  rd 1:1
  address-family ipv4
    route-target import 1:1
    route-target export 1:1
  exit-address-family

Use the command, show ip multicast vrf [<id>] {adroute [<ip>] | traffic
[docsis | video] | tunnel
[<ip>]}, to view your various multicast VRF functions.

Use the commands shown below to view your VRF interfaces.

CASA#show ip vrf brief
Name                            Default RD    VRF ID  Interface
casalabs                        1:1           1       ip-bundle1.1

CASA#show ip vrf
Name                            Default RD    VRF ID  Interface
casalabs                        1:1           1       ip-bundle1.1

CASA#show ip vrf interface
Interface      Name             Default RD    VRF ID
ip-bundle1.1   casalabs         1:1           1

CASA#show ip route vrf casalabs
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       I - ISIS L1 - LEVEL-1  L2 - LEVEL-2  IA - inter area, B - BGP, > -
select
ed route, * - FIB route.

B    *> 10.3.1.0/24 [200/0] via 10.254.5.13 (recursive via 10.3.11.5),
06:42:12
B    *> 10.3.110.0/24 [200/11] via 10.254.5.13 (recursive via 10.3.11.5),
06:42:12
```

```
-output cut-

Use the command, show ip bgp vpnv4 rd <id> [label] to view your VPNv4 routes
in BGP based on the route distinguisher.

CASA#show ip bgp vpnv4 rd 1:1
   Network          Next Hop      Metric  LocPrf Weight Path
Route Distinguisher: 1:1 (Default for VRF casalabs)
*>i10.3.1.0/24      10.254.5.13   0        100      0   ?
*>i10.3.110.0/24    10.254.5.13   11       100      0   ?
*>i10.3.111.0/24    10.254.5.13   11       100      0   ?
-output cut-
```

3.18.10. Verifying Resource Reservation Protocol Configurations Overview

The Resource Reservation Protocol (RSVP), in the form of its extension, RSVP Traffic Engineering (RSVP-TE), supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so forth) of the packet streams they want to receive. Hosts and routers that support both RSVP and Multi-Protocol Label Switching (MPLS) can associate labels with RSVP flows.

RSVP runs on both IPv4 and IPv6 and is based on RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*, subsequently updated by other RFCs.

3.18.10.1. Video Use Case on Verifying RSVP Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
show rsvp [interface {gige | trunk | vlan | xgige} <if> | neighbor |
nexthop-cache | path | session [egress | ingress | transit] | statistics |
trunk <if>]

CASA# show rsvp
RSVP Version : 1
Process uptime : 15 hours 27 minutes
RSVP Refresh Reduction : Enabled
RSVP Message Acknowledgment : Disabled
Bundle Send : Disabled
```

```
NSM Connection : Up
RSVP Refresh Timer : 30
Keep Multiplier : 3
Acknowledgment Await Timeout : 10
Explicit-Null For Direct Conn : Disabled
Local Protection : Disabled
Hello Receipt : Disabled
Hello Interval : 2
Hello Timeout : 7
Loop detection : Enabled (all interface)
Ingress : 192.168.8.105
Ingress : N/A (not in use)
Penultimate Hop Popping : Enabled
Refresh PATH msg parsing : Enabled
Refresh RESV msg parsing : Enabled

show rsvp running-config

CASA#show rsvp run
rsvp-path 1
192.85.1.4 loose
192.0.0.1 loose
!
rsvp-path 2
192.85.1.4 loose
!
router rsvp
explicit-null
hello-interval 10

show rsvp statistics

CASA#show rsvp statistics
PacketType Total
Sent Received
Path 0 0
PathErr 0 0
PathTear 0 0
Resv FF 0 0
Resv WF 0 0
Resv SE 0 0
Resv Err 0 0
ResvTear 0 0
ResvConf 0 0
Hello 0 0
Bundle 0 0
Ack 0 0

show rsvp graceful-restart [neighbor <ipv4_addr>]

CASA#show rsvp graceful-restart
Graceful Restart: Enabled
Advertised Restart Time: 60000 msec
Advertised Recovery Time: 60000 msec
Sending Recovery Time: No

 Remote addr: 13.13.13.2 Local addr: 13.13.13.1
 Nbr State: Normal, Type: Reroute
 Nbr Hello State: Lost
 LSPs protecting: 5
 Restart Time: 0 msec, Recovery Time: 0 msec
 Rest of Restart Time: 0 msec, Rest of Recovery Time: 0 msec

show rsvp neighbor [<addr>]
```

```
CASA#show rsvp neighbor
IP Address UpStrm LSP DnStrm LSP RefreshReduc Srefresh In Type
192.166.8.10 0 0 Disabled not running Explicit

show rsvp path

CASA#show rsvp path
Path name: RSVPPATH, id: 1, hop-count: 1 type: mpls
192.168.8.8 strict

show rsvp trunk [<name> | detail]

CASA#show rsvp trunk RSVPTRUNK
Trunk name: RSVPTRUNK, tunnel-id: 101
Type: P2P
Ext-tunnel-id: 192.168.8.8/32
Egress: 192.168.8.10/32
# of LSPs in trunk: 1
```

