Avaya

Configuration Guide

AVAYA C460

MULTILAYER MODULAR SWITCH

SOFTWARE VERSION 2.0

May 2003

AVAYA

avaya.com

Document no. 555-500-105

Contents

List of Tables

List of Figures

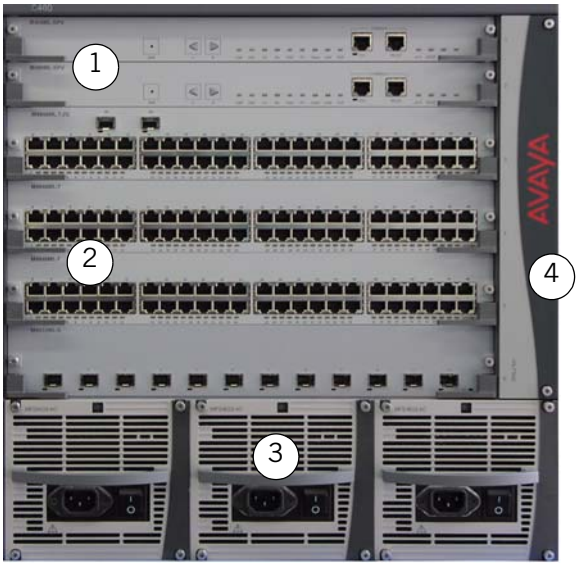
Chapter 1

Avaya C460 Product Overview

Introduction

The Avaya C460 is a high-performance multilayer modular switch with two Supervisor module slots, four I/O slots and up to three Power Supply Units. It features full redundancy from switching fabric to port level.

Figure 1.1 The Avaya C460 Switch – Front View



Key

1 Supervisor modules
2 I/O modules
3 PSUs
4 Fan module

Avaya C460 Main Components

ⓘ For information on Installation, Troubleshooting and Maintenance of these components, refer to the "Avaya C460 Installation and Maintenance Guide."

Supervisor Modules

The C460 Supervisor modules form the core of the C460. Their functions include:

- Chassis-wide controlling
- I/O module initialization
- Switching fabric initialization
- Switching
- Layer 3 functionality, including routing
- SNMP management agent
- PSU & fan monitoring
- Power budgeting and management
- User interface
- Management interface

I/O Modules

The I/O modules provide the connections to your network devices, such as workstations, printers, servers and other switches.

The I/O modules include:

Name	Description
M4648ML-T	48 10/100 Mbps ports
M4648ML-T-2G	48 10/100 Mbps + 2 SFP GBIC ports
M4612ML-G	12 SFP GBIC ports
M4648ML-T-PWR	48 10/100 Mbps PoE ports
M4648ML-T-2G-PWR	48 10/100 Mbps PoE ports + 2 SFP GBIC ports

PSUs (Power Supply Units)

You can install up to three PSUs in a C460 chassis. Each PSU is equipped with a cooling fan, an AC power entry filter module, an on/off switch and a status LED.

Chapter 2

Establishing Switch Access

Introduction

This chapter describes how to access the Avaya C460 CLI from the following devices:

- A terminal to the serial port on the Supervisor Module
- A workstation running a Telnet session connected via an I/O module (Inband)
- A workstation running a Telnet session connected to the Console Fast Ethernet port on a Supervisor module (outband)
- A remote terminal/workstation attached via a modem (PPP connection) to the Supervisor Console Serial port. (Sideband)

Establishing a Console Connection with the C460

Figure 2.1 M460ML-SPV Supervisor Module Serial Console Port

Perform the following steps to connect a terminal to the C460 Serial Console port for configuration of switch parameters:

1 Use the serial cable supplied to attach the RJ-45 console connector to the Console port of the active M460ML-SPV module. Connect the DB-9 connector to the serial (COM) port on your PC/terminal.

ⓘ The active Supervisor module is indicated by the ACT and OPR LEDs being lit.

2 Ensure that the serial port settings on the terminal are:

— 9600 baud
— 8 bits
— 1 stop bit
— no parity.

▶ If you reset or powered up the switch after connecting and configuring the terminal, `Welcome to C460` appears followed by the Login Name prompt.

ⓘ If the login prompt does not appear, press a key on the terminal.

3 Enter the default login: **`root`**.

▶ The Password prompt appears

4 Enter the user level password: **`root`**.

ⓘ If you connect your terminal to the Standby SPV, you can get access to all the CLI commands by opening a Session to the Active SPV.

Establishing a Telnet Connection with the Switch (Inband)

Perform the following steps to establish a Telnet connection to the C460 for configuration:

ⓘ You need to assign an inband interface IP address using a direct connection to the console serial port before you can establish the Telnet session.

1 Connect your station to the I/O module (directly or via the network).

2 Verify that you can communicate with the C460 using Ping to the inband interface IP of the C460. If there is no response using the Ping command, check the IP address and default gateway of both the C460 and the station.

ⓘ The default subnet mask is 255.255.255.0.

3 Start a Telnet session:

— From the Microsoft Windows® taskbar of your PC click **Start** and then **Run** or access the command prompt

— Start the Telnet session by typing: **telnet** *<C460_IP_address>*
For example: **telnet 149.49.35.214**

▶ The Login Name prompt is displayed

4 Enter the default name **root**

▶ The password prompt is displayed

5 Enter the password **root** in lower case letters.

ⓘ You can now configure the C460.

Inband Interface Connection CLI Commands

In order to...	Use the following command...
Configure the management interface	set interface inband
Configure the management VLAN ID	set inband vlan
Enable the inband interface	enable interface inband
Disable the inband interface	disable interface inband
Display information on the device network interfaces	show interface

In order to...	Use the following command...
Send an ICMP echo request packets to another node on the network.	ping

ⓘ For more detailed information on the CLI commands, please refer to the *Avaya C460 Reference Guide*

Establishing a Telnet Connection with the Switch (Outband)

Figure 2.2 M460ML-SPV Supervisor Module Fast Ethernet Console Port

Perform the following steps to establish a Telnet connection to the C460 for configuration:

ⓘ You need to assign an outband interface IP address using a direct connection to the console serial port before you can establish the Telnet session.

ⓘ You can configure the Fast Ethernet console port parameters if necessary.

ⓘ The outband interface should be on a different subnet from the inband interface.

1 Connect your station to the Fast Ethernet console port (directly or via the network).

2 Verify that you can communicate with the C460 using "ping" to the outband interface IP of the C460. If there is no response using the Ping command, check the IP address and default gateway of both the C460 and the station.

3 Start a Telnet session:

— From the Microsoft Windows® taskbar of your PC click **Start** and then **Run** or access the command prompt

— Start the Telnet session by typing: **telnet** *<C460_IP_address>*
For example: **telnet 149.49.35.214**

▶ The Login Name prompt is displayed

4 Enter the default name **root**

▶ The password prompt is displayed

5 Enter the password **root** in lower case letters.

ⓘ You can now configure the C460.

ⓘ You can connect the Out-band interface to either of the Supervisor modules.

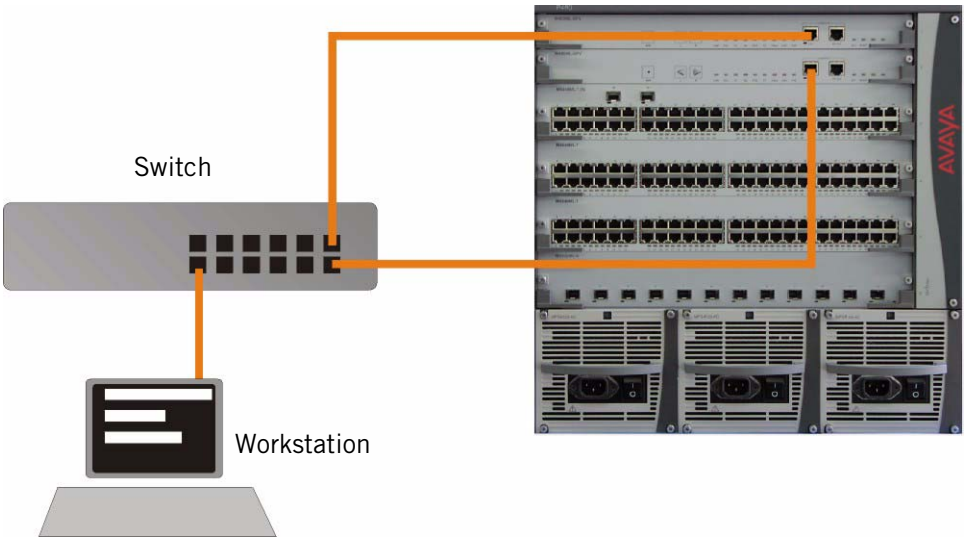
Outband Interface Connection CLI Commands

In order to...	Use the following command...
Configure the management interface	set interface outband
Enable the outband interface	enable interface outband
Disable the outband interface	disable interfaceoutband
Enable or disable the link negotiation protocol on the Fast Ethernet console port	set outband negotiation
Set the speed of Fast Ethernet Console port	set outband speed
Set the duplex mode of the Ethernet Console port	set outband duplex
Display information on the device network interfaces	show interface
Display outband interface parameters	show outband
Send an ICMP echo request packets to another node on the network.	ping

Redundant Outband Connections

You can create a redundant outband management connection by connecting both Supervisor modules to the NMS via the Fast Ethernet interface by a switch (see Figure 2.3).

Figure 2.3 Redundant Outband Connections



In this configuration, the Active SPV will respond to its Out-band port and the port of the other SPV will be ignored.

Establishing a PPP via Modem Connection with the C460 (Sideband)

Overview

The Point-to-Point Protocol (PPP) provides a Layer 2 method for transporting multi-protocol datagrams over point-to-point links. Here only IP datagrams will be exchanged, over a RS232 serial connection, between the C460 supervisor module and a remote peer (such as Ethernet) via a modem and the telephone lines. This provides remote access the sideband management interface of a C460 via a modem.

Sideband (PPP) Interface CLI Commands

In order to...	Use the following command...
Configure the device ppp interface and control a PPP session	set interface ppp
Configure the shared secret used in PPP sessions with CHAP authentication	set ppp chap-secret
Set the time after which the system automatically disconnects an idle PPP incoming session	set ppp incoming timeout
Define the PPP authentication method	set ppp authentication incoming
Set the baud rate used in PPP sessions	set ppp baud-rate
Display the PPP parameters of the active PPP session.	show ppp session
Display the authentication method used for PPP sessions	show ppp authentication
Display the time after which the system automatically disconnects an idle PPP incoming session	show ppp incoming timeout
Display the baud rate used in PPP sessions	show ppp baud-rate
Display the ppp configuration	show ppp configuration

Setting Up Sideband (PPP) Connection Configuration

ⓘ You need to configure an IP address and netmask for the sideband interface before you can establish a ppp link.

1 Connect a terminal to the Serial console port.

2 When you are prompted for a Login Name, enter the default name **root**.

3 When you are prompted for a password, enter the password **root**. You are now in Supervisor Level.

4 At the prompt, type:
set interface ppp <ip_addr><net-mask>
with an IP address and netmask to be used by the Avaya C460 Supervisor module to connect via its PPP interface.

ⓘ The PPP interface you configure with the set interface ppp command must be on a different subnet from the inband and outband interfaces.

5 Set the baud rate, ppp authentication, and ppp time out required to match your modem. These commands are described in the "Command Line Interface" chapter.

6 At the prompt, type:
set interface ppp enable

▶ The following is displayed:

```
Entering the Modem mode within 60 seconds...
Please check that the proprietary modem cable is plugged
into the console port
```

7 Use the DB-25 to RJ-45 connector to plug the console cable to the modem's DB-25 connector. Plug the other end of the cable RJ-45 connector to an Avaya C460 Supervisor module RJ-45 port.

8 The Avaya C460 Supervisor module enters modem mode.

9 You can now dial into the switch from a remote station, and open a Telnet, ping or SNMP management session to the PPP interface IP address.

ⓘ If you have two Supervisor modules installed, you can make a serial connection to one SPV and configure the PPP parameters through one session and deploy the PPP connection on the second Supervisor module.

Chapter 3

Avaya C460 Supervisor Module Features

Introduction

The Avaya C460 Supervisor module provides the following functionality:

- Chassis-wide control
- I/O module initialization
- Fabric initialization
- Switching that also uses also the fabric of the second SPV
- Layer 3 functionality including routing
- SNMP Management agent
- PSU & Fans monitoring
- Power Budgeting & Management
- User interface
- Management interface

At least one SPV is essential for the switch operation. When two SPVs are installed, one serves as the active, while the other one is a stand-by.

The switching fabric of a standby Supervisor module actively participates in packet switching/routing even when its CPU is inactive.

M460ML-SPV Supervisor Module Modes:

- *Active* – The Supervisor Module is operating
- *Standby* – This Supervisor Module is fully synchronized with the Active one and can replace it in the case of failure.
- *Halted* – This Supervisor Module is not synchronized with the Active one and cannot act as a standby module.

You can verify the Supervisor Module mode by:

- The ACT and OPR LED status (refer to Table 3.1),
- The **`show SPV`** CLI using the command, or
- The C460 Manager

Table 3.1 ACT and OPR LED Summary

ACT LED is...	OPR LED is...	M460ML-SPV Module mode
ON	ON	Active

Table 3.1 ACT and OPR LED Summary

ACT LED is...	OPR LED is...	M460ML-SPV Module mode
ON	Blinking	Active *No fan module present*
OFF	ON	Standby
OFF	Blinking	Halted or booting

Supervisor Synchronization

Configuring the Supervisor Modules for Active/Standby Operation

In order to operate in an Active-Standby configuration, the two SPVs must be synchronized.

- If the SPVs are not synchronized, one is Active and the other Halted.
  In this case you will need to synchronize them manually. See "Synchronizing the Supervisor Modules Manually" on page 12.
- Only in Active-Standby configuration do both SPV fabrics participate in switching/routing
- An SPV which was Active stays Active after a chassis reset

One of the SPVs can operate as Standby automatically only if both of the following conditions are fulfilled:

- The current chassis is the last one in which you inserted this SPV
- The current running SW images are the same version

Synchronizing the Supervisor Modules Manually

If the SPVs are not synchronized, you need to synchronize them manually using the Avaya C460 CLI.

