



Configuring Ethernet Switching

This section describes the Ethernet switching capabilities of the Catalyst 4224. These capabilities are designed to work as part of the Cisco IP Telephony solution.

This section also outlines how to configure Ethernet ports on the Catalyst 4224 to support IP phones in a branch office on your network.

This section contains the following topics:

- [Configuring the Catalyst 4224 for Cisco IP Telephony, page 3-1](#)
- [Configuring Ethernet Ports to Support IP Phones and a Daisy-Chain Workstation, page 3-3](#)
- [Configuring Ethernet Ports to Support IP Phones with Multiple Ports, page 3-9](#)
- [Managing the Catalyst 4224 Access Gateway Switch, page 3-10](#)

Configuring the Catalyst 4224 for Cisco IP Telephony

The Catalyst 4224 has 24 10/100 switched Ethernet ports with integrated inline power and Quality of Service (QoS) features. These features allow you to extend Voice-over-IP (VoIP) networks to small branch offices.

As an access gateway switch, the Catalyst 4224 can be deployed as a component of a centralized call processing network using a centrally deployed Cisco CallManager. Instead of deploying and managing key systems or PBXs in small branch offices, applications are centrally located at the corporate headquarters or data center and are accessed via the IP WAN.

Default Switch Configuration

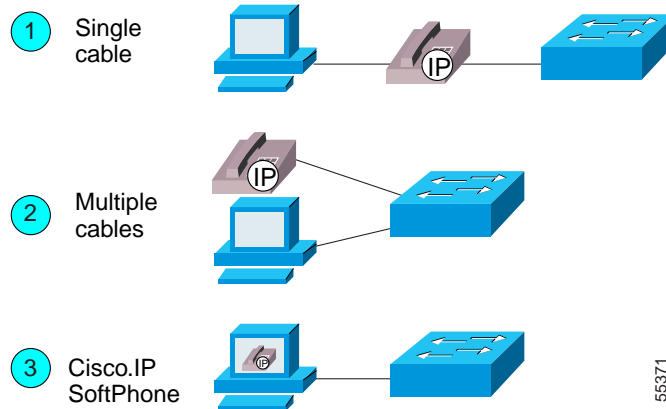
By default, the Catalyst 4224 provides the following settings with respect to Cisco IP Telephony:

- All switch ports are in access VLAN 1.
- All switch ports are static access ports, not 802.1Q trunk ports.
- Default voice VLAN is not configured on the switch.
- Inline power is automatically supplied on the 10/100 ports.

Connecting IP Phones to Your Campus Network

There are three ways to connect an IP phone to a campus network. You can use a single cable, multiple cables, or the Cisco IP SoftPhone application running on a PC. (See [Figure 3-1](#).)

Figure 3-1 Ways to Connect IP Phones to the Network



For more information about Option 1, see the “[Configuring Ethernet Ports to Support IP Phones and a Daisy-Chained Workstation](#)” section on page 3-3.

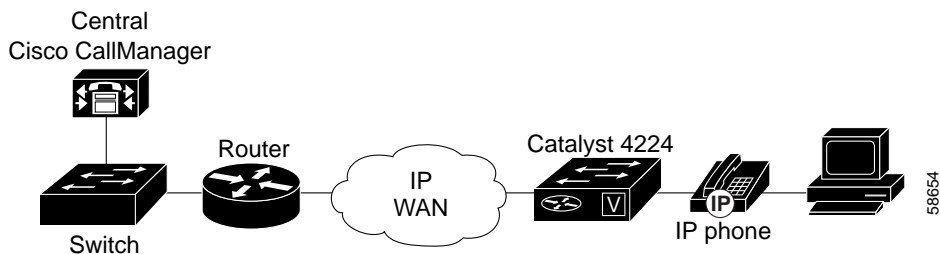
For more information about Option 2, see the “[Configuring Ethernet Ports to Support IP Phones with Multiple Ports](#)” section on page 3-9.

For more information about Option 3, which entails the Cisco IP SoftPhone application, see the Cisco IP SoftPhone documentation library. The Cisco IP SoftPhone application was developed to provide clients with a phone that runs on software. This application can be installed on any PC that connects to an IP telephony network.