3.18.11. Verifying Internet Group Management Protocol Configurations Overview

The Internet Group Management Protocol (IGMP) is used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicasting and can be used for one-to-many networking applications such as online streaming video and gaming. It allows more efficient use of resources when supporting these types of applications. (Cablelabs, 2015)

IGMP is used on IPv4 networks. Multicast management on IPv6 networks is handled by the Multicast Listener Discovery (MLD) protocol that uses ICMPv6 messaging instead of IGMP’s bare IP encapsulation. IGMPv1 is defined by RFC 1112, IGMPv2 is defined by RFC 2236, and IGMPv3 was initially defined by RFC 3376 and has been updated by RFC 4604, which defines both IGMPv3 and MLDv2. The IGMP and MLD clients are supported simultaneously but must be configured independently.

An IGMP proxy interface can be configured to handle traffic on multiple interfaces. Also, DOCSIS MAC and video interfaces should independently join different, non-overlapping multicast sessions. If they join the same multicast session (*,G or S,G), a configuration error occurs. DOCSIS and video interfaces cannot share the same VLAN ID. For overlapping sessions, the video stream receives priority.

IGMP (or MLD) and the Protocol Independent Multicast (PIM) protocol cannot coexist on the same interface. The two protocols behave differently. While PIM/PIM6 selects only one upstream interface to forward the multicast join based on routing table lookup (best/equal cost path to the source/RP), IGMP/MLD joins all enabled upstream interfaces without a route lookup. Therefore only one mode of operation for IP multicasting is supported, IGMP/MLD proxy mode or PIM/PIM6 routing. To configure IGMP, PIM (if previously enabled) must first be disabled.

3.18.11.1. Video Use Case on Verifying IGMP Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
show igmp mroute [<grp_addr>] [source <mcast_src>]

CASA#show igmp mroute 224.10.10.0
224.10.10.1/0.0.0.0
Incoming Interface: video 1 (gige 7/1)
Outgoing Interface List: qam 2
Total entries : 1

show igmp {cache-table | client-db | debug | interface | mroute}

CASA#show igmp interface
Interface Ver Pri Prefix ACL Link FibCnt Address
gige 6/1 v3 0 GIGE6/1 up 0 17.56.203.2
Total entries : 1

show igmp client-db [<ip_addr> [source <ip_addr>]]

CASA#show igmp client-db 229.0.99.1
VRF Group/Source Vif Module Pri State
0 229.0.99.1/0.0.0.0

show ip multicast traffic [<grp_addr> | docsis | video]