ⓘ Synchronization can be required for a complete synchronization also if the SPVs are in an Active-Standby configuration. For example, when the SPVs boot with the same SW but from different banks

1 Access the CLI. See Chapter 2, "Establishing Switch Access"

2 Enter the **`sync spv`** command from the Active Supervisor Module.

ⓘ This command transfers the following information from the Active Supervisor module to the other Supervisor module.

- Firmware images
- Embedded Web image
- Preferred boot bank
- Chassis synchronization

- The transfer process can take up to 90 seconds.
- The following screen capture shows the process:

```
C460-1(super)# sync spv
This command may overwrite the neighbor SPV software and
reset both SPVs
*** Confirmation *** - do you want to continue (Y/N)? y
Copying Bank A to the neighbor SPV ...
Copying Bank A to the neighbor SPV done
Copying Bank B to the neighbor SPV ...
Copying Bank B to the neighbor SPV done
Copying Embedded Web image to the neighbor SPV ...
Copying Embedded Web image to the neighbor SPV done
Setting boot bank of the neighbor SPV ...
Setting boot bank of the neighbor SPV done
Setting chassis sync on for the neighbor SPV...
Setting chassis sync on for the neighbor SPV done
SPVs are resetting.
Please wait till the process is finished. The SPVs will be
synchronized after the reset is completed
```

- After the transfer is finished, the Supervisor Modules are reset automatically.
  - After the reset the configuration files of the Active Supervisor Module will be copied to the Standby Supervisor Module.
- This process can take up to two minutes.

Configuration File Synchronization

Three configuration files are stored in the Supervisor module flash memory:

- Layer 2 configuration (L2-config)
- Layer 3 running configuration (running-config)
- Layer 3 startup configuration (startup-config)

If SPVs are present, the configuration is automatically synchronized between the Active and Standby Supervisor modules.

- *Initial configuration* synchronization takes place after the boot: this process can take up to thirty seconds.
- *Layer 2* configuration changes are saved in both Supervisor modules when you press Enter.
- The Supervisor module Ethernet outband interface configuration is *not* synchronized between the modules.
- *Layer 3 startup configuration* is saved in the Standby SPV when you execute the `copy running-config startup-config` CLI command. This

configuration is also saved in the Active SPV

ⓘ The Layer 3 running configuration is not saved in the Standby SPV

Chapter 4

Avaya C460 Layer 2 Features

Ethernet

Ethernet is one of the most widely implemented LAN standards.

It uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method to handle simultaneous demands. CSMA/CD is a multi-user network allocation procedure in which every station can receive the transmissions of any other station. Each station waits for the network to be idle before transmitting and each station can detect collisions by other stations.

The first version of Ethernet supported data transfer rates of 10 Mbps, and is therefore known as 10BASE-T.

Fast Ethernet

Fast Ethernet is a newer version of Ethernet, supporting data transfer rates of 100 Mbps. Fast Ethernet is similar enough to Ethernet to support the use of most current Ethernet applications and network management tools. Fast Ethernet is also known as 100BASE-T (over copper) or 100BASE-FX (over fiber).

Fast Ethernet is standardized as IEEE 802.3u.

Gigabit Ethernet

Gigabit Ethernet supports data rates of 1 Gbps. It is also known as 1000BASE-T (over copper) or 1000BASE-FX (over fiber).

Gigabit Ethernet is standardized as IEEE 802.3z.

Configuring Ethernet Parameters

Auto-negotiation

Auto-Negotiation is a protocol that runs between two stations, two switches or a station and a switch. When enabled, Auto-Negotiation negotiates port speed and duplex mode by detecting the highest common denominator port connection for the endstations. For example, if one workstation supports both 10 Mbps and 100 Mbps speed ports, while the other workstation only supports 10 Mbps, then Auto-Negotiation sets the port speed to 10 Mbps.

For Gigabit ports, Auto-Negotiation determines the Flow Control configuration of the port.

The Avaya C460 supports auto-negotiation enabling/disabling on a per-port basis.

Flow Control

Flow Control ensures that the receiving device can handle all the incoming data. Flow control does this by adjusting the data flow from one device to another. This is particularly important where the sending device can send data much faster than the receiving device can receive the data.

There are many flow control mechanisms. One of the most common flow control protocols for asynchronous communication is called xon-xoff. In this case, the receiving device sends a an xoff message to the sending device when its buffer is full. The sending device then stops sending data. When the receiving device is ready to receive more data, it sends an *xon* signal.

Flow control can be implemented in hardware or software, or a combination of both. The C460 uses hardware flow control.

Duplex Mode

Devices that support full-duplex can transmit and receive data simultaneously. Half-duplex transmission where each device can only communicate in turn.

Full-duplex provides higher throughput than half-duplex.

The Avaya C460 supports both full duplex and half duplex.

Speed

The IEEE defines three standard speeds for Ethernet: 10, 100 and 1000 Mbps, also known as Ethernet, Fast Ethernet and Gigabit Ethernet respectively.

The Avaya C460 supports the following port speeds:

- 10/100 Mbps
- 1000 Mbps

MAC Address

The MAC address is a unique 48-bit value associated with any network adapter. MAC addresses are also known as hardware addresses or physical addresses. They uniquely identify an adapter on a LAN.

MAC addresses are 12-digit hexadecimal numbers (48 bits in length). By convention, MAC addresses are usually written in one of the following two formats:

- MM:MM:MM:SS:SS:SS
- MM-MM-MM-SS-SS-SS

The first half of a MAC address contains the ID number of the device manufacturer. An Internet standards body regulates these IDs. The second half of a MAC address represents the serial number assigned to the device by the manufacturer.

CAM Table

It might be inefficient if the Avaya C460 could not "remember" which MAC address was accessible from which port, that is, where a specific device is attached. Therefore, the C460 stores a mapping of learned MAC addresses to port and VLANs in the *CAM table.* The switch then checks subsequent frames. If the MAC address appears in the CAM Table, then the packet is forwarded to the appropriate port.

If the MAC address does not appear in the CAM table, or the MAC Address mapping has changed, then the frame is duplicated and copied to all the ports. Once a reply is received, the CAM table is updated with the new address/VLAN port mapping.

The CAM table size in the Avaya C460 is a minimum of 4k and a maximum of 8k.

Ethernet Configuration CLI Commands

In order to...	Use the following command...
Set the auto negotiation mode of a port	set port negotiation
Administratively enable a port	set port enable
Administratively disable a port	set port disable
Set the speed for a 10/100 port	set port speed
Configure the duplex mode of a 10/100BASE-T port	set port duplex
Configure a name for a port	set port name
Set the send/receive mode for flow-control frames on a full duplex port	set port flowcontrol
Set the flow control advertisement for a Gigabit port when performing autonegotiation	set port auto-negotiation-flowcontrol-advertisement
Display settings and status for all ports	show port
Display per-port status information related to flow control	show port flowcontrol
Display the flow control advertisement for a Gigabit port used to perform auto-negotiation	show port auto-negotiation-flowcontrol-advertisement

In order to...	Use the following command...
Display the CAM table entries for a specific port	show cam
Display a specific mac/vlan in the CAM CAM table	show cam mac
Display all MAC entries for a specific VLAN in the CAM	show cam vlan
Clear all the CAM entries.	clear cam
Send ICMP echo request packets to another node on the network.	ping

Ethernet Configuration Examples

This example shows basic Ethernet configuration for port 40 on I/O module 6:

1 Disabling port negotiation

```
C460-1(super)# set port negotiation 6/40 disable

Link negotiation protocol disabled on port 6/40
```

2 Setting port duplex to full

```
C460-1(super)# set port duplex 6/40 full

Port 6/40 speed set to full duplex
```

3 Setting port speed to 100 Mbps

```
C460-1(super)# set port speed 6/40 100mb

Port 6/40 speed set to 100MBps
```

4 Enabling port negotiation

```
C460-1(super)# set port negotiation 6/40 enable

Link negotiation protocol enabled on port 6/40
```

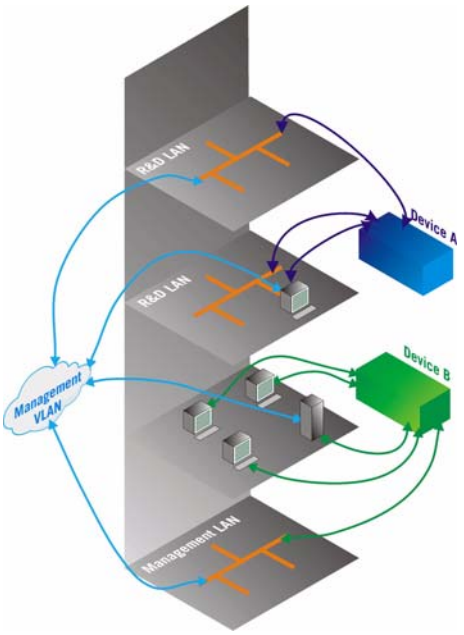
VLAN Configuration

VLAN Overview

A VLAN is made up of a group of devices on one or more LANs that are configured so the devices operate as if they form an independent LAN. These devices can, in fact, be located on several different LAN segments. VLANs can be used to group together departments and other logical groups, thereby reducing network traffic flow and increasing security within the VLAN.

Figure 4.1 illustrates how a simple VLAN can connect several endpoints in different locations and attached to different hubs. In this example, the Management VLAN consists of stations on numerous floors of the building which are connected to both Device A and Device B.

Figure 4.1 VLAN Overview



In virtual topological networks, the network devices can be located in diverse places around the LAN. These devices can be in different departments, on different floors or in different buildings. Connection is achieved through software. Each network device is connected to a hub, and the network manager uses management software to assign each device to a virtual topological network. Elements can be combined into a VLAN even if they are connected to different devices.

You can use VLANs whenever there are one or more groups of network users that you want to separate from the rest of the network.

In Figure 4.2, the switch has three separate VLANs: Sales, Engineering, and Marketing. Each VLAN has several physical ports assigned to it with PC's connected to those ports. When traffic flows from a PC on the Sales VLAN, for example, that traffic is *only* forwarded out the other ports assigned to that VLAN. Thus, the Engineering and Mktg VLANs are not burdened with processing that traffic.

Figure 4.2 VLAN Switching and Bridging

VLAN Tagging

VLAN Tagging is a method of controlling the distribution of information on the network. The ports on devices supporting VLAN Tagging are configured with the following parameters:

- Port VLAN ID
- Tagging Mode

The Port VLAN ID is the number of the VLAN to which the port is assigned.

ⓘ You need to create a VLAN with the `set vlan` command before you can assign it to a port.

Untagged frames and frames tagged with VLAN 0 entering the port are assigned the port's VLAN ID. Tagged frames are unaffected by the port's VLAN ID.

The Tagging Mode determines the behavior of the port that processes outgoing frames:

- If Tagging Mode is set to "Clear", the port transmits frames that belong to the port's VLAN table. These frames leave the device untagged.
- If Tagging Mode is set to "IEEE-802.1Q", all frames keep their tags when they leave the device. Frames that enter the switch without a VLAN tag are tagged with the VLAN ID of the port they entered through.

Multi VLAN Binding

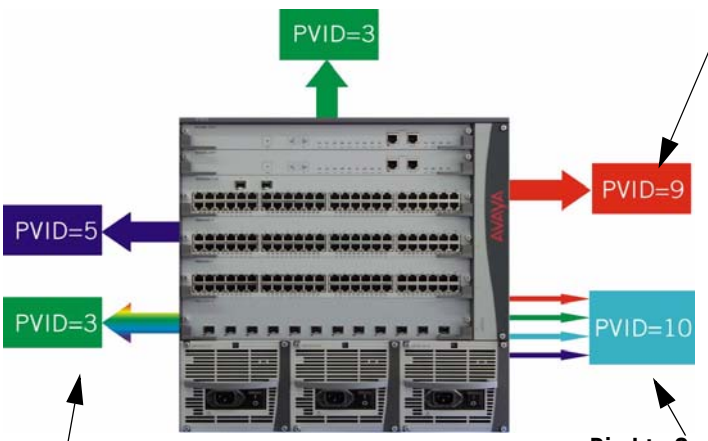
Multi VLAN binding, also known as Multiple VLANs per port, allows access to shared resources by stations that belong to different VLANs through the same port. This is useful in applications such as multi-tenant networks, where each user has his or her own VLAN for privacy. The whole building has a shared high-speed connection to the ISP.

In order to accomplish this, the C460 enables multiple VLANs per port. The three available Port Multi-VLAN binding modes are:

- **Bound to All** - the port is programmed to support the entire 4K VLANs range. Traffic from any VLAN is forwarded through a port defined as "Bound to All". This is intended mainly for easy backbone link configuration
- **Bound to Configured** - the port supports all the VLANs configured in the switch. These may be either PVIDs (Port VLAN IDs) or VLANs that were manually added to the switch.
- **Statically Bound** - the port supports VLANs manually configured on it.

Figure 4.3 shows these binding modes.

Figure 4.3 Multiple VLAN Per-port Binding Modes



Static Binding

- The user manually specifies the list of VLAN IDs to be bound to the port, up to 250 VLANs
- Default mode for all ports
- Only VLAN 9, and any other VLANs statically configured on the port will be allowed to access this port

Bind to All

- Any VLAN in the range of 1-4080 are allowed access through this port
- Intended mainly for easy backbone link configuration

Bind to Configured

- The VLAN table of the port will support all the Static VLAN entries and all the ports' VLAN IDs (PVIDs) present in the switch
- VLANs 1,3,5,9,10 coming from the bus are allowed access through this port
- All the ports in Bound to Configured mode support the same list of VLANs

C460 VLAN Table

The C460 VLAN table includes two types of VLANs:

- User-configured VLANs
- Dynamically learnt from the incoming traffic on the "Bind to All" ports

When the VLAN list reaches its maximum capacity it is locked. No VLANs are dynamically learned and it is not be possible to configure more VLANs manually.

If this occurs, use the `clear dynamic vlans` CLI command to free space in the VLAN list.

Any new VLAN, either configured by you or learnt from incoming traffic, are made known to all the modules in the system.