Configuring Ethernet Ports to Support IP Phones and a Daisy-Chained Workstation

Figure 3-2 shows the topology of a centralized Cisco CallManager deployment model used to enable converged networks.

Figure 3-2 Catalyst 4224 with IP Phone and Workstation



The configurations described in this section use the model shown in Figure 3-2. In this model, voice traffic is given a higher priority (CoS=5) than data traffic (CoS=0). Hence, voice traffic is placed in a high-priority queue that gets serviced first, and data traffic is placed in a low-priority queue that gets serviced later.

This section describes the following configuration schemes:

- [Configuring Separate Voice and Data Subnets, page 3-4](#)
- [Configuring a Single Subnet for Voice and Data, page 3-7](#)

For details on the commands used in the following configuration examples, refer to [Appendix A, “Command Reference for Voice VLAN.”](#)



Note In the following configurations, the **powerinline** command is set to **auto** by default.

Configuring Separate Voice and Data Subnets

For ease of network administration and increased scalability, network managers can configure the Catalyst 4224 to support Cisco IP phones such that the voice and data traffic reside on separate subnets. You should always use separate VLANs when you are able to segment the existing IP address space of your branch office.

User priority bits in the 802.1p portion of the 802.1Q standard header are used to provide prioritization in Ethernet switches. This is a vital component in designing Cisco IP Telephony networks.

The Catalyst 4224 provides the performance and intelligent services of Cisco IOS software for branch office applications. The Catalyst 4224 can identify user applications—such as voice or multicast video—and classify traffic with the appropriate priority levels. QoS policies are enforced using Layer 2 and 3 information such as 802.1p, IP precedence, and DSCP.



Note Refer to the *Cisco AVVID QoS Design Guide* for more information on how to implement end-to-end QoS as you deploy Cisco IP Telephony solutions.

The following exit procedure shows how to automatically configure Cisco IP phones to send voice traffic on the voice VLAN ID (VVID). (See the [“Voice Traffic and VVID”](#) section on page 3-5.)

	Task	Command
Step 1	Enable VLAN database. ID range is 1 to 1005.	<code>enable</code> <code>vlan database</code> <code>vlan id</code> <code>exit</code>
Step 2	Set up switch port to configure IP phone on voice VLAN (on per-port basis).	

	Task	Command
	Enter the privileged EXEC mode. A preset password may be required to enter this mode.	<code>enable</code>
	Enter global configuration mode.	<code>configure terminal</code>
	Enter the interface configuration mode and the port to be configured (for example, interface fa5/1).	<code>interface interface</code>
	Configure the port as access and assign a data VLAN.	<code>switchport access vlan vlan-id</code>
	Configure the voice port with a VVID that will be used exclusively for voice traffic.	<code>switchport voice vlan vlan-id</code>
Step 3	Verify the switch port configuration and save it.	
	Verify the port configuration you just entered.	<code>show run interface interface</code>
	Save the current configuration in Flash memory.	<code>write memory</code>

Voice Traffic and VVID

The Catalyst 4224 can automatically configure voice VLAN. With the automatically configured voice VLAN feature, network administrators can segment phones into separate logical networks even though the data and voice infrastructure is physically the same. The voice VLAN feature places the phones into their own VLANs without the need for end-user intervention. A user can plug the phone into the switch, and the switch provides the phone with the necessary VLAN information.

Sample Configuration 1

The following example shows how to configure separate subnets for voice and data on the Catalyst 4224:

```
interface FastEthernet5/1
  description DOT1Q port to IP Phone
  switchport access vlan 50
  switchport voice vlan 150
  spanning-tree portfast (See Note below)

interface Vlan 150
  description voice vlan
  ip address 10.150.1.1 255.255.255.0
  ip helper-address 172.20.73.14 (See Note below)

interface Vlan 50
  description data vlan
  ip address 10.50.1.1 255.255.255.0
```

This configuration instructs the IP phone to generate a packet with an 802.1Q VLAN ID of 150 with an 802.1p value of 5 (default for voice bearer traffic).



Note

The portfast command is only supported on nontrunk ports.



Note

In a centralized Cisco CallManager deployment model, the DHCP server might be located across the WAN link. If so, an **ip helper-address** command pointing to the DHCP server should be included on the voice VLAN interface for the IP phone. This is done to obtain its IP address as well as the address of the TFTP server required for its configuration.