CASA#show ip multicast traffic
Flags: VI = video, DS = docsis, FW = forward, BL = blocked
NONE = no reason, NOMR = no mroute, DUPL = duplicate
RPTP = rpt prune, WIIF = wrong iif, WMAC = wrong mac
WOIF = wrong oif, NRPF = no rpf route, NARP = unresolved arp
Multicast Group Source IP NextHop MAC Src Intf Out Intf Rate (pps, kbps)
Flags Up Time
230.55.0.1 198.24.25.55 20fd.f1e4.3f4a xgige 7/0 qam 4 445 , 912 VI,FW
15:04:51
```

3.18.12. Verifying Multicast Listener Discovery Configurations

Overview

The Multicast Listener Discovery (MLD) protocol is a component of IPv6 and used by IPv6 routers for discovering multicast listeners on a directly attached link, much like the Internet Group Management Protocol (IGMP) is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 similar to IGMPv3. The protocol is described in RFC 3810, updated by RFC 4604. The IGMP and MLD clients are supported simultaneously but need to be configured independently.

DOCSIS MAC and video interfaces should independently join different, non-overlapping multicast sessions. If they join the same multicast session (*,G or S,G), a configuration error occurs. DOCSIS and video interfaces cannot share the same multicast session. If they do overlap, the video stream takes priority.

MLD (or IGMP) and the Protocol Independent Multicast (PIM) cannot coexist on the same interface. The two protocols behave differently. While PIM/PIM6 selects only one upstream interface to forward the multicast join based on routing table lookup (best/equal cost path to the source/RP), IGMP/MLD joins all enabled upstream interfaces without any route lookup. Therefore only one mode of operation for IP multicasting is supported, IGMP/MLD proxy mode or PIM/PIM6 routing. To configure MLD, PIM (if previously enabled) must first be disabled. However, MLD and IGMP can exist on the same interface in that they serve different IP versions.

3.18.12.1. Video Use Case on Verifying MLD Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
show mld interface

CASA#show mld interface
Interface Ver Pri Prefix ACL Link FibCnt Address
vlan 1862 v2  0              up   0      2001:0:144::178
xgige 6/7 v1  0   MldGige6/7 up   0      2001:178:88:11::178
gige 6/0  v2  0              up   0      2001:0:143::178
trunk 10  v2  0              up   0      2001:191:78:1::178
```

```
Total entries : 4

show mld client-db [<ip6_addr> [source <ip6_addr>]]

CASA#show mld client-db
VRF Group/Source Vif Module Pri State
Total entries : 0

CASA#show mld mroute
ff9e::94:1234/::
  Incoming Interface: gige 7/1
  Outgoing Interface List: qam 0, qam 2
ff9e::94:5678/4080::10:94
  Incoming Interface: gige 7/1
  Outgoing Interface List: qam 0, qam 2
Total entries : 2

CASA(config)# show ipv6 multicast traffic
Flags: VI = video, DS = docsis, FW = forward, BL = blocked
  NONE = no reason, NOMR = no mroute, DUPL = duplicate
  RPTP = rpt prune, WIIF = wrong iif, WMAC = wrong mac
  WOIF = wrong oif, NRPF = no rpf route, NARP = unresolved arp
Multicast Group Source Intf NextHop MAC    Src Intf
                            Out Intf  Rate (kb) Flags Up Time
ff9e::94:1234   4080::10:94 0001.7016.8010 gige 6/0
                            qam 4     20        DS,FW 00:00:04
                            qam 4     20        DS,FW 00:00:04
ff9e::94:5678 4080::10:94 0001.7016.8010   gige 6/0
                            qam 4     20        DS,FW 00:00:28
                            qam 4     20        DS,FW 00:00:28
```

3.18.13. Verifying Protocol Independent Multicast Configurations

```
Overview
```

Protocol Independent Multicast in Sparse Mode (PIM-SM), as defined in RFC 2362, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*, is a multicast routing protocol that maintains multicast datagram forwarding tables for wide area and sparse multicast distribution. The PIM-SM implementation on the CMTS supports shared distribution from a configured Rendezvous Point (RP), RP discovery using a static configuration or a bootstrap router (BSR), and sourced-based trees over Source-Specific Multicast (SSM) where hosts can specify the source and multicast group from which to receive multicast data streams.

PIM-SM can be enabled and configured on GigE and loopback interfaces. Internet Group Management Protocol (IGMP) and PIM-SM cannot coexist on the same interface. To configure PIM-SM, IGMP (if previously enabled) must first be disabled.

3.18.13.1. Video Use Cases on Verifying PIM-SM Configurations

Click here for a video use case on this topic.

The use case on Verifying PIM-SM Configurations contain the commands below.

```
show ip pim running-config

CASA#show ip pim running-config
-output cut-
ip pim jp-rate-limit 50 5

show ip pim running-config [verbose]

CASA#show ip pim running-config verbose
ip pim spt-threshold infinity
ip pim ssm default
ip pim rpf-profile default

show run | include pim

CASA#show run | include pim
!pim command
ip pim bsr-candidate gige 1 16 100 slot 6

show run | inc “ip pim”

CASA#show run | inc “ip pim”
ip pim rp-address 105.105.105.105 access-list 105-rp
ip pim trap invalid-pim-message enable

show ip pim interface

CASA#show ip pim interface
IP Address Interface Ver/ Nbr DR DR IP Address DR MAC Address State Cnt
Prior

show ip pim debug

CASA#show ip pim debug
PIM debugging status:
IP PIM error debug on
```