The C460 supports up to 250 VLANs in the table, both user-defined and dynamic.

Ingress VLAN Security

The Avaya C460 allows only packets tagged with VLANs that are configured on a specific port are permitted to enter the through that port. Ingress VLAN Security therefore allows easy implementation of security.

VLAN CLI Commands

In order to...	Use the following command...
Assign the Port VLAN ID (PVID)	set port vlan
Define the port binding method	set port vlan-binding-mode
Define a static VLAN for a port	set port vlan
Configure the tagging mode of a port	set trunk
Create VLANs	set vlan
Display the port VLAN binding mode settings	show port vlan-binding-mode
Display VLAN tagging information of the ports, port binding mode, port VLAN ID and the allowed VLANs on a port	show trunk
Display the VLANs configured in the switch.	show vlan

In order to...	Use the following command...
Display dynamically learned VLANs	show dynamic vlans
Clear VLAN entries	clear vlan
Clear a VLAN statically configured on a port	clear port static-vlan
Clear dynamic vlans *Only the VLANs learned by the switch from incoming traffic on the "bind to all" ports are cleared using this command*	clear dynamic vlans

VLAN Configuration Example

This example shows VLAN configuration for port 40 on I/O module on I/O module 6:

1 Defining VLAN 10 (switch-level)

```
C460-1(super)# set vlan 10

VLAN ID 10 created
```

2 Assigning VLAN 10 to port 40 on I/O module 6

```
C460-1(super)# set port vlan 10 6/40

VLAN 10 modified.
VLAN Mod/Ports
---- ---------
  10 6/40
```

3 Setting the port to “bind to configured” mode

```
C460-1(super)# set port vlan-binding-mode 6/40 bind-to-
configured

Set Port Vlan binding method:6/40
```

4 Assigning static vlan 22 to the port

```
C460-1(super)# set port static-vlan 6/40 22

VLAN 22 is bound to port 6/40
```

5 Displaying the VLAN configuration for the port

```
C460-1(super)# sh trunk 6/40
Port  Mode  Binding mode              Native vlan Vlans allowed on trunk
----- ----  ------------------------  ----------- ---------------------
 6/40 dot1q bound to configured vlans        10    1-3,10,22
```

ⓘ Ports 1 to 3 were already defined on the switch so were bound automatically to the port by the “bind-to-configured” CLI command

Spanning Tree Configuration

The Avaya C460 devices support both common Spanning Tree protocol (802.1d) and the enhanced Rapid Spanning Tree protocol (802.1w). The 802.1w is a faster and more sophisticated version of the 802.1d (STP) standard. Spanning Tree makes it possible to recover connectivity after an outage within a minute or so. RSTP, with its "rapid" algorithm, can restore connectivity to a network where a backbone link has failed in much less time.

Spanning Tree Protocol

The Spanning Tree Algorithm ensures the existence of a loop-free topology in networks that contain parallel bridges. A loop occurs when there are alternate routes between hosts. If there is a loop in an extended network, bridges may forward traffic indefinitely, which can result in increased traffic and degradation in network performance.

The Spanning Tree Algorithm:

- Produces a logical tree topology out of any arrangement of bridges. The result is a single path between any two end stations on an extended network.
- Provides a high degree of fault tolerance. It allows the network to automatically reconfigure the spanning tree topology if there is a bridge or data-path failure.

The Spanning Tree Algorithm requires five values to derive the spanning tree topology. These are:

1 A multicast address specifying all bridges on the extended network. This address is media-dependent and is automatically determined by the software.
2 A network-unique identifier for each bridge on the extended network.
3 A unique identifier for each bridge/LAN interface (a port).
4 The relative priority of each port.
5 The cost of each port.

After these values are assigned, bridges multicast and process the formatted frames (called Bridge Protocol Data Units, or BPDUs) to derive a single, loop-free topology throughout the extended network. The bridges exchange BPDU frames quickly, minimizing the time that service is unavailable between hosts.

Spanning Tree per Port

The Spanning Tree can take up to 30 seconds to open traffic on a port. This delay can cause problems on ports carrying time-sensitive traffic. You can therefore enable/disable Spanning Tree in the C460 on a per-port basis to minimize this effect.

Rapid Spanning Tree Protocol (RSTP)

About the 802.1w (RSTP) Standard

The enhanced feature set of the 802.1w standard includes:

- Bridge Protocol Data Unit (BPDU) type 2
- New port roles: Alternate port, Backup port
- Direct handshaking between adjacent bridges regarding a desired topology change (TC). This eliminates the need to wait for the timer to expire.
- Improvement in the time it takes to propagate TC information. Specifically, TC information does not have to be propagated all the way back to the Root Bridge (and back) to be changed.
- Origination of BPDUs on a port-by-port basis.

Port Roles

At the center of RSTP—specifically as an improvement over STP (802.1d)—are the roles that are assigned to the ports. There are four port roles:

- Root port — port closest to the root bridge
- Designated port — corresponding port on the remote bridge of the local root port
- Alternate port — an alternate route to the root
- Backup port — an alternate route to the network segment

The RSTP algorithm makes it possible to change port roles rapidly through its fast topology change propagation mechanism. For example, a port in the "blocking" state can be assigned the role of "alternate port." When the backbone of the network fails the port may be rapidly changed to forwarding.

Whereas the STA *passively* waited for the network to converge before turning a port into the forwarding state, RSTP *actively* confirms that a port can safely transition to forwarding without relying on any specific, programmed timer configuration.

RSTP provides a means of fast network convergence after a topology change. It does this by assigning different treatments to different port types. The port types and the treatment they receive follow:

- Edge ports — Setting a port to "edge-port" admin state indicates that this port is connected directly to end stations that cannot create bridging loops in the network. These ports transition quickly to forwarding state. However, if BPDUs are received on an Edge port, it's operational state will be changed to "non-edge-port" and bridging loops will be avoided by the RSTP algorithm. The default admin state of all ports is "edge-port".

ⓘ You must manually configure uplink and backbone ports (including LAG logical ports) to be "non-edge" ports, using the CLI command `set port edge admin state`.

- Point-to-point Link ports — This port type applies only to ports interconnecting RSTP compliant switches and is used to define whether the devices are interconnected using shared Ethernet segment or point-to-point Ethernet link. RSTP convergence is faster when switches are connected using point-to-point links. The default setting for all ports – automatic detection of point-to-point link – is sufficient for most networks.

Spanning Tree CLI Commands

In order to...	Use the following command...
Enable/Disable the spanning tree application for the switch	set spantree enable/disable
Set the version of the spanning tree default costs used by this bridge	set spantree default-path-cost
Set the bridge priority for spanning tree	set spantree priority
Set the RSTP bridge spanning tree max-age parameter	set spantree max-age
Set the RSTP bridge hello-time parameter	set spantree hello-time
Set the RSTP bridge forward-delay time parameter	set spantree forward-delay
Select between STP operation or RSTP switch operation	set spantree version
Set the cost of a port	set port spantree cost
Set the port as an RSTP port (and not as a common STA port)	set port spantree force-protocol-migration
Set the port as an RSTP edge port or non-edge port	set port edge admin state
Set the port point-to-point admin status	set port point-to-point admin status
Display the bridge and per-port spanning tree information	show spantree

In order to...	Use the following command...
Show the port's point-to-point admin and operational RSTP status	show port point-to-point status
Display a port's edge admin and operational RSTP state	show port edge state

LAG Configuration

LAG Overview

A LAG uses multiple ports to create a high bandwidth connection with another device. For example, assigning four 100BASE-T ports to a LAG on an M4648ML-T I/O module, allows the module to communicate at an effective rate of 400 Mbps with another switch.

LAGs provide a cost-effective method for creating a high bandwidth connection. LAGs also provide built-in redundancy for the ports that belong to a LAG. If a port in a LAG fails, another port in the LAG handles its traffic .

To create a LAG, you must select a base port. The behavior of the LAG is derived from the base port. The attributes of the base port, such as port speed, VLAN number, etc., are applied to the other ports in the LAG.

When created, each LAG is automatically assigned a logical port number. You can then use this logical port number for all configuration required for the LAG, such as Spanning Tree, Redundancy, and so on.

Configuring LAGs

- ⓘ You can only create LAGs by combining the same port types on the same I/O Module.
- ⓘ Table 4.1 summarizes possible LAG configurations:

Table 4.1 Possible LAG Configurations

Module	Maximum number of LAGs	Base port is...	Additional ports must be...	Logical port numbers
M4648ML-T M4648ML-T-PWR	6	10/100 Mbps	10/100 Mbps Part of the same group of 24 ports (1-24; 25-28)	101-103 (ports 1-24) 104-106 (ports 25-48)
M4648ML-T-2G M4648ML-T-2G-PWR	6	10/100 Mbps	10/100 Mbps Part of the same group of 24 ports (1-24; 25-28)	101-103 (ports 1-24) 104-106 (ports 25-48)
	1	GBIC	GBIC On same the module	107

Table 4.1 Possible LAG Configurations

Module	Maximum number of LAGs	Base port is...	Additional ports must be...	Logical port numbers
M4612ML-G	6	GBIC	GBIC Part of the same group of six ports (1-6; 7-12)	101-103 (ports 1-6) 104-106 (ports 7-12)

Logical Port Numbers

The logical port number is used to identify the LAG. For example, if you define one LAG containing ports 1 to 3 on an M4612ML-G module, the LAG has the logical port number 101.

This is useful for port configuration commands and port redundancy among other features.

LAG Redundancy

See Port Redundancy Configuration on page 33.

LAG CLI Commands

In order to...	Use the following command...
Enable or disable a Link Aggregation Group interface on the switch	set port channel
Display Link Aggregation Group information for a specific switch or port	show port channel

LAG Configuration Example

This example shows definition of a LAG called “C460lag” using ports 41 to 47 on I/O module 6:

```
C460-1(super)# set port channel 6/41-47 on C460lag
Port 6/41 channel mode set to on 6/104
Port 6/42 was added to channel 6/104
Port 6/43 was added to channel 6/104
Port 6/44 was added to channel 6/104
Port 6/45 was added to channel 6/104
Port 6/46 was added to channel 6/104
Port 6/47 was added to channel 6/104
```

ⓘ Port 41 is the base port

Port Redundancy Configuration

Port Redundancy Overview

Redundancy involves the duplication of devices, services, or connections, so, in the event of a failure, the redundant duplicate can take over for the one that failed.

Since computer networks are critical for business operations, it is vital to ensure that the network continues to function even if a piece of equipment fails. Even the most reliable equipment might fail on occasion, but a redundant component can ensure that the network continues to operate despite such failure.

Along with Link Aggregation Groups, which provide basic redundancy, the C460 offers an additional port redundancy scheme.

To achieve port redundancy, you can define a redundancy relationship between any two ports in a switch. One port is defined as the primary port and the other as the secondary port. If the primary port fails, the secondary port takes over.

You can configure up to 32 pairs of ports or LAGs per chassis: each pair contains a primary and secondary port or LAG. You can configure any type of port to be redundant to any other.

Secondary Port Activation

The secondary port takes over within one second and is activated when:

- The Primary port link not functioning
- The Primary port I/O module is removed
- The Primary port I/O module failed because of power down, hardware failure, and so on.
- Subsequent switchovers take place after the “min-time-between-switchovers” has elapsed.

Switchback

When the Primary port recovers a switch-back takes place if you have not disabled this in management.

Switchback Parameters

- “min-time-between-switchovers” - minimum time that is allowed to elapse before a Primary-Backup switchover
- “switchback-interval” – the minimum time the Primary port link has to be up before a switch-back to the Primary port takes place. If you set this to “never”, there is no switch-back to the Primary port when it recovers.

Redundancy CLI Commands

In order to...	Use the following command...
Define/delete a redundancy entry.	set port redundancy on/off
Enable port redundancy on the switch	set port redundancy enable
Disable port redundancy on the switch	set port redundancy disable
Set the minimum time that is elapses before a Primary-Backup switchover and the minimum time the Primary port link has to be up before a switch-back to the Primary port takes place	set port redundancy-intervals
Show port redundancy configuration	show port redundancy

- When you remove an I/O module, the port redundancy configurations are retained.
- If you replace the I/O module with the same type, redundancy will be re-established.
- If you replace the I/O module with a different type, the redundancy configuration will be restored to the default values.
- Any new redundancy definitions over-ride the retained configuration.

Port Redundancy Configuration Example

This example shows configuration of a port redundancy pair called "C460red" between ports 40 and 48 on I/O module 6 and its configuration.

```
C460-1(super)# set port redundancy 6/40 6/48 on C460red
C460red: Port 6/48 is redundant to port 6/40

Port redundancy is active - entry is effective immediately

C460-1(super)# set port redundancy disable
All redundancy schemes are disabled but not removed

C460-1(super)# set port redundancy enable
All redundancy schemes are now enabled

C460-1(super)# set port redundancy-intervals 10 none
Done!

C460-1(super)# sh port redundancy
Redundancy Name  Primary Port Secondary Port Status
---------------  ------------ -------------- ------
C460red          6/40         6/48           primary

Minimum Time between Switchovers: 10
Switchback interval: none
```

ⓘ When the user executes the set port redundancy disable command, the redundancy is disabled but the definitions are saved.

IP Multicast Filtering Configuration

Overview

IP Multicast is a method of sending a single copy of an IP packet to multiple destinations. Different applications including video streaming and video conferencing can use IP multicast.

The Multicast packet is forwarded from the sender to the recipients, duplicated only when needed by routers along the way. The packet is sent in multiple directions such that it reaches all the members of the Multicast group. Multicast addresses are a special kind of IP addresses (class D), each identifying a multicast group. Stations join and leave multicast groups using IGMP. This is a control-plane protocol through which IP hosts register with their router to receive packets for certain multicast addresses.

IP multicast packets are transmitted on LANs in MAC multicast frames. Traditional LAN switches flood these multicast packets like broadcast packets to all stations in the VLAN. In order to avoid sending multicast packets where they are not required, multicast filtering functions can be added to the layer 2 switches. This is described in the IEEE standard 802.1D. Layer 2 switches capable of multicast filtering send the multicast packets only to ports connecting members of that multicast group. This is usually based on IGMP snooping.