Be aware that Cisco IOS supports a DHCP server function. If this function is used, the Catalyst 4224 serves as a local DHCP server and a helper address would not be required.

Sample Configuration 2

Configuring inter-VLAN routing is identical to the configuration on a Catalyst 6000 with an MSFC. Configuring an interface for WAN routing is consistent with other Cisco IOS platforms.

The following example provides a sample configuration:

```
interface Vlan 160
  description voice vlan
  ip address 10.6.1.1 255.255.255.0

interface Vlan 60
  description data vlan
  ip address 10.60.1.1 255.255.255.0

interface Serial1/0
  ip address 160.3.1.2 255.255.255.0
```

**Note**

Standard IGP routing protocols such as RIP, Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), and open shortest path first (OSPF) are supported on the Catalyst 4224. Multicast routing is also supported for PIM dense mode, sparse mode, and sparse-dense mode.

Configuring a Single Subnet for Voice and Data

For network designs with incremental IP telephony deployment, network managers can configure the Catalyst 4224 so that the voice and data traffic coexist on the same subnet. This might be necessary when it is impractical to allocate an additional IP subnet for IP phones. You must still prioritize voice above data at both Layer 2 and Layer 3.

Layer 3 classification is already handled because the phone sets the type of service (ToS) bits in all media streams to an IP Precedence value of 5. (With Cisco CallManager Release 3.0(5), this marking changed to a Differentiated Services Code Point [DSCP] value of EF.) However, to ensure that there is Layer 2 classification for admission to the multiple queues in the branch office switches, the phone must also use the User Priority bits in the Layer 2 802.1p header to provide class of service (CoS) marking. Setting the bits to provide marking can be done by having the switch look for 802.1p headers on the native VLAN.

This configuration approach must address two key considerations:

- Network managers should ensure that existing subnets have enough available IP addresses for the new Cisco IP phones, each of which requires a unique IP address.
- Administering a network with a mix of IP phones and workstations on the same subnet might pose a challenge.

The following procedure shows how to automatically configure Cisco IP phones to send voice and data traffic on the same VLAN.

	Task	Command
Step 1	Set up switch port to configure IP phone on the same VLAN as the access VLAN.	
	Enter global configuration mode.	<code>configure terminal</code>
	Enter the interface configuration mode and the port to be configured (for example, <code>interface fa5/1</code>)	<code>interface interface</code>
	Set the native VLAN for untagged traffic. <i>vlan-id</i> represents the ID of the VLAN that is sending and receiving untagged traffic on the port. Valid IDs are from 1 to 1001. Leading zeroes are not accepted.	<code>switchport access vlan vlan-id</code>
	Configure the Cisco IP Phone to send voice traffic with higher priority (CoS=5 on 802.1Q tag) on the access VLAN. Data traffic (from an attached PC) is sent untagged for lower priority (port default=0).	<code>switchport voice vlan dot1p</code>
	Return to the privileged EXEC mode.	<code>end</code>
Step 2	Verify the switch port configuration and save.	
	Verify the port configuration you just entered.	<code>show run interface interface</code>
	Save the current configuration in Flash memory.	<code>write memory</code>

Sample Configuration

The Catalyst 4224 supports the use of an 802.1p-only option when configuring the voice VLAN. Use this option to allow the IP phone to tag VoIP packets with a CoS of 5 on the native VLAN, while all PC data traffic is sent untagged.

The following example shows a single subnet configuration for the Catalyst 4224 switch:

```
interface FastEthernet5/2
description Port to IP Phone in single subnet
    switchport access vlan 40
    switchport voice vlan dot1p
    spanning-tree portfast
```

The Catalyst 4224 instructs the IP phone to generate an 802.1Q frame with a null VLAN ID value but with an 802.1p value (default is CoS of 5 for bearer traffic). The voice and data vlans are both 40 in this example.

Configuring Ethernet Ports to Support IP Phones with Multiple Ports

You might want to use multiple ports to connect the IP phones (option 2 in [Figure 3-1](#)) if any of the following conditions apply to your Cisco IP telephony network:

- You are connecting IP phones that do not have a second Ethernet port for attaching a PC.
- You want to create a physical separation between the voice and data networks.
- You want to provide in-line power easily to the IP phones without having to upgrade the data infrastructure.
- You want to limit the number of switches that need UPS power.