The use case on Verifying PIM-SM Networking Configurations contains the commands below.

```
show ip pim neighbor

CASA# show ip pim neighbor
IP Address Interface Hold Join DR Uptime/Expires MAC Address Time Attr Prior

show ip pim bsr-router

CASA#show ip pim bsr-router
This system is the Bootstrap Router (BSR)
BSR address:192.168.3.232
Uptime: 0:0:10:8,BSR Priority:0, Hash mask length:10
Next bootstrap message in 7
Candidate RP: 192.168.3.232(gige 1)
Holdtime 150 seconds
Advertisement interval 60 seconds
Next advertisement in 7

show ip pim rp

CASA#show ip pim rp
Group(s) 224.0.0.0/4, Static
RP 143.1.1.1, static

show ip pim rp mapping

CASA#show ip pim rp mapping
Group(s) 224.0.0.0/4
RP 192.168.3.232, v2
Info source: 192.168.3.232, via bootstrap, priority 0, holdtime 150
Uptime: 0:0:44:8, expires: 148

show ip pim rp-hash <grp_addr>

CASA#show ip pim rp-hash 192.168.8.232
rp address :76.160.35.72
RP 76.160.35.72, v2
Info source: 0.0.0.7, via bootstrap, priority 0, holdtime 1
Uptime: 14677:11:17:52, expires:0
PIMv2 Hash Value (mask 192.168.3.232)

show ip pim vrf <name> <property>

Shows the VRF setting for the specified property, as follows:
• bsr-router
• interface
• neighbor
• rp
• rp-hash <grp_addr>
• running-config [verbose]
```

3.19. Verifying IPsec Configurations

Overview

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), a pair of security gateways (network-to-network), or a security gateway and a host (network-to-host).

3.19.1.1. Video Use Case on Verifying IPsec Configurations

Click here for a video use case on this topic.

The use case contains the commands below.

```
show ipsec info

CASA#show ipsec info
IKE status: running
---------------------------------------
phase I:
policy name : POLIPSEC1
IP address : 192.168.2.125
exchange mode: aggressive, main
lifetime : 60
proposal : encryption : tripple DES
hash : MD5
auth-method: other
dh-group : 1
phase II:
policy name : POLIPSEC2
IP address source : 192.168.2.126
IP address remote : 192.168.5.205
lifetime : 20
encryption : null
hash : SHA
compression-method: deflate

show ipsec prekey

CASA#show ipsec prekey
192.168.2.125 PACKETCABLE

show ipsec spd
```

```
CASA#show ipsec spd
IPsec SPD configuration:
remote ip address: 192.168.2.125
local ip address : 192.168.2.247
protocol : any
direction : in
ipsec mode : ESP
local ip address : 192.168.2.247
remote ip address: 192.168.2.125
protocol : any
direction : out
ipsec mode : ESP
```

4. Example Configuration Demos and Text Files

Chapter Overview

This section will provide links to downloadable example configuration files and, in some cases, a companion video demonstration.

4.1. Physical RFI Configuration

4.1.1. Demonstrations

Configuring OFDM Demo

Configuring OFDMA Demo

Configuring Pre-equalization

Configuring Small Signal Compensation

Configuring Interleaving

Configure Casa Spectrum Management Demo

4.1.2. Example Configuration Text Files

OFDM Example Configuration Text File

OFDMA Example Configuration Text File

Pre-equalization Example Configuration Text File

Small Signal Compensation Example Configuration Text File

Interleaving Example Configuration Text File

Casa Spectrum Management Example Configuration Text File

4.2. MAC Domain Configuration

Configuring Service Groups Demo

Service Groups Example Configuration Text File

Configuring Load Balancing Demo

Load Balancing Example Configuration Text File

4.3. Cable Modem IP Operations Configuration

Configuring Cable Modem IP Operations

Configuring DHCP Leasequery Demo

4.4. OSSI Configuration

Configuring TACACS Presentation

Configuring SNMP Presentation

Configuring IPDR Presentation

4.5. Layer 2 Configuration

Configuring VLANs

4.6. Security Configuration

Configuring Access Controls

Configuring an Access Group Demonstration

4.7. Routing Configuration

Configuring Static Routes Demonstration

Configuring OSPFv2 Demonstration

Configuring IS-IS Demonstration

Configuring BGP

Configuring Policy Based Routing

Configuring VRF

5. Table of Video Presentations

100 Old River Suite 100
Andover MA 01810
USA
978-688-6706

Casa Systems Learning Solutions