The Avaya C460 includes multicast filtering support. The C460 learns which switch ports need to receive which multicast packets and configures the necessary information into the switch's hardware tables. This learning is based on IGMP (version 1 or 2) snooping. Using the learned information, IP multicast packets are forwarded only to ports connecting members of that multicast group.

The multicast filtering function in the C460 is transparent to the IP hosts and routers. It does not affect the forwarding behavior apart from filtering multicast packets from certain ports where they are not needed. To the ports that do get the multicast, forwarding is performed in the same way as if there was no filtering. The multicast packet will not be sent to any ports that would not receive it if there was no filtering.

The multicast filtering function operates per VLAN. A multicast packet arriving at the device on a certain VLAN is forwarded only to a subset of the ports of that VLAN. If VLAN tagging mode is used on the output port, then the multicast packet is tagged with the same VLAN number with which it arrived. This is interoperable with multicast routers that expect Layer 2 switching to be done independently for each VLAN.

IP Multicast Filtering configuration is associated with the setting up of three timers:

- The **Router Port Pruning** timer ages out Router port information if IGMP queries are not received within the configured time.
- The **Client Port Pruning** time is the time after the C460 switch reset that the filtering information is learned by the switch but not configured on the ports.

- The **Group Filtering Delay** time is the time that the switch should wait between becoming aware of a Multicast group on a certain VLAN and starting to filter traffic for this group.

IP Multicast CLI Commands

In order to...	Use the following command...
Enable or disable IP multicast filtering	set intelligent-multicast
Define aging time for client ports	set intelligent-multicast client port pruning time
Define aging time for router ports	set intelligent-multicast router port pruning time
Define group filtering time delays	set intelligent-multicast group-filtering delay time
Display the IP multicast filtering status	show intelligent-multicast

Broadcast Storm Control

Broadcast Storm Control Overview

This feature allows you to protect the network or switch from excessive Broadcast or Unknown traffic.

When the Broadcast Storm Control is enabled, the switch discards broadcast, multicast and unknown packets when the Broadcast Threshold Rate on a switch port exceeds a specified threshold. The Broadcast Threshold Rate is the number of broadcast packets received by a port per second.

When you enable Broadcast Storm Control, counters are set on all 10/100 Mbps ingress ports.

ⓘ Broadcast Storm Control is only supported on 10/100 Mbps I/O ports.

The C460 hardware includes separate counters for broadcast, multicast and unknown packets. When any of these counters crosses the specified threshold, the respective storm packets are dropped.

Broadcast Storm Control CLI Commands

In order to...	Use the following command...
Enable or disable broadcast storm control.	set broadcast storm control
Set the broadcast storm control threshold (in packets per second)	set broadcast storm control threshold
Display broadcast storm status and settings.	show broadcast storm control

Broadcast Storm Control Configuration Examples

This example shows configuration of broadcast storm control with a threshold of 100,000 pps.

```
C460-1(super)# set broadcast storm enable

Broadcast storm control enabled

C460-1(super)# set broadcast storm threshold 100000

Broadcast storm threshold was set

C460-1(super)# sh broadcast storm control
Broadcast        Threshold
Storm Control
---------------  ------------
enabled          100000
```

Priority Configuration

Overview

By its nature, network traffic varies greatly over time, so short-term peak loads might exceed the switch capacity. When this occurs, the switch must buffer frames until there is enough capacity to forward them to the appropriate ports.

This, however, can interrupt time-sensitive traffic streams, such as Voice and other converged applications. These packets need to be forwarded with the minimum of delay or buffering. In other words, they need to be given high priority over other types of network traffic.

Priority determines in which order packets are sent on the network and is a key part of QoS (Quality of Service).

The IEEE standard for priority on Ethernet networks is 802.1p.

Priority Queues

Avaya C460 switches supports two internal priority queues – the "High Priority" queue and the "Normal Priority" queue.

- Packets tagged with priorities 4-7 are mapped to the High Priority queue; packets tagged with priorities 0-3 are mapped to the Normal Priority queue. This classification is based either on the packet's original priority tag, or, if the packet arrives at the port untagged, based on the priority configured for the ingress port (set using the `set port level` CLI command).

In cases where the packet was received tagged, this priority tag is retained when the packet is transmitted through a tagging port.

In cases where the priority is assigned based on the ingress priority of the port, then on an egress tagging port the packet will carry either priority 0 or priority 4, depending on the queue it was assigned to (High Priority=4, Normal Priority=0).

Priority Configuration CLI Commands

In order to...	Use the following command...
Set the priority level of a port	set port level
Display priority settings and status for all ports	show port

PBNAC (Port-Based Network Access Control) – 802.1x

Port-Based Network Access Control (IEEE 802.1X) is a method for performing authentication to obtain access to IEEE 802 LANs. The protocol defines an interaction between three entities:

- Supplicant — an entity at one end of a point-to-point LAN segment that is being authenticated by an authenticator attached to the other end of that link.
- Authenticator — an entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link; in this case, the C460.
- Authentication (RADIUS) Server — an entity that provides an authentication service to an authenticator. This service determines, from the credentials provided by the supplicant, whether the supplicant is authorized to access the services provided by the authenticator.

The process begins with the supplicant trying to access a certain restricted network resource, and upon successful authentication by the authentication server, the supplicant is granted access to the network resources.

How "Port-Based" Authentication Works

802.1X provides a means of authenticating and authorizing users attached to a LAN port and of preventing access to that port in cases where the authentication process fails. The authentication procedure is port based, which means:

- access control is achieved by enforcing authentication on connected ports
- if an end-point station that connects to a port is not authorized, the port state is set to "unauthorized" which closes the port to any traffic.
- As a result of an authentication attempt, the C460 port can be either in a "blocked" or a "forwarding" state.

802.1X interacts with existing standards to perform its authentication operation. Specifically, it makes use of Extensible Authentication Protocol (EAP) messages encapsulated within Ethernet frames (EAPOL), and EAP over RADIUS for the communication between the Authenticator and the Authentication Server.

PBNAC Implementation in the C460 Switch

PBNAC is implemented in C460 over the 10/100Mbps ports only. The balance of this section lists the conditions that govern the implementation of the 802.1X standard in the C460:

- PBNAC is enabled over the 10/100 access ports only.
- PBNAC can work only if a RADIUS server is configured on the C460 and the RADIUS server is carefully configured to support 802.1X.
- PBNAC and port/intermodule redundancy can co-exist on the same ports.
- PBNAC and LAGs can coexist on the same ports.
- PBNAC and Spanning Tree can be simultaneously active on a module.

ⓘ If either PBNAC or STP/RSTP are in a blocking state, the final state of the port will be blocked.

- When PBNAC is activated, the application immediately places all ports in a blocking state unless they were declared “Force Authenticate”. They will be reverted to “Forwarding” state only when the port is authorized by the RADIUS server.

ⓘ The actual state of ports configured as “Force Authenticate” is determined by the STA.

Configuring the C460 for PBNAC

This section lists the basic tasks required to configure a C460 for PBNAC. In order to configure the C460 for PBNAC, do the following:

- Configure a RADIUS server on a network reachable from the C460:
  - — Create user names and passwords for allowed users.
  - — Make sure the EAP option is enabled on this server.
- Configure the C460 for RADIUS:
  - — Configure RADIUS parameters.
  - — Enable the RADIUS feature.
  - — Configure the port used to access the RADIUS server as “force-authorized.”

ⓘ You can configure on the RADIUS server a PVID, static VLAN binding and port level for each authenticated user. If the port that the user is connected to is authorized, those parameters will be assigned to the port.

- Connect the Supplicant – i.e., Windows XP or Windows 2000 clients – directly to the C460.
- Verify that the dot1x port-control is in auto mode.
- Set the dot1x system-auth-config to enable; the authentication process starts:
  - — The supplicant is asked to supply a user name and password.
  - — If authentication is enabled on the port, the Authenticator initiates authentication when the link is up.
  - — Authentication Succeeds: after the authentication process completes, the supplicant will receive a Permit/Deny notification.
  - — Authentication Fails: authentication will fail when the Supplicant fails to respond to requests from the Authenticator, when management controls prevent the port from being authorized, when the Supplicant issues an explicit EAPOL-Logoff request, when the link is down, or when the user supplied incorrect logon information.

PBNAC CLI Commands

The following table contains a list of the CLI commands for the PBNAC feature. The rules of syntax and output examples are all set out in detail in the *Avaya C460 Reference Guide*.

Table 4.2 PBNAC CLI Commands

In order to...	Use the following command...
Set the minimal idle time between authentication attempts	set dot1x quiet-period
Set the time interval between attempts to access the Authenticated Station	set dot1x tx-period
Set the server retransmission timeout period for all ports	set dot1x server-timeout
Set the authentication period (an idle time between re-authentication attempts)	set dot1x re-authperiod
Set the authenticator-to-supplicant retransmission timeout period (the time for the switch to wait for a reply from the Authenticated Station)	set dot1x supp-timeout
Set the max-req for all ports (the maximal number of times the port tries to retransmit requests to the Authenticated Station before the session is terminated)	set dot1x max-req
Globally enable 802.1x	set dot1x system-auth-control enable
Globally disable 802.1x	set dot1x system-auth-control disable
Set dot1x control parameter per port	set port dot1x port-control
Initialize port dot1x	set port dot1x initialize
Set the port to re-authenticate	set port dot1x re-authenticate

In order to...	Use the following command...
Set dot1x re-authentication mode per port	set port dot1x re-authentication
Set the 802.1x quiet period per port	set port dot1x quiet-period
Set the transmit period per port (a time interval between attempts to access the Authenticated Station)	set port dot1x tx-period
Set the supp-timeout per port (a time for the port to wait for a reply from the Authenticated Station)	set port dot1x supp-timeout
Set the server-timeout per port (a time to wait for a reply from the Authentication Server)	set port dot1x server-timeout
Set the re-authentication period per port (an idle time between re-authentication attempts)	set port dot1x re-authperiod
Set the max-req per port (the maximal number of times the port tries to retransmit requests to the Authenticated Station before the session is terminated)	set port dot1x max-req
Disable dot1x on all ports and return to default values	clear dot1x config
Display the system dot1x capabilities, protocol version, and timer values	show dot1x
Display all the configurable values associated with the authenticator port access entity (PAE) and backend authenticator	show port dot1x
Display all the port dot1x statistics	show port dot1x statistics

Multilayer Policy

Multilayer Policy is a set of features for enforcing QoS and Access Control policy on routed and switched packets. One of its major goals is supporting Differentiated Services for Avaya VoIP solutions.

About Multilayer Policy

Multilayer Policy is enforced on the 10/100 Mbps ports of a C460 switch. In general, Multilayer Policy consists of the following parts:

- Policy Lists — groupings of Access lists, DSCP-to-COS maps, and Trust mode attributes.
- Access Lists — ordered lists of classification rules applied to frames received and action pairs determining how they are to be handled.
- DSCP-to-COS Maps — mapping function that set the frame 802.1p priority according to its DSCP value.
- Trust Modes — policy-list attribute; either “untrusted,” “trust-COS,” or “trust-DSCP.”

Access Lists

Access Lists (ACL) are at the center of Multilayer Policy. Typically, users specify their classification demands by defining Access Lists. An Access List is an ordered list of classification rules and actions. For each frame received by the system, the Multilayer Policy application tries the classification rules – one-by-one – and executes the action associated with the first rule that matches.

Rules are based on the following properties:

- IP:IP version 4 packets with specific source and destination addresses (+ wildcards)
- IP version 4 packets with a specific protocol number – 0 to 255 – with specific source and destination addresses (+ wildcards).
- TCP:TCP/IPv4 packets with specific source and destination addresses (+ wildcards) and source and destination ports (+port ranges). The keyword “established” enables “permit” for TCP packets with “ack” flag set. For example, this will not allow matching packets that open TCP connections.
- UDP:UDP/IPv4 packets with specific source and destination addresses (+ wildcards) and source and destination ports (+ port ranges).

Actions supported include:

- permit – allows the packet through
- deny – drops the packet
- deny-and-notify – drops the packet and sends an SNMP trap
- fwd0, fwd1 .... fwd7 – assigns priority to the packet

DSCP-to-COS Maps

DSCP-to-COS maps set the frame 802.1p priority according to the DSCP priority value. For each DSCP value, the map contains a corresponding COS. The map changes the COS value for frames that match an active Access List rule with a "permit" action.

The following conditions apply to DSCP-to-COS maps:

- DSCP-to-COS maps are defined within the Policy Lists.
- Only packets that match an Access List rule with a "permit" action can be modified based on a DSCP-to-COS map.
- Actions supported per DSCP include: Fwd 0, Fwd1 ....Fwd7, Forward no change.

Trust Modes

The C460 supports the following Trust Mode values:

- "untrusted" — forwards the packet with 802.1p priority=0.
- "trust-cos" — forwards the packet with its original 802.1p priority (default).
- "trust-dscp" — forwards the packet with an 802.1p priority obtained from the DSCP-to-COS mapping table.

Multilayer Policy Implementation in the C460

Each C460 can store up to 20 Policy Lists. These lists consist of: Access Lists, DSCP-to-COS Maps, and Trust Modes.

The C460 supports two policy types:

- "Router" – the switch enforces the active Policy List only on routed packets. This applies to C460 switches in "Router" device mode.
- "All" – the switch enforces the active Policy List on all packets that enter through the Fast Ethernet ports. This applies to C460 switches in "Router" or "Layer2" device mode.
  "All" is the policy type available when the C460 is in device mode "Layer2."

There can be only one active Policy List per module with either policy type.

The following conditions apply to Policy Lists:

- Policy Lists can be defined in the "switch" context when the C460 is in "Layer2" device-mode or in the "router" context when the C460 is in "Router" device-mode.
- Policy Lists are shared by Layer 2 and Layer 3 applications.
- The maximum number of rules per L3 Access List is 9999 when the policy type is "Router". If the Policy List is to be applied to Layer 2 as well – policy type "all", the maximum number of rules per list is 254.