IP Addressing

The recommended configuration for using multiple cables to connect IP phones to the network is to use a separate IP subnet and separate VLANs for IP telephony.

Sample Configuration

The following example illustrates the configuration on the IP phone:

```
interface FastEthernetx/x
    switchport voice vlan x
```

The following example illustrates the configuration on the PC:

```
interface FastEthernetx/y
    switchport access vlan y
```



Note

Using a separate subnet, and possibly a separate IP address space, may not be an option for some small branch offices due to the IP routing configuration. If the IP routing can handle an additional subnet at the remote branch, you can use Cisco Network Registrar and secondary addressing.

Managing the Catalyst 4224 Access Gateway Switch

This section illustrates how to perform basic management tasks on the Catalyst 4224 with the Cisco IOS command-line interface (CLI). You might find this information useful when you configure the switch for the previous scenarios.



Note

For reference information on the voice commands used in this section, refer to the [Appendix A, “Command Reference for Voice VLAN.”](#)

This section contains the following topics:

- [Adding Trap Managers, page 3-11](#)
- [Configuring IP Information, page 3-11](#)
- [Configuring Voice Ports, page 3-14](#)
- [Enabling and Disabling Switch Port Analyzer, page 3-16](#)
- [Managing the ARP Table, page 3-17](#)
- [Managing the MAC Address Tables, page 3-18](#)

Adding Trap Managers

A trap manager is a management station that receives and processes traps. When you configure a trap manager, community strings for each member switch must be unique. If a member switch has an assigned IP address, the management station accesses the switch by using its assigned IP address.

By default, no trap manager is defined, and no traps are issued.

Beginning in privileged EXEC mode, follow these steps to add a trap manager and community string:

	Task	Command
Step 1	Enter global configuration mode.	<code>config terminal</code>
Step 2	Enter the trap manager IP address, community string, and the traps to generate.	<code>snmp-server host 172.2.128.263 traps1 snmp vlan-membership</code>
Step 3	Return to privileged EXEC mode.	<code>end</code>
Step 4	Verify that the information was entered correctly by displaying the running configuration.	<code>show running-config</code>

Configuring IP Information

This section describes how to assign IP information on the Catalyst 4224, and contains the following topics:

- [Assigning IP Information to the Switch—Overview, page 3-11](#)
- [Assigning IP Information to the Switch—Procedure, page 3-12](#)
- [Removing an IP Address, page 3-13](#)
- [Specifying a Domain Name and Configuring the DNS, page 3-13](#)

Assigning IP Information to the Switch—Overview

You can use a BOOTP server to automatically assign IP information to the switch; however, the BOOTP server must be set up in advance with a database of physical MAC addresses and corresponding IP addresses, subnet masks, and default

gateway addresses. In addition, the switch must be able to access the BOOTP server through one of its ports. At startup, a switch without an IP address requests the information from the BOOTP server; the requested information is saved in the switch running the configuration file. To ensure that the IP information is saved when the switch is restarted, save the configuration by entering the **write memory** command in privileged EXEC mode.

You can change the information in these fields. The mask identifies the bits that denote the network number in the IP address. When you use the mask to create a subnet on a network, the mask is then referred to as a subnet mask. The broadcast address is reserved for sending messages to all hosts. The CPU sends traffic to an unknown IP address through the default gateway.

Assigning IP Information to the Switch—Procedure

Beginning in privileged EXEC mode, follow these steps to enter the IP information:

	Task	Command
Step 1	Enter global configuration mode.	<code>configure terminal</code>
Step 2	Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. VLAN 1 is the management VLAN, but you can configure any VLAN from IDs 1 to 1001.	<code>interface vlan 1</code>
Step 3	Enter the IP address and subnet mask.	<code>ip address ip_address subnet_mask</code>
Step 4	Return to global configuration mode.	<code>exit</code>
Step 5	Enter the IP address of the default router.	<code>ip default-gateway ip_address</code>
Step 6	Return to privileged EXEC mode.	<code>end</code>
Step 7	Verify that the information was entered correctly by displaying the running configuration. If the information is incorrect, repeat the procedure.	<code>show running-config</code>

Removing an IP Address

Use the following procedure to remove IP information from a switch.



Note

Using the **no ip address** command in configuration mode disables the IP protocol stack and removes the IP information. Cluster members without IP addresses rely on the IP protocol stack being enabled.

Beginning in privileged EXEC mode, follow these steps to remove an IP address:

	Task	Command
Step 1	Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. VLAN 1 is the management VLAN, but you can configure any VLAN from IDs 1 to 1001.	<code>interface vlan 1</code>
Step 2	Remove the IP address and subnet mask.	<code>no ip address</code>
Step 3	Return to privileged EXEC mode.	<code>end</code>
Step 4	Verify that the information was removed by displaying the running configuration.	<code>show running-config</code>



Caution

If you are removing the IP address through a Telnet session, your connection to the switch will be lost.

Specifying a Domain Name and Configuring the DNS

Each unique IP address can have an associated host name. Cisco IOS software maintains a cache of host name-to-address mappings for use by the EXEC mode commands **connect**, **telnet**, **ping**, and related Telnet support operations. This cache speeds the process of converting names to addresses.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, such as the File Transfer Protocol (FTP) system, is identified as *ftp.cisco.com*.

To track domain names, IP has defined the concept of a domain name server (DNS), whose purpose is to hold a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names and then specify a name server and enable the DNS, the Internet's global naming scheme that uniquely identifies network devices.

Specifying the Domain Name

You can specify a default domain name that the software uses to complete domain name requests. You can specify either a single domain name or a list of domain names. When you specify a domain name, any IP host name without a domain name will have that domain name appended to it before being added to the host table.

Specifying a Name Server

You can specify up to six hosts that can function as a name server to supply name information for the DNS.

Enabling the DNS

If your network devices require connectivity with devices in networks for which you do not control name assignment, you can assign device names that uniquely identify your devices within the entire internetwork. The Internet's global naming scheme, the DNS, accomplishes this task. This service is enabled by default.

Configuring Voice Ports

The Catalyst 4224 can connect to a Cisco 7960 IP Phone and carry IP voice traffic. If necessary, the Catalyst 4224 can supply electrical power to the circuit connecting it to the Cisco 7960 IP Phone.

Because the sound quality of an IP telephone call can deteriorate if the data is unevenly transmitted, the current release of the Cisco IOS software supports Quality of Service (QoS) based on IEEE 802.1p Class of Service (CoS). QoS uses classification and scheduling to transmit network traffic from the switch in a predictable manner.

The Cisco 7960 IP Phone contains an integrated three-port 10/100 switch. These dedicated ports connect to the following devices:

- Port 1 connects to the Catalyst 4224 switch or other Voice-over-IP device.
- Port 2 is an internal 10/100 interface that carries the phone traffic.
- Port 3 connects to a PC or other device.

[Figure 3-2 on page 3-3](#) shows a sample configuration for a Cisco 7960 IP Phone.

Configuring a Port to Connect to a Cisco 7960 IP Phone

Because a Cisco 7960 IP Phone also supports connection to a PC or other device, a port connecting a Catalyst 4224 to a Cisco 7960 IP Phone can carry a mix of traffic. There are three ways to configure a port connected to a Cisco 7960 IP Phone:

- All traffic is transmitted according to the default CoS priority (0) of the port. This is the default.
- Voice traffic is given a higher priority by the phone, and all traffic is in the same VLAN.
- Voice and data traffic are carried on separate VLANs, and voice traffic always has a CoS priority of five.

Disabling Inline Power on a Catalyst 4224

The Catalyst 4224 can supply inline power to the Cisco 7960 IP Phone if necessary. The Cisco 7960 IP Phone can also be connected to an AC power source and supply its own power to the voice circuit. When the Cisco 7960 IP Phone is supplying its own power, a Catalyst 4224 can forward IP voice traffic to and from the phone.

A detection mechanism on the Catalyst 4224 determines whether it is connected to a Cisco 7960 IP Phone. If the switch senses that there is no power on the circuit, the switch supplies the power. If there is power on the circuit, the switch does not supply it.

You can configure the switch to never supply power to the Cisco 7960 IP Phone and to disable the detection mechanism.