- TCP/UDP port ranges can only have sizes of 2^n, where the lower port of the range is aligned to the range number.
  - For example, for a range of 32 ports (2^5), the lower ports can have the value of 32, 64, 96, etc.
  - This limitation does not apply when the device is in "Router" policy type.
- Only L3 rules (based on Src/Dest IP address) will be enforced on IP fragments. Therefore, if an L4 rule is applicable to an IP fragment, the fragment will be dropped.
- The following rules are *not* supported for TCP/UDP port numbers:
  - "lower then"
  - "greater then"
- If a packet matches a rule with a "permit" action and subsequently a rule with "fwd…" action, the packet's priority will be changed to the one specified in the second rule, instead of being forwarded with the original priority as per "permit" action
  - This limitation is relevant only for Layer 2 policy (i.e., when the policy type is "all").

Configuring the C460 for Multilayer Policy

This section describes the configuration of the C460 for Multilayer Policy functionality.

Configuration Requirements

The following specific requirements impact on the configuration of Multilayer Policy in an Avaya C460:

- If the device mode is "Layer 2," the policy commands will appear in the L2 CLI tree; if the device mode is "Router," the commands will appear in the L3 CLI tree.
- Policy List validation will be performed during list activation.
- A CLI command for policy simulation is available.

Configuration File Management

The following specific requirements impact on the management of the Multilayer Policy configuration file:

- Unlike other Layer 2 settings, the Layer 2 policy is not automatically saved in NVRAM. In order to save the Layer 2 or Layer 3 policy configuration , the user must copy the running configuration to the startup configuration file. To do this, use the command `copy running-config startup-config`.

Multilayer Policy CLI Commands

The following table contains a list of the CLI commands for the Multilayer Policy feature. The rules of syntax and output examples are all set out in detail in the *Avaya C460 Reference Guide*.

Table 4.3 Multilayer Policy CLI Commands

Display the active policy list number	show ip access-group
Display a summary of policy lists	show ip access-list-summary

Chapter 5

PoE (Power over Ethernet) Features

Introduction

The C460 switch provides "Inline" DC power over the signal pairs in addition to switched Ethernet on the existing LAN infrastructure for devices such as IP telephones and Wireless LAN access points. This allows you to deploy devices in the network that require power without installing standard power cables in hard to access areas. The C460 provides power over standard Category 3 and Category 5 cables.

The C460 is designed to comply to the specification of the latest draft of the IEEE 802.3af. Please refer to the Avaya Web site, www.avaya.com, for the updates.

Load Detection

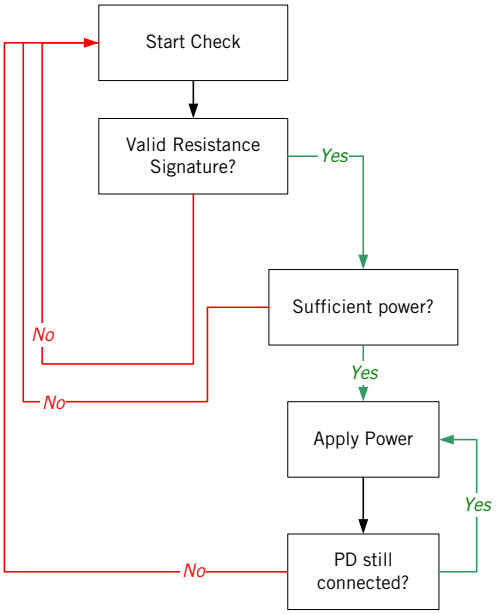
The C460 periodically checks all ports, powered and non-powered to check their status and the power status of connected devices.

The C460 will supply power to a port only after it has detected a suitable PD (powered device) is connected to the port. The check consists of the C460 looking for a signature from the device that indicates it needs to supply power.

How the C460 Detects a Powered Device

The C460 uses specific resistance between the power feed pairs and PD connection verification to determine whether to supply power to a give port. Figure 5.1 shows the process.

Figure 5.1 Powered Device Detection



Specific Resistance Signature (IEEE 802.3af)

The C460 PoE IO module applies a low voltage to the power feed pairs and measuring the current. A resistance of 19kΩ to 26.5kΩ is considered valid: if a valid signature is detected, power is supplied to the port.

PD Connected

Once power is provided to a port, it is checked periodically to see if a PD is still connected. If a PD is disconnected from a powered port, then power is denied to the port.

"Plug and Play" Operation

You can add and remove powered devices without manually reconfiguring the switch, since it performs a periodic automatic load detection scan on non-powered ports.

- If a powered device that fits the above criteria is detected on a non-powered port, then power is applied to the port.
- If a powered device is removed from a port, then power is denied to that port. The disconnected port is then scanned as well.

Powering Devices

Each port can supply up to 15.4 W by default.

Priority

Since the internal power supply may not be capable of driving powered devices on all the ports simultaneously, Avaya has implemented a priority mechanism.

This mechanism determines the order in which ports are powered after the switch is booted and powered down if the power resources of the switch are exhausted.

There are three user-configurable priority levels:

- Low
- High
- Critical

The default value is “Low” for all ports.

Power will automatically be restored to PDs according to their priority when the power budget increases. If the power budget is exceeded, power will not be provided to a new PD when you attach it, even if you define its priority as “High” or “Critical.”

PoE Power Calculation

Table 5.1 shows PoE power consumption for powered devices with different power requirements (5 W, 10 W and 15 W.

Assumptions

- The PSUs work in “no redundancy” mode.
- If mode is set to “redundant”, only two PSU are considered as available, while the 3rd PSU power is reserved for the case of PSU failure
- Chassis components power consumption:
  - SPV 1 – 68W
  - SPV 2 – 68W
  - Fans – 45W
  - Modules – 48 PoE Ports – 48W
- 1000 W Total power per PSU (in load-sharing mode)
  - up to 400 W main power
  - plus up to 800 W PoE power

Table 5.1 Powered Device Power Consumption

Number of modules	Number of PSUs (Total Power)						Watts per port
	1 (1000 W)		2 (2000 W)		3 (3000 W)		
	Main 400 W	PoE 800 W	Main 800 W	PoE 1600 W	Main 1200 W	PoE 2400 W	
1	229	48 (240 W) 48 (480 W) 48 (720 W)	229	48 (240 W) 48 (480 W) 48 (720 W)	229	48 (240 W) 48 (480 W) 48 (720 W)	5 10 15
2	277	96 (480 W) 72 (720 W) 48 (720 W)	277	96 (480 W) 96 (960 W) 96 (1440 W)	277	96 (480 W) 96 (960 W) 96 (1440 W)	5 10 15
3	325	135 (675 W) 67 (670 W) 45 (675 W)	325	144 (720 W) 144 (1440 W) 106 (1590 W)	325	144 (720 W) 144 (1440 W) 144 (2160 W)	5 10 15
4	373	125 (625 W) 62 (620 W) 41 (615 W)	373	192 (960 W) 160 (1600 W) 106 (1590 W)	373	192 (960 W) 192 (1920 W) 160 (2400 W)	5 10 15

ⓘ Refer to “Power Requirements” on page 83 for power requirements for C460 components.

PoE Configuration

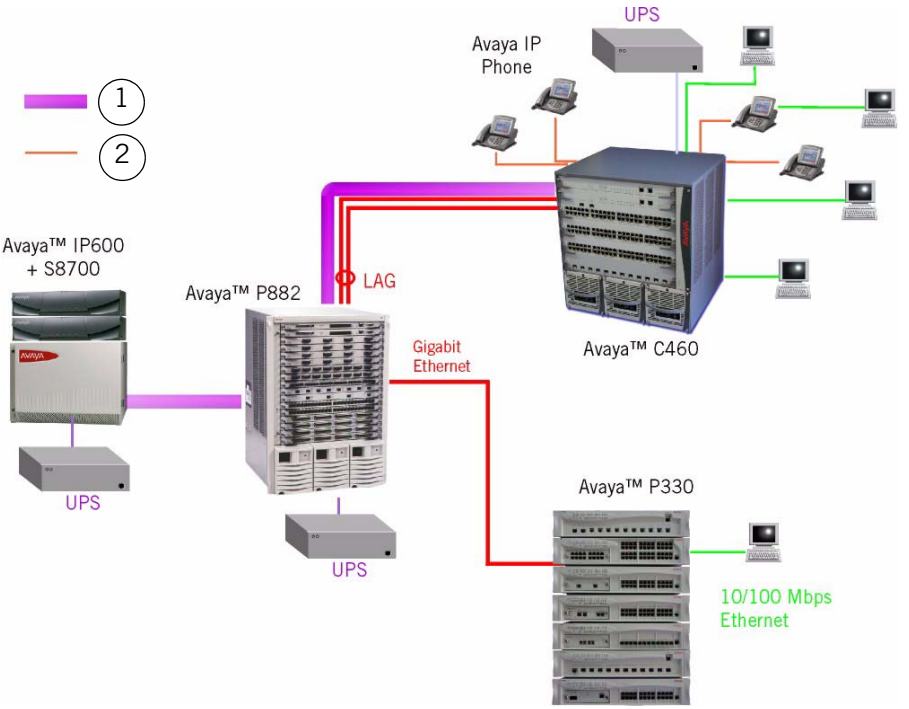
If the PoE module is removed and replaced with module of the same type, the port power configuration of this module is retained

- When PoE module is removed and replaced with module of another type, the port power configuration will be configured with default values
  - — This refers to parameters set by the `set port powerinline` and `set port powerinline priority` CLI commands
  - — Parameters set by the `set slot power admin` and `set slot power priority` CLI commands are NOT set to defaults even when the module type is changed

Power over Ethernet in Converged Networks

Figure 5.2 shows the C460 as part of an ultra-reliable Avaya network. It provides power to IP telephones, wireless network access devices and Web cameras.

Figure 5.2 Power over Ethernet Application



Key

1 Fully reliable path for telephony applications

2 Power over Ethernet

Both the data and power paths from the Avaya P333T-PWR to the PBX are backed-up. Using LAGs for data with UPSs (Uninterruptible Power Supplies) for power ensures non-stop IP communications.

PoE Configuration CLI Commands

In order to...	Use the following command...
Enable or disable the load detection process on the port	set port powerinline
Set the priority level for powering the port.	set port powerinline priority
Recalculate and reapply the PoE budget.	set powerinline budget
Display the port powerinline configuration	show powerinline
Display the PoE budget distribution for modules in the switch.	show powerinline budget
Display the current power configuration for the switch	show environment power

Chapter 6

Avaya C460 Layer 3 Features

Introduction

What is Routing?

Routing allows transfer of a data packet from source to destination by a device called a router. Routing involves two basic activities: determination of optimal routing paths and transmission of information packets through an internetwork.

Routers use routing tables to determine the routes to particular network destinations and, in some cases, metrics associated with those routes. Routers communicate with one another, and maintain their routing tables through the transmission of a variety of messages. Routers can only route a message that is transmitted by a routable protocol such as IP or IPX. Messages in non-routable protocols, such as NetBIOS and LAT, cannot be routed, but they can be transferred from LAN to LAN by a bridge.

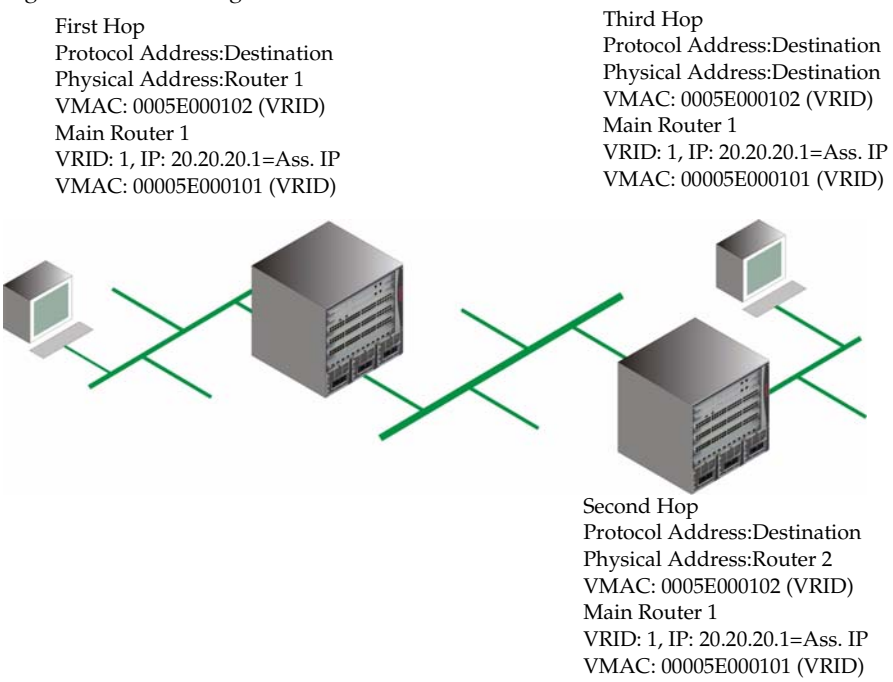
The Routing Update Message is one such message. Routing Updates usually consist of all or a portion of a routing table. By analyzing Routing Updates from all routers, a router can build a detailed picture of network topology.

A Link-State Advertisement is another example of a message sent between routers. Link-State Advertisements inform other routers of the state of the sender's links. Link information can also be used to build a complete picture of the network's topology. Once the network topology is understood, routers can determine optimal routes to network destinations.

When a router receives a packet, it examines the packet's destination protocol address. The router then determines whether it knows how to forward the packet to the next hop. If the router does not know how to forward the packet, it usually drops the packet unless a default gateway is defined. If the router knows how to forward the packet, it changes the packet destination’s physical address to that of the next hop and transmits the packet.

The next hop might not be the ultimate destination host. If not, the next hop is usually another router, which executes the same switching decision process. While the packet moves through the internetwork, its physical address changes but its protocol address remains constant. This process is shown in Figure 6.1.

Figure 6.1 Routing



The routers obtain the relation between the destination host's protocol address and its physical address using the ARP request/reply mechanism.The information is stored within the ARP table in the router. See "The ARP Table" on page 71.

Within an enterprise, routers serve as an internet backbone interconnecting all networks. This architecture strings several routers together by a high-speed LAN topology such as Fast Ethernet or Gigabit Ethernet. Within the global Internet, routers do all the packet switching in the backbones.