Beginning in privileged EXEC mode, follow these steps to configure a port to never supply power to Cisco 7960 IP Phones:

	Task	Command
Step 1	Enter global configuration mode.	<code>configure terminal</code>
Step 2	Enter interface configuration mode, and enter the port to be configured.	<code>interface interface</code>
Step 3	Permanently disable inline power on the port.	<code>power inline never</code>
Step 4	Return to privileged EXEC mode.	<code>end</code>
Step 5	Verify the change by displaying the setting as configured.	<code>show power inline interface configured</code>



Note

Entering the **show power inline** [*interface-type number*] command in privileged EXEC mode displays the power allocated to the IP phone by the Catalyst 4224. To display the maximum power requested by the IP phone, enter the **show cdp neighbors** [*interface-type number*] **detail** command in privileged EXEC mode.

Enabling and Disabling Switch Port Analyzer

You can monitor traffic on a given port by forwarding incoming and outgoing traffic on the port to another port in the same VLAN. A Switch Port Analyzer (SPAN) port cannot monitor ports in a different VLAN, and a SPAN port must be a static-access port. Any number of ports can be defined as SPAN ports, and any combination of ports can be monitored. SPAN is supported for up to two sessions.

Enabling the Switch Port Analyzer

Beginning in privileged EXEC mode, follow these steps to enable SPAN:

	Task	Command
Step 1	Enter global configuration mode.	<code>configure terminal</code>
Step 2	Enable port monitoring for a specific session (“ <i>number</i> ”). Optionally, supply a SPAN <i>destination</i> interface, and a <i>source</i> interface	<code>monitor session <i>number</i> <i>destination source</i></code>
Step 3	Return to privileged EXEC mode.	<code>end</code>
Step 4	Verify your entries.	<code>show running-config</code>

Disabling Switch Port Analyzer

Beginning in privileged EXEC mode, follow these steps to disable SPAN:

	Task	Command
Step 1	Enter global configuration mode.	<code>configure terminal</code>
Step 2	Disable port monitoring for a specific session.	<code>no monitor session <i>number</i></code>
Step 3	Return to privileged EXEC mode.	<code>end</code>
Step 4	Verify your entries.	<code>show running-config</code>

Managing the ARP Table

To communicate with a device (on Ethernet, for example), the software first must determine the 48-bit MAC or local data link address of that device. The process of determining the local data link address from an IP address is called *address resolution*.

The Address Resolution Protocol (ARP) associates a host IP address with corresponding media or MAC addresses and VLAN ID. Taking an IP address as input, ARP determines the associated MAC address. Once a MAC address is determined, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then, the IP datagram is encapsulated in a link-layer frame and sent over the network.

Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the **arpa** keyword) is enabled on the IP interface.

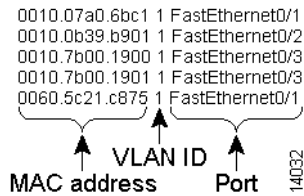
When you manually add entries to the ARP Table by using the CLI, you must be aware that these entries do not age and must be manually removed.

Managing the MAC Address Tables

The switch uses the MAC address tables to forward traffic between ports. All MAC addresses in the address tables are associated with one or more ports. These MAC tables include the following types of addresses:

- Dynamic address—A source MAC address that the switch learns and then drops when it is not in use.
- Secure address—A manually entered unicast address that is usually associated with a secured port. Secure addresses do not age.
- Static address—A manually entered unicast or multicast address that does not age and that is not lost when the switch resets.

The address tables list the destination MAC address and the associated VLAN ID, module, and port number associated with the address. Figure 3-3 shows an example of a list of addresses as they would appear in the dynamic, secure, or static address table.

Figure 3-3 Contents of the Address Table

MAC Addresses and VLANs

All MAC addresses are associated with one or more VLANs. An address can exist in more than one VLAN and have different destinations in each. Multicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 11 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN. An address can be secure in one VLAN and dynamic in another. Addresses that are statically entered in one VLAN must be static addresses in all other VLANs.

Changing the Address Aging Time

Dynamic addresses are source MAC addresses that the switch learns and then drops when they are not in use. Use the Aging Time field to define how long the switch retains unseen addresses in the table. This parameter applies to all VLANs.

Configuring the Aging Time

Setting too short an aging time can cause addresses to be prematurely removed from the table. When the switch receives a packet for an unknown destination, the switch floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses; it can cause delays in establishing connectivity when a workstation is moved to a new port.