Another approach within an enterprise is the collapsed backbone. This uses a single router with a high-speed backplane to connect the subnetworks, making network management simpler and improving performance.

Routing Configuration

Forwarding

The C460 forwards IP packets between IP networks. When it receives an IP packet through one of its interfaces, it forwards the packet through one of its interfaces. The C460 supports multinetting. This allows it to forward packets between IP subnetworks on the same VLAN and between different VLANs. Forwarding is performed through standard means in Router mode.

Multinetting (Multiple Subnetworks per VLAN)

In Router Mode, most applications such as RIP and OSPF, operate per IP interface. Other applications such as VRRP and DHCP/BOOTP Relay operate per VLAN. Configuration of these applications is done in the Interface mode. When there is only a single interface (subnetwork) per VLAN then system behavior is intuitive since a subnet and a VLAN are the same.

If the configuration includes multiple interfaces (subnetworks) per VLAN things start to become complicated.

For example, if there are two interfaces over the same VLAN and you configure DHCP server on one interface, the DHCP server will be used also for the second interface over the same VLAN. This behavior might be less expected and in some cases wrong.

The C460 prevents configuration of VLAN-oriented commands on an interface unless the user explicitly enables it, using the `enable vlan commands` CLI command. This stops misconfiguration and unexpected results.

If there is only one interface over a VLAN, you can configure this VLAN through the single interface without the need to issue the `enable vlan commands` command.

ⓘ 1. When you issue VLAN-oriented commands, the commands affect the VLAN of the interface that was used at the time the you issued the command.
2. If the you move the interface is moved to another VLAN with the `ip vlan/ ip vlan name` CLI command, VLAN oriented configuration still applies to the original VLAN.

IP Configuration

IP Configuration CLI Commands

In order to...	Use the following command...
Enable IP routing	ip routing
Set ICMP error messages	ip icmp-errors
Specify the format of netmasks in the show command output	ip netmask-format
Create an interface or enter the Interface Configuration Mode	interface
Assign an IP address and mask to an interface	ip address
Set the administrative state of an IP interface	ip admin-state
Update the interface broadcast address	ip broadcast-address
Define a default gateway (router)	ip default-gateway
Define the interface RIP route metric value	default-metric
Enable net-directed broadcast forwarding	ip directed-broadcast
Set the IP routing mode of the interface	ip routing-mode
Enable or disable the sending of redirect messages on the interface	ip redirects
Check host reachability and network connectivity	ping
Use this command when there is more than one interface on the same VLAN	enable vlan commands
Trace route utility	traceroute

In order to...	Use the following command...
Create a router Layer 2 interface	set vlan (Layer 3)
Specify the VLAN on which an IP interface resides	ip vlan/ip vlan name
Display information about the IP unicast routing table	show ip route (Layer 3)
Display information for an IP interface	show ip interface
Display the status of ICMP error messages	show ip icmp

Basic Router Configuration

ⓘ You need to install the Layer 3 license before you can configure Layer 3 parameters.

The following example shows configuration of a basic IP interface and the routing protocol over this interface. It is not intended to provide comprehensive configuration information.

The example shows the following steps:

- Entering router mode
- Configuring a VLAN for a specific interface
- Enabling the required protocol

1 Enter Router mode:

```
C460-1(super)# set device-mode router
```

ⓘ Changing the device mode requires a switch reset.

2 Wait for the switch to restart and for the CLI prompt to reappear.

3 Use the `session` command to switch to the router entity:

```
C460-1(super)# session router
Router-1(super)#
```

4 Configure a VLAN for the specific IP interface Marketing:

```
Router-1(super)# set vlan 100 name vlan#100
Router-1(super)#
```

5 Define an interface called Marketing:

```
Router-1(super)# interface Marketing
Router-1(configure-if:marketing) #
```

6 Assign an IP address and network mask:

```
Router-1(marketing) # ip address 149.49.37.1 255.255.255.0
Router-1(configure)#
```

7 Assign a VLAN:

```
Router-1(configure-if:marketing) # ip vlan 100
Router-1(configure-if:marketing) #
```

8 Exit interface mode:

```
Router-1(configure-if:marketing) # Exit
Router-1(super)#
```

9 Display the settings:

```
Router-1(super)# sh ip interface
Showing 1 Interface
Marketing is administratively up
On vlan vlan#100
Internet address is 149.49.37.1  subnet mask is 255.255.255.0
Broadcast address is 149.49.37.255
Directed broadcast forwarding is disabled
Proxy ARP is disabled
Router-1(configure)#
Router-1(configure)#
```

10 Enable the required protocols:

```
C460-1(super)# router rip
Router-1 (configure router:rip) # network 149.49.37.0
```

or

```
C460-1(super)# router ospf
Router-1 (configure router:rip) # network 149.49.37.0
```

11 Start the operation to copy the running configuration to the startup configuration:

ⓘ This is necessary to retain the configuration after a reset

```
Router-1(configure)# copy running-config startup-config
```

RIP (Routing Interchange Protocol) Configuration

RIP Overview

RIP is one of the two main groups of routing protocols. The other group is OSPF (refer to "OSPF Overview" on page 65 for details). It is a "distance vector protocol" – the router decides which path to use on distance or the number of intermediate hops. In order for this protocol to work correctly, all the routers – and possibly the nodes – need to gather information on how to reach each destination in the Internet. The very simplicity of RIP has a disadvantage however: this protocol does not take into account he network bandwidth, physical cost, data priority, and so on.

The C460 supports the widely used RIP routing protocol – both RIPv1 and RIPv2. The RIPv1 protocol imposes some limitations on the network design with regard to subnetting. When operating RIPv1, you must not configure variable length subnetwork masks (VLMS). Each IP network must have a single mask, implying that all subnetworks in a given IP network are of the same size. Also, when operating RIPv1, you must not configure supernets. These are networks with a mask smaller than the natural net mask of the address class, such as 192.1.0.0 with mask 255.255.0.0, smaller than the natural class C mask which is 255.255.255.0. For detailed descriptions of RIP refer to the standards and published literature.

RIPv2 is a new version of the RIP routing protocol but with some advantages over RIPv1. RIPv2 solves some of the problems associated with RIPv1. The most important change in RIPv2 is the addition of a subnetwork mask field which allows RIPv2 to support variable length subnetworks. RIPv2 also includes an authentication mechanism similar to the one used in OSPF.

Configuration of the RIP version, 1 or 2, is per IP interface. Configuration must be homogenous on all routers on each subnetwork, that is, there should not be both RIPv1 and RIPv2 routers on the same subnetwork. However, you can configure different IP interfaces of the C460 with different RIP versions. This configuration is valid as long as all routers on the subnet are configured to the same version.

RIPv2 and RIPv1 are considered the same protocol with regard to redistribution to/from OSPF and static route preferences.

The Avaya C460 supports both RIPv1 and RIPv2 in Router mode.

RIP2

RIP2 overcomes some of the shortcomings of RIP. Table 6.2 summarizes the differences between RIP and RIP2.

Table 6.2 Differences Between RIP and RIP2

RIP2	RIP
Multicast addressing	Broadcast Addressing
Event-driven	Timer-based – update every 30 seconds
VLSM support – subnet information transmitted	Fixed subnetwork masks
Security (authentication)	No security
Provision for EGP/BGP (Route tag)	No provision for external protocols

RIP CLI Commands

In order to...	Use the following command...
Configure the Routing Information Protocol (RIP)	router rip
Specify a list of networks on which the RIP is running	network (OSPF)
Redistribute routing information from other protocols into RIP	redistribute (RIP)
Specify the RIP version running on the interface basis	ip rip rip-version
Set the interface RIP route metric value	default-metric (RIP)
Set the RIP Send and Receive mode on an interface	ip rip send-receive-mode
Enable learning of the default route received by the RIP	ip rip default-route-mode
Enable split-horizon with poison-reverse on an interface	ip rip poison-reverse

In order to...	Use the following command...
Enable split-horizon mechanism	ip rip split-horizon
Specify the type of authentication used in RIP Version 2 packets	ip rip authentication mode
Set the authentication string used on the interface	ip rip authentication key
Specify the RIP timers values	timers basic

OSPF (Open Shortest Path First) Configuration

OSPF Overview

OSPF is a routing protocol developed for IP networks based on the shortest path first or link-state algorithm. It was introduced to overcome the limitations of RIP in increasingly complex network designs.

OSPF is based on the cost of a particular path. In contrast, RIP uses hops as a path criterion. Also, updates are sent on a "need to know" basis rather than every 30 seconds as with RIP.

The advantage of shortest path first algorithms is that they results in smaller more frequent updates everywhere. They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity, when routers continuously increment the hop count to a particular network. These algorithms make a stable network.

The disadvantage of shortest path first algorithms is that they require a lot of CPU power and memory.

Routers use link-state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node. This calculation is based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links, and it also sends the complete routing structure (topography).

The C460 supports the OSPF routing protocol. You can configure the C460 as an OSPF ASBR (Autonomous System Boundary Router) by route redistribution. The C460 can be installed in the OSPF backbone area – area 0.0.0.0 – or in any OSPF area that is part of a multiple areas network. However, the C460 cannot be configured to be an OSPF area border router itself.

The C460 supports the ECMP (equal-cost multipath) feature which allows load balancing by splitting traffic between several equivalent paths.

While you can activate OSPF with default values for each interface using a single command, you can configure many of the OSPF parameters.

For a detailed description of OSPF, see the OSPF standards and published literature.

OSPF CLI Commands

In order to...	Use the following command...
Enable OSPF protocol	router ospf
Configure the area ID of the router	area

In order to...	Use the following command...
Configure router identity	ip ospf router-id
Redistribute routing information from other protocols into OSPF	redistribute (RIP)
Configure the delay between runs of OSPF's SPF calculation	timers ospf
Configure interface metric	ip ospf cost
Specify the time interval between hellos the router sends	ip ospf hello-interval
Configure the interval before declaring the neighbor as dead.	ip ospf dead-interval
Configure interface priority used in DR election	ip ospf priority
Configure the interface authentication password	ip ospf authentication-key
Display general information about OSPF routing	show ip ospf
Display the OSPF-related interface information	show ip ospf interface
Display OSPF neighbor information on a per-interface basis	show ip ospf neighbor
Display lists of information related to the OSPF database for a specific router	show ip ospf interface

Static Routing Configuration

Static Routing Overview

When dynamic routing protocols – RIP or OSPF – are not appropriate, you can manually configure *static routes* to indicate the next hop on the path to the final packet destination.

A static route becomes inactive if the interface over which the route is defined is disabled. When the interface is enabled, the static route becomes active again. They are never timed-out, or lost over reboot, and can only be removed by manual configuration. Deletion by configuration of the IP interface deletes the static routes using this interface as well.

Static routes can only be configured for remote destinations, i.e. destinations that are reachable through another router as a next hop. The next hop router must belong to one of the directly attached networks for which the C460 has an IP interface. “Local” static routes, such as those that have no next hop, are not allowed.

You can configure two types of static routes:

- High Preference static routes which are preferred to routes learned from any routing protocol
- Low Preference static routes which are used temporarily until the route is learned from a routing protocol. By default, a static route has Low Preference.

Static routes can be advertised by the RIP and OSPF routing protocols, as described under Route redistribution.

Static routes also support load-balancing similar to OSPF. You can configure a static route with multiple next hops so traffic is split between these next hops.

This can be used, for example, to load-balance traffic between several firewalls which serve as the default gateway.

Static Routing Configuration CLI Commands

In order to...	Use the following command...
Establish a static route	ip route
Remove a static route	no ip route
This command exists for compatibility with P550	ip max-route-entries
Set the maximum number of route entries in the routing table to the default value	no ip max-route-entries

In order to...	Use the following command...
Define a default gateway (router)	ip default-gateway
Remove the default gateway (router)	no ip default-gateway
Delete all the dynamic routing entries from the Routing Table	clear ip route (Layer 3)
Display information about the IP unicast routing table	show ip route (Layer 3)
Display a routing table for a destination address	show ip route best-match
Display the static routes	show ip route static
Display the number of routes known to the switch	show ip route summary

Route Preferences

The routing table can contain routes from different sources. Routes to a certain destination can be learned independently from RIP and from OSPF. At the same time, a static route can also be configured to the same destination. While metrics are used to choose between routes of the same protocol, protocol preferences are used to choose between routes of different protocols.

The preferences only apply to routes for the same destination IP address and mask. They do not override the longest-match selection. For example, a high-preference static default route will not be preferred over a RIP route to the subnetwork of the destination.

The following list shows C460 protocol preferences from the most to the least preferred:

1 Local (directly attached network)
2 High-preference static (manually configured routes)
3 OSPF internal routes
4 RIP
5 OSPF external routes
6 Low-preference static (manually configured routes).

Route Redistribution

Route redistribution is the interaction of multiple routing protocols. OSPF and RIP can be operated concurrently in the C460. In this case, you can configure the C460 to redistribute routes learned from one protocol into the domain of the other routing protocol. Similarly, static routes can be redistributed to RIP and OSPF. Take care when you configure Route redistribution. It involves metric changes and might cause routing loops in the presence of other routes with incompatible schemes for route redistribution and route preferences.

The C460 scheme for metric translation in route redistribution is as follows:

- Static to RIP metric configurable (default 1)
- OSPF internal metric N to RIP metric 1
- OSPF external type 1 metric N to RIP metric 1
- OSPF external type 2 metric N to RIP metric N+1
- Static to OSPF external type 2, metric configurable (default 1)
- RIP metric N to OSPF external type 2, metric N
- Direct to OSPF external type 2, metric 1.

By default, the C460 does not redistribute routes between OSPF and RIP. Redistribution from one protocol to the other can be configured. Static routes are, by default, redistributed to RIP and OSPF. the C460 allows the user to globally disable redistribution of static routes to RIP, and separately to globally disable redistribution of static routes to OSPF. In addition you can configure, on a per static route basis, whether the route is to be redistributed to RIP and OSPF, and what metric (in the range of 1-15). The default state is to allow the route to be redistributed at metric 1. When static routes are redistributed to OSPF, they are always redistributed as external type 2.