Beginning in privileged EXEC mode, follow these steps to configure the dynamic address table aging time.

	Task	Command
Step 1	Enter global configuration mode.	<code>configure terminal</code>
Step 2	Enter the number of seconds that dynamic addresses are to be retained in the address table. You can enter a number from 10 to 1000000.	<code>mac-address-table aging-time</code> <i>seconds</i>
Step 3	Return to privileged EXEC mode.	<code>end</code>
Step 4	Verify your entry.	<code>show mac-address-table</code> <code>aging-time</code>

Removing Dynamic Address Entries

Beginning in privileged EXEC mode, follow these steps to remove a dynamic address entry:

	Task	Command
Step 1	Enter global configuration mode.	<code>configure terminal</code>
Step 2	Enter the MAC address to be removed from dynamic MAC address table.	<code>no mac-address-table dynamic</code> <i>hw-addr</i>
Step 3	Return to privileged EXEC mode.	<code>end</code>
Step 4	Verify your entry.	<code>show mac-address-table</code>

You can remove all dynamic entries by using the **clear mac-address-table dynamic** command in privileged EXEC mode.

Adding Secure Addresses

The secure address table contains secure MAC addresses and their associated ports and VLANs. A secure address is a manually entered unicast address that is forwarded to only one port per VLAN. If you enter an address that is already assigned to another port, the switch reassigns the secure address to the new port.

You can enter a secure port address even when the port does not yet belong to a VLAN. When the port is later assigned to a VLAN, packets destined for that address are forwarded to the port.

Adding Secure Addresses

Beginning in privileged EXEC mode, follow these steps to add a secure address:

	Task	Command
Step 1	Enter global configuration mode.	<code>configure terminal</code>
Step 2	Enter the MAC address, its associated port, and the VLAN ID.	<code>mac-address-table secure hw-addr interface vlan vlan-id</code>
Step 3	Return to privileged EXEC mode.	<code>end</code>
Step 4	Verify your entry.	<code>show mac-address-table secure</code>

Removing Secure Addresses

Beginning in privileged EXEC mode, follow these steps to remove a secure address:

	Task	Command
Step 1	Enter global configuration mode.	<code>configure terminal</code>
Step 2	Enter the secure MAC address, its associated port, and the VLAN ID to be removed.	<code>no mac-address-table secure hw-addr vlan vlan-id</code>
Step 3	Return to privileged EXEC mode.	<code>end</code>
Step 4	Verify your entry.	<code>show mac-address-table secure</code>

You can remove all secure addresses by using the `clear mac-address-table secure` command in privileged EXEC mode.

Adding and Removing Static Addresses

A static address has the following characteristics:

- It is manually entered in the address table and must be manually removed.
- It can be a unicast or multicast address.
- It does not age and is retained when the switch restarts.

Because all ports are associated with at least one VLAN, the switch acquires the VLAN ID for the address from the ports that you select on the forwarding map. A static address in one VLAN must be a static address in other VLANs. A packet with a static address that arrives on a VLAN where it has not been statically entered is flooded to all ports and not learned.

Adding Static Addresses

Beginning in privileged EXEC mode, follow these steps to add a static address:

	Task	Command
Step 1	Enter global configuration mode.	<code>configure terminal</code>
Step 2	Enter the static MAC address, the interface, and the VLAN ID of those ports.	<code>mac-address-table static hw-addr [interface] interface [vlan] vlan-id</code>
Step 3	Return to privileged EXEC mode.	<code>end</code>
Step 4	Verify your entry.	<code>show mac-address-table static</code>

Removing Static Addresses

Beginning in privileged EXEC mode, follow these steps to remove a static address:

	Task	Command
Step 1	Enter global configuration mode.	<code>configure terminal</code>
Step 2	Enter the static MAC address, the interface, and the VLAN ID of the port to be removed	<code>no mac-address-table static hw-addr [interface] interface [vlan] vlan-id</code>
Step 3	Return to privileged EXEC mode.	<code>end</code>
Step 4	Verify your entry.	<code>show mac-address-table static</code>

You can remove all secure addresses by using the **clear mac-address-table static** command in privileged EXEC mode.