Route Redistribution Commands

In order to...	Use the following command...
Redistribute routing information from other protocols	redistribute (RIP)

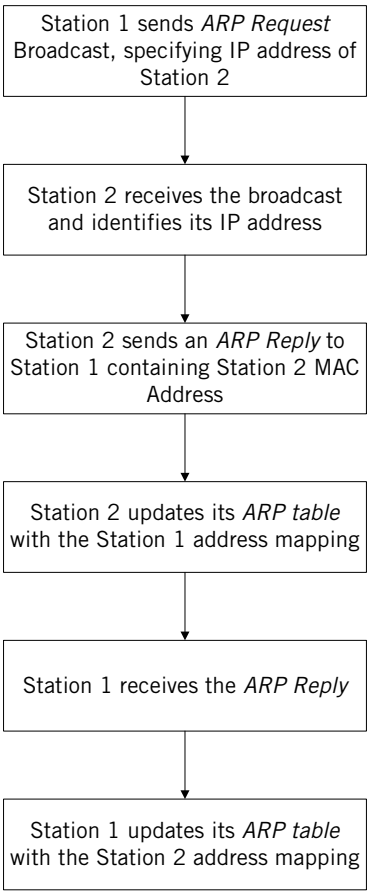
ARP (Address Resolution Protocol) Table Configuration

ARP Overview

IP logical network addresses are independent of physical addresses. The physical address must be used to convey data in the form of a frame from one device to another. Therefore, a mechanism is required to acquire a destination device hardware address from its IP address. This mechanism is called ARP (Address Resolution Protocol).

The following mechanism describes how a station builds an ARP table:

Figure 6.3 Building an ARP Table



The ARP Table

The ARP table stores recently used pairs of IP/MAC addresses. This storage saves time and communication costs, since the host looks in the ARP cache first when transmitting a packet. If the information is not there, then the host sends an ARP Request. See Figure 6.3.

ARP CLI Commands

In order to...	Use the following command...
Add a permanent entry to the ARP cache	arp
Configure the amount of time that an entry remains in the ARP cache	arp timeout
This command exists for compatibility with P550	ip max-arp-entries
Enable or disable proxy ARP on an interface	ip proxy-arp
Delete all dynamic entries from the ARP cache and the IP route cache	clear arp-cache
Display the ARP cache	show ip arp
Display the IP address of a host, based on a known MAC address	show ip reverse-arp

BOOTP/DHCP (Dynamic Host Configuration Protocol) Relay Configuration

BOOTP/DHCP Overview

BOOTP

Short for Bootstrap Protocol, BootP is an Internet protocol that allows a diskless workstation to discover the following:

- Its own IP address
- The IP address of a BOOTP server on the network
- A file to be loaded into memory to boot the workstation.

BOOTP allows the workstation to boot without requiring a hard disk or diskette drive. It is used when the user/station location changes frequently.

The protocol is defined by RFC 951.

DHCP

Short for Dynamic Host Configuration Protocol, DHCP assigns dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address whenever the device connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means you can add a new computer to a network without the hassle of manually assigning a unique IP address. Many ISPs use dynamic IP addressing for dial-up users. However, dynamic addressing may not be desirable for a network server.

DHCP/BOOTP Relay

The C460 supports the DHCP/BOOTP Relay Agent function. This is an application that accepts DHCP/BOOTP requests that are broadcast on one VLAN. The application sends them to a DHCP/BOOTP server. That server connects to another VLAN or a server that might be located across one or more routers that might otherwise not get the broadcast request. The relay agent handles the DHCP/BOOTP replies as well. The relay agent transmits the replies to the client directly or as broadcast, according to a flag in the reply message. Note that the same DHCP/BOOTP relay agent serves both the BOOTP and DHCP protocols.

When there is more than one IP interface on a VLAN, the C460 chooses one of the IP addresses on this VLAN when relaying the DHCP/BOOTP request. The DHCP/BOOTP server then uses this address to decide from which subnetwork to allocate the address.

When the DHCP/BOOTP server is configured to allocate addresses only from a single subnetwork among the different subnetworks defined on the VLAN, you might need to configure the C460 with the relay address on that subnet so the DHCP/BOOTP server can accept the request.

DHCP/BOOTP Relay in C460 is configurable per VLAN and allows for two DHCP/BOOTP servers to be specified. In this case, the C460 duplicates each request, and sends it to both servers. This duplication provides redundancy and prevents the failure of a single server from blocking hosts from loading.

You can enable or disable or DHCP/BOOTP Relay in C460.

BOOTP/DHCP CLI Commands

In order to...	Use the following command...
Enable or disable relaying of bootp and dhcp requests to the BOOTP/DHCP server	ip bootp-dhcp relay
Add or remove a BOOTP/DHCP server to handle BOOTP/DHCP requests received by this interface	ip bootp-dhcp server
Select the network from which the bootp/dhcp server allocates an address	ip bootp-dhcp network

NetBIOS Re-broadcast Configuration

NetBIOS Overview

Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities.

The Avaya C460 can be configured to relay netbios UDP broadcast packets. This feature is used for applications such as WINS that use broadcast but might need to communicate with stations on other subnetworks or VLANs.

Configuration is performed on a per-interface basis. A netbios broadcast packet arrives from an interface on which netbios rebroadcast is enabled. The packet is distributed to all other interfaces configured to rebroadcast netbios.

If the netbios packet is a net-directed broadcast, for example, 149.49.255.255, the packet is relayed to all other interfaces on the list, and the IP destination of the packet is replaced by the appropriate interface broadcast address.

If the netbios broadcast packet is a limited broadcast, for example, 255.255.255.255, it is relayed to all VLANs on which there are netbios-enabled interfaces. In that case, the destination IP address remains the limited broadcast address.

NetBIOS Re-broadcast Configuration CLI Commands

In order to...	Use the following command...
Set NetBIOS rebroadcasts mode on an interface	ip netbios-rebroadcast
Disable NetBIOS rebroadcasts mode on an interface	no ip netbios-rebroadcast

VRRP (Virtual Router Redundancy Protocol) Configuration

VRRP Overview

VRRP is an IETF protocol designed to support redundancy of routers on the LAN, and load balancing of traffic. VRRP is transparent to host stations, making it an ideal option when redundancy, load balancing and ease of configuration are all required.

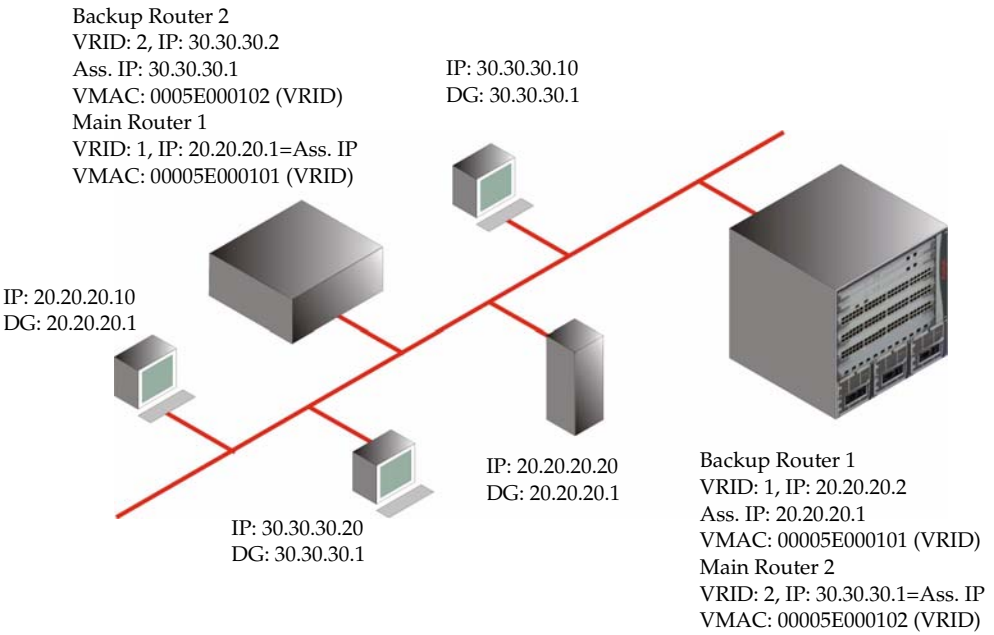
The concept underlying VRRP is that a router can backup other routers, in addition to performing its primary routing functions. This redundancy is achieved by introducing the concept of a virtual router. A virtual router is a routing entity associated with multiple physical routers. One of the physical routers with which virtual router is associated preforms the routing functions. This router is known as the master router. For each virtual router, VRRP selects a master router. If the selected master router fails, another router is selected as master router.

In VRRP, two or more physical routers can be associated with a virtual router, thus achieving extreme reliability. In a VRRP environment, host stations interact with the virtual router. The stations are not aware that this router is a virtual router, and are not affected when a new router takes over the role of master router. Thus VRRP fully interoperable with any host station.

You can activate VRRP on an interface using a single command while allowing for the necessary fine-tuning of the many VRRP parameters. For a detailed description of VRRP, see VRRP standards and published literature.

VRRP Configuration Example 1

Figure 6.4 VRRP Configuration Example



Case#1

One main router on IP subnet 20.20.20.0, such as a P333R, C460 or any router that supports VRRP, and a redundant router. You can configure more backup routers.

- The C460 itself must have an interface on the IP subnetwork, for example, 20.20.20.2
- Configure all the routers under the same VRID, for example, 1
  You must configure the routers per VLAN.
- This VRID must not be used in the network, even in a different VLAN
- By the end of the routers configuration, and when the network is up, the main router for each virtual router will be elected according to this order of preference:
  - The virtual router IP address is also the router's interface IP address
  - It has the highest priority (you can configure this parameter)
  - It has the highest IP address if the previous cases do not apply
- The virtual router IP address needs to be configured as Default Gateway on the stations

- The Main router advertises a six-byte Virtual MAC address in the format 00.00.5E.00.01.VRID as a response to the stations ARP requests.
- In the meantime, the redundant router will use a VRRP polling protocol to check the Main router integrity at one second intervals (default). Otherwise, it is idle
- If the Main router fails, the redundant router that does not receive a response from four consecutive polling requests (default) will take over and start to advertise the same Virtual MAC for the ARP requests. Therefore the stations will not 'sense' any change neither in the configured DG nor in the MAC level
- VRRP has no provisions for routing database synchronization among the
- redundant routers. You need to perform this manually if needed.

Case #2

- One router is Main on one IP subnetwork, for example, 20.20.20.0, and redundant on another, for example, 30.30.30.0.
- In this case each IP subnetwork must be in different VRID, for example, 1 & 2
- This detailed information is valid for each router in its Main or Redundant roles

VRRP CLI Commands

In order to...	Use the following command...
Enable or disable VRRP routing globally	router vrrp
Create or delete a virtual router on the interface	ip vrrp
Assign or remove an IP address to the virtual router	ip vrrp address
Set the virtual router advertisement timer value (in seconds) for the virtual router ID	ip vrrp timer
Set the virtual router priority value used when selecting a master route	ip vrrp priority
Set or disable the virtual router simple password authentication for the virtual router ID.	ip vrrp auth-key

In order to...	Use the following command...
Configure or disable the router to pre-empt a lower priority master for the virtual router ID	ip vrrp preempt
Set the primary address used as the source address of VRRP packets for the virtual router ID	ip vrrp primary
Accept or discard packets addressed to the IP address(es) associated with the virtual router, such as ICMP, SNMP, and TELNET. Use this command if the virtual router is not the IP address owner)	ip vrrp override addr owner
Display VRRP information	show ip vrrp
Display full VRRP-related information	show ip vrrp detail

Policy Configuration

Policy Configuration Overview

The C460 supports QoS (Quality of Service) by using multiple priority levels and IEEE 802.1p priority tagging. This QoS ensures that data and voice receive the necessary levels of service.

The Avaya C460 can enforce QoS policy on routed packets and change their 802.1p priority, according to the following criteria:

- The packet protocol
- Matching the packet's source or destination IP address to the configured priority policy.
- Whether the packet source or destination TCP/UDP port number falls within a pre-defined range.

In addition, the 802.1p priority of a packet can be modified according to the DSCP value in the IP header. This value is based on the DSCP-802.1p mapping configured by the user.

The C460 supports Access Control policy. Access Control rules define how the C460 handles routed packets. There are three possible ways to handle such packets:

- Forward the packet (Permit operation)
- Discard the packet (Deny operation)
- Discard the packet and notify the management station (Deny and Notify)

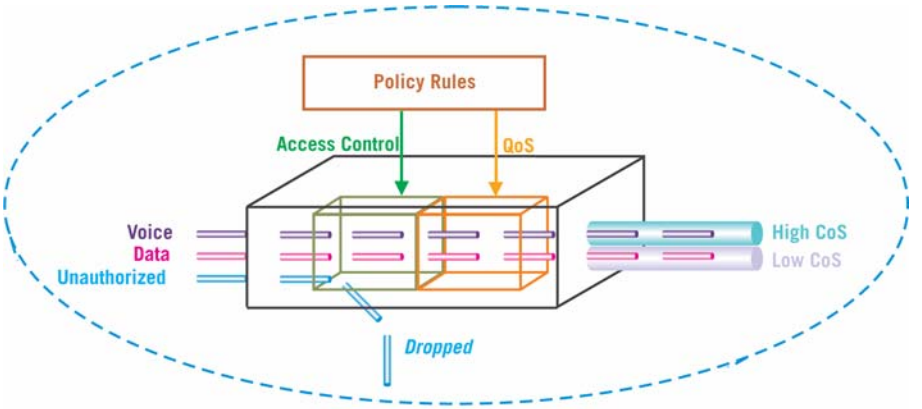
The Avaya C460 can enforce Access Control policy on each routed packet, according to the following criteria:

- Matching the packet's source or destination IP address to the configured Access Control policy.
- Determine if the packet protocol and source or destination TCP/UDP port number falls within a pre-defined range.
- Using the ACK bit of the TCP header.

The C460 uses policy lists containing both Access Control rules and QoS rules. The policy lists are ordered by rule indexing.

You can configure the Avaya C460 access control rules with the Command Line Interface and the Avaya QoS Manager central policy management application under Avaya™ MSNM.

Figure 6.5 Avaya C460 Policy



Policy Configuration CLI Commands

In order to...	Use the following command...
Activate a specific policy list	ip access-group
Deactivate a specific policy list	no ip access-group
Set the default action for a specific policy list	ip access-default-action
Set a name for a policy list	ip access-list-name
Set the owner for a specific policy list	ip access-list-owner
Create a specific policy rule	ip access-list
Delete a specific policy rule	no ip access-list
Check the policy for a simulated packet	ip simulate
Set the list cookie for a specific policy list	ip access-list-cookie
Copy a configured source policy list to a destination policy list	ip access-list-copy
Verify that all the rules in a priority list are valid	validate-group

In order to...	Use the following command...
Display information about the configured active access list.	show ip access-group
Display all the current policy lists	show ip access-lists

Policy Configuration Example

The following shows configuration of Access List 100

1 Assigning priority 6 to all TCP traffic originating in network 149.49.0.0 – rule 1:

```
C460-1(super)# ip access-list 100 1 fwd6 tcp 149.49.0.0
0.0.255.255 any
done!
```

2 Assigning priority 3 to all TCP traffic going to the host 172.44.17.1 – rule 2:

```
C460-1(super)# ip access-list 100 2 fwd3 tcp any host
172.44.17.1
done!
```

3 Denying Telnet sessions originated by the host 192.168.5.33 – rule 3

```
C460-1(super)# ip access-list 100 3 deny tcp host
192.168.5.33 any eq 23
done!
```

IP Fragmentation and Reassembly

IP Fragmentation and Reassembly Overview

The C460 supports IP Fragmentation and Reassembly. This feature allows the router to send and receive large IP packets where the underlying data link protocol constrains MTU (maximum transport unit).

IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. The IP source, destination, identification, total length, and fragment offset fields, along with the “more” fragment and “don't” fragment flags in the IP header, are used for IP fragmentation and reassembly.

IP Fragmentation works as follows:

- IP packet is divided into fragments
- each fragment becomes its own IP packet
- each packet has same identifier, source, destination address
- fragments are usually not reassembled until final destination

IP Fragmentation/Reassembly CLI Commands

In order to...	Use the following command...
Clear the fragment database and restore its defaults	clear fragment
Set the maximum number of fragments that can comprise a single IP packet	fragment chain
Set the maximum number of fragmented IP packets, destined for the router, to reassemble at any given time	fragment size
Set the maximum number of seconds to reassemble a fragmented IP packet destined for the router.	fragment timeout
Display information regarding fragmented IP packets that are destined for the router	show fragment

Chapter 7

Switch Monitoring Features

SNMP Configuration

SNMP Configuration Overview

Managers and Agents

SNMP uses software entities called managers and agents to manage network devices:

The manager monitors and controls all other SNMP-managed devices or network nodes on the network. There must be at least one SNMP Manager in a managed network. The manager is installed on a workstation located on the network.

An agent resides in a managed device or network node. The agent receives instructions from the SNMP Manager, and also sends management information back to the SNMP Manager as events occur. The agent can reside on:

- Routers
- Bridges
- Hubs
- Workstations
- Printers
- Other network devices.

There are many SNMP management applications, but all these applications perform the same basic task. They allow SNMP managers to communicate with agents to get statistics and receive alerts from the network devices. You can use any SNMP-compatible network management system to monitor and control an Avaya C460.

Manager/Agent Communication

There are several ways that the SNMP manager and the agent communicate.

The manager can:

- Retrieve a value – a *get* action
  The SNMP manager requests information from the agent, such as the number of users logged on to the agent device, or the status of a critical process on that device. The agent gets the value of the requested MIB variable and sends the value back to the manager.
- Retrieve the value immediately after the variable you name – a *get-next* action).
  The SNMP manager retrieves values from within a MIB. Using the get-next

function, you do not need to know the exact variable name you are looking for. The SNMP manager takes the variable you name and then uses a sequential search to find the desired variable.

- Retrieve a number of values – a *get-bulk* action
  The SNMP manager performs the number of get-next actions that you specify.
- Change a setting on the agent – a *set* action
  The SNMP manager requests the agent to change the value of the MIB variable. For example, you can run a script or an application on a remote device with a set action.
- An agent can send an unsolicited message to the manager at any time if a significant, predetermined event takes place on the agent. This message is called a *trap*.
  When a trap condition occurs, the SNMP agent sends an SNMP trap message to the device specified as the trap receiver or trap host. The SNMP Administrator configures the trap host, usually the SNMP management station, to perform the action needed when a trap is detected.

SNMP Communities

Each SNMP device or member is part of a *community*. An SNMP community determines the access rights for SNMP devices.

You supply a name to the community. After that, all SNMP devices that are assigned to that community as *members* have the same access rights. The access rights are:

- **read** - Allows read-only access to the MIB tree for devices included in this community
- **read-write** - Allows both read and write access to the MIB tree for devices included in this community
- **trap** – Allows traps to be sent between devices included in this community

SNMP Configuration CLI Commands

In order to...	Use the following command...
Set or modify the switch's SNMP community strings	set snmp community
Add an entry into the SNMP trap receiver table and to enable or disable the different SNMP traps for a specific receiver	set snmp trap

In order to...	Use the following command...
Enable/Disable the sending of SNMP traps upon SNMP authentication failure	set snmp trap auth
Set the number of retries initiated by the Device Manager application when it tries to send SNMP messages to the device	set snmp retries
Set the SNMP timeout	set snmp trap
Enable or disable generic SNMP uplink/downlink traps from a port	set port trap
Display SNMP information	show snmp
Display the number of retries initiated by the Device Manager application when it tries to send SNMP messages to the device	show snmp retries
Display the default SNMP timeout.	show snmp timeout
Display information on SNMP generic link up/down traps sent for a specific port	show port trap
Clear an entry from the SNMP trap receiver table	clear snmp trap

RMON

RMON Overview

RMON, the internationally recognized network monitoring standard, is a network management protocol that allows network information to be gathered at a single workstation. You can use RMON probes to monitor and analyze a single segment only. When you deploy a switch on the network, there are additional components in the network that cannot be monitored using RMON. These components include the switch fabric, VLAN, and statistics for all ports.

RMON is the internationally recognized and approved standard for detailed analysis of shared Ethernet media. It ensures consistency in the monitoring and display of statistics between different vendors.

RMON's advanced remote networking capabilities provide the tools needed to monitor and analyze the behavior of segments on a network. In conjunction with an RMON agent, RMON gathers details and logical information about network status, performance and users running applications on the network.

RMON has two levels:

- RMON I analyzes the MAC layer (Layer 2 in the OSI seven-layer model).
- RMON 2 analyzes the upper layers (Layers 3 and above).

An RMON agent is a probe that collects information about segments, hosts and traffic and sends the information to a management station. You use specific software tools to view the information collected by the RMON agent on the management station.

RMON 2

The C460 implements the following components of AnyLayer™ SMON (RMON2)

- IP protocol distribution counters
- TCP/UDP protocols counters
- DSMON (DSCP Monitoring)
  - — Only non-zero DSCP values are counted

The following IP control protocols are counted by default

- ICMP over IP
- OSPF over IP
- VRRP over IP
- ARP
- Routing software in the CPU counts these protocols.

The following seven TCP/UDP protocols statistics are gathered by default:

- FTP-data over TCP/IP
- Telnet over TCP/IP
- SMTP over TCP/IP
- HTTP over TCP/IP
- POP3 over TCP/IP
- SNMP over UDP/IP
- SNMP Trap over UDP/IP
- The eighth counter is available to count all the undefined routed traffic

ⓘ You can change any of the above counters can be to present statistics on other TCP/UDP port numbers

Router Statistics Overview

Router Statistics provides you with a high-level view of the traffic being routed through each of the I/O modules in the selected C460 switch.

Router Statistics enables you to view graphically which devices are handling the most traffic. This can help you discover overloaded or under-utilized routers in the network.

Router Statistics also enables you to save the information displayed in reports. By comparing reports generated over time, you can optimize the placement of your routers.

Protocol Distribution Overview

Protocol Distribution provides you with details about the protocols routed by a C460 I/O routing module, and tracks the distribution of traffic through the device among various network and application layer protocols. Protocol Distribution collects all information in real-time, and displays it in a variety of powerful and easy to use graphic formats.

Protocol Distribution for the C460 I/O modules includes monitoring of DSCP (Differentiated Services Code Point) tagged traffic. DSCP is an extension of IP which provides a method of encoding QoS (Quality of Service) information in the IP header of traffic. This enables you to change the priority of packets to conform to standards for applications such as Voice Over Internet. Protocol Distribution for C460 I/O modules provides graphical representations of IP traffic with non-zero DSCP headers and IP traffic with zero DSCP headers.

Protocol Distribution stores all data recently collected from the device. Protocol Distribution also allows you to save collected information in reports. You can learn what is normal and abnormal behavior for your specific network by viewing the reports and analyzing changes in your network's traffic. This can help you discover problems in your network configuration. In general, the Protocol Distribution tool can help you see things that become apparent over time from a high-level view.

RMON CLI commands

In order to...	Use the following command...
Create an RMON history entry	rmon history
Delete an existing RMON history entry	no rmon history
Create a new RMON alarm entry	rmon alarm
Delete an existing RMON alarm entry	no rmon alarm
Create an RMON event entry	rmon event
Delete an existing RMON event entry	no rmon event
Display the RMON statistics counters for a certain interface number according to the MIB-2 interface table numbering scheme	show rmon statistics
Display the most recent RMON history log for a given History Index	show rmon history
Display the parameters set for a specific alarm entry that was set using the rmon alarm command	show rmon alarm
Display the parameters of an Event entry defined by the rmon event command or Device Manager	show rmon event

RMON 2 CLI Commands

In order to...	Use the following command...
Add a protocol to the protocol directory.	rmon2 protocol-dir
Remove a protocol from the protocol directory	no rmon2 protocol-dir

In order to...	Use the following command...
Enable the RMON2 Protocol Distribution application	rmon2 protocol-dist
Disable the RMON2 Protocol Distribution application	no rmon2 protocol-dist
Display the DSCP distribution (routed traffic only) for the RMON2 application	show rmon2 dscp-stats
Display the RMON2 protocol distribution information	show rmon2 protocol-dir
Display the status of the rmon2 application	show rmon2 state
Clear RMON 2 statistics	clear rmon2 statistics

SMON

SMON Overview

SMON is Avaya's standard-setting switch monitoring technology that has now been adopted as IETF standard RFC 2613. SMON extends the RMON standard to provide the switch monitoring tools and features you need to analyze the switched network and all its components.

SMON provides the basis for top-down network monitoring. Top-down monitoring starts when the you notice particular traffic flow patterns in a global view of the network. The network manager can progressively focus in and find the specific source or sources of the traffic.

Using this method, the amount of information the network manager must assess is kept to a minimum. Top-down monitoring is robust enough to enable control of even the most complex and sophisticated networks.

SMON is an extension of the RMON standard. SMON adds to the monitoring capabilities of RMON in the following ways:

- It provides additional tools and features for monitoring in the switch environment.
- It allows monitoring of ATM networks that are based on cells rather than packets.
- It provides a global view of traffic flow on a network with multiple switches.

SMON monitoring provides:

- A global view of traffic for all switches on the network
- An overall view of traffic passing through a specific switch
- Detailed data of the hosts transmitting packets or cells through a switch
- An analysis of traffic passing through each port connected to a switch, and
- A view of traffic between various hosts connected to a switch.

SMON extends both RMON I for the MAC layer, and RMON 2 for the network layer and higher. SMON monitoring collects and displays data in real-time.

Top-down view of all traffic:

- Network view for selected switches
- Network view for selected ports
- VLAN view
- History

ⓘ In order to use SMON, you need to install the SMON license on the C460 switch and use Avaya MSNM with SMON. See "Basic Switch Configuration" in the *Avaya C460 Installation and Maintenance Guide*.

Logs

Log Overview

There are two logs are available for each Supervisor module – the *System Log* file and the *Event Log* file.

- The System Log displays all the resets that took place in the supervisor with their time stamp and cause.
- The Event Log displays all the resets in the System log plus SW errors which did not result in a reset, or special events, such as VRRP switchover, and so on

You can view logs of both SPVs from the Active Supervisor module CLI, but the files are encrypted. You can view the unencrypted files in "Tech" mode.

Log CLI Commands

In order to...	Use the following command...
Display the System Log	show system-log show system-log (Layer 3)
Display the Event log	show event-log show event-log (Layer 3)
Clear the System Log	clear system-log
Clear the Event Log	clear event-log

Port Mirroring Configuration

Port Mirroring Overview

Port Mirroring copies all received and transmitted packets (including local traffic) from a source port to a predefined destination port, in addition to the normal destination port of the packets. Port Mirroring, also known as “sniffing” is useful in debugging network problems.

Port mirroring allows you to define a source port and a destination port, regardless of port type. For example, a 10 Mbps and a 100 Mbps port can form a valid source/destination pair. You cannot, however define the port mirroring source and destination ports as the same port.

You can define one source port and one destination port on each C460 chassis for either received – Rx – or transmitted and received – Tx + Rx – traffic.

Port Mirroring CLI commands

In order to...	Use the following command...
Define a port mirroring source-destination pair in the switch	set port mirror
Display port mirroring information for the switch	show port mirror
Cancel port mirroring	clear port mirror

Port Mirroring Constraints

Note the following two limitations:

- If the source port is a 10/100 Mbps port, the destination port must be located on the same 24-port range – 1 to 24 or 25 to 48
- If the source port is a Gigabit Ethernet port, the destination port must also be a Gigabit Ethernet port. The destination port can be on any I/O module.

Port Classification

Port Classification Overview

With the Avaya C460, you can classify any port as “regular” or “valuable”. Setting a port to “valuable” classification means that a link fault trap is sent in the event of a link failure. The trap is sent even when the port is disabled.
This feature is particularly useful for the port redundancy application, where you need to be informed about a link failure on the dormant port.

Port Classification CLI Commands

In order to...	Use the following command...
Set the port classification to either regular or valuable	set port classification
Display a port’s classification	show port classification