Cisco IOS Commands

abort

Use the **abort** VLAN database command to abandon the proposed new VLAN database, exit VLAN database mode, and return to privileged EXEC mode. This command is available only in the Enterprise Edition Software.

abort

Syntax Description

This command has no arguments or keywords.

Default

No default is defined.

Command Mode

VLAN database

Usage Guidelines

If you have added, deleted, or modified VLAN parameters in VLAN database mode but you do not want to keep the changes, the **abort** command causes all the changes to be abandoned. The VLAN configuration that was running before you entered VLAN database mode continues to be used.

Example

The following example shows how to abandon the proposed new VLAN database and exit to the privileged EXEC mode:

```
Switch(vlan)# abort
Switch#
```

You can verify that no VLAN database changes occurred by entering the **show vlan brief** command in privileged EXEC mode.

Related Commands

apply
exit
reset
show vlan
shutdown vlan
vlan database

apply

Use the **apply** VLAN database command to implement the proposed new VLAN database, increment the database configuration revision number, propagate it throughout the administrative domain, and remain in VLAN database mode. This command is available only in the Enterprise Edition Software.

apply

Syntax Description

This command has no arguments or keywords.

Default

No default is defined.

Command Mode

VLAN database

Usage Guidelines

The **apply** command implements the configuration changes you made after you entered VLAN database mode and uses them for the running configuration. This command keeps you in VLAN database mode.

You cannot use this command when the switch is in the VLAN Trunk Protocol (VTP) client mode.

Example

The following example shows how to implement the proposed new VLAN database and recognize it as the current database:

```
Switch(vlan)# apply
```

You can verify that VLAN database changes occurred by entering the **show vlan** command in privileged EXEC mode.

Related Commands

abort
exit
reset
show vlan
shutdown vlan
vlan database

cgmp

Use the **cgmp** global configuration command to enable Cisco Group Management Protocol (CGMP). You can also enable and disable the Fast Leave parameter and set the router port aging time. Use the **no** form of this command to disable CGMP.

cgmp [**leave-processing** | **holdtime** *time*]
no cgmp [**leave-processing** | **holdtime**]

Syntax Description

leave-processing	(Optional) Enable Fast Leave processing on the switch.
holdtime	(Optional) Set the amount of time a router connection is retained before the switch ceases to exchange messages with it.
time	Number of seconds a router connection is retained before the switch ceases to exchange messages with it. You can enter a number from 10 to 6000 (seconds).

Defaults

CGMP is enabled.

Fast Leave is disabled.

The hold time is 300 seconds.

Command Mode

Global configuration

Usage Guideline

CGMP must be enabled before the Fast Leave option can be enabled.

Examples

The following example shows how to disable CGMP:

```
Switch(config)# no cgmp
```

The following example shows how to disable the Fast Leave option:

```
Switch(config)# no cgmp leave-processing
```

The following example shows how to set the amount of time the switch waits before ceasing to exchange messages with a router:

```
Switch(config)# cgmp holdtime 400
```

The following example shows how to remove the amount of time the switch waits before ceasing to exchange messages with a router:

```
Switch(config)# no cgmp holdtime
```

You can verify the previous commands by entering the **show cgmp** command in privileged EXEC mode.

Related Commands

clear cgmp
show cgmp

clear cgmp

Use the **clear cgmp** privileged EXEC command to delete information that was learned by the switch using the Cisco Group Management Protocol (CGMP).

clear cgmp [**vlan** *vlan-id*] | [**group** [*address*] | **router** [*address*]]

Syntax Description

vlan	(Optional) Delete groups only within *vlan-id*.
*vlan-i*d	VLAN for which the CGMP groups or routers are to be deleted.
group	(Optional) Delete all known multicast groups and their destination ports. Limited to a VLAN if the **vlan** keyword is entered. Limited to a specific group if the *address* parameter is entered.
address	MAC address of the group or router.
router	(Optional) Delete all routers, their ports, and expiration times. Limited to a given VLAN if the **vlan** keyword is entered. Limited to a specific router if the *address* parameter is entered.

Command Mode

Privileged EXEC

Usage Guidelines

Using **clear cgmp** with no arguments deletes all groups and routers in all VLANs.

Examples

The following example shows how to delete all groups and routers on VLAN 2:

```
Switch# clear cgmp vlan 2
```

The following example shows how to delete all groups on all VLANs:

```
Switch# clear cgmp group
```

The following example shows how to delete a router address on VLAN 2:

```
Switch# clear cgmp vlan 2 router 0012.1234.1234
```

You can verify the previous commands by entering the **show cgmp** command in privileged EXEC mode.

Related Commands

cgmp
show cgmp

clear ip address

Use the **clear ip address** privileged EXEC command to delete an IP address for a switch without disabling the IP processing.

clear ip address [**vlan** *vlan-id*]

Syntax Description

vlan	(Optional) Delete IP address only within *vlan-id*.
*vlan-i*d	VLAN for which the IP address are to be deleted.

Default

No IP address is defined for the switch.

Command Mode

Privileged EXEC

Usage Guidelines

A switch can have one IP address.

The IP address of the switch can be accessed only by nodes connected to ports that belong to VLAN 1.

Example

The following example shows how to clear the IP address for the switch on VLAN 1:

```
Switch# clear ip address vlan 1
```

You can verify the previous commands by entering the **show running-config** command in privileged EXEC mode.

Related Commands

show running-config

clear mac-address-table

Use the **clear mac-address-table** privileged EXEC command to delete entries from the MAC address table.

clear mac-address-table [**static** | **dynamic** | **secure**] [**address** *hw-addr*] [**interface** *interface*] [**atm** *slot/port*] [**vlan** *vlan-id*]

Syntax Description

static	(Optional) Delete only static addresses.
dynamic	(Optional) Delete only dynamic addresses.
secure	(Optional) Delete only secure addresses.
address	(Optional) Delete the address *hw-addr* of type static, dynamic, and secure as specified.
hw-addr	Delete this address.
interface	(Optional) Delete an address on the interface *interface* of type static, dynamic, or secure as specified.
interface	Delete MAC addresses on this port.
atm	(Optional) Delete only ATM addresses.
slot	Delete ATM addresses on this slot.
port	Delete ATM addresses on this port.
vlan	(Optional) Delete all the addresses for *vlan-id*.
vlan-id	Delete MAC addresses in this VLAN.

Command Mode

Privileged EXEC

Usage Guidelines

This command deletes entries from the global MAC address table. Specific subsets can be deleted by using the optional keywords and values. If more than one optional keyword is used, all of the conditions in the argument must be true for that entry to be deleted.

Examples

The following example shows how to delete static addresses with the *in-port* value equal to fa0/7:

```
Switch# clear mac-address-table static interface fa0/7
```

The following example shows how to delete all secure addresses in VLAN 3:

```
Switch# clear mac-address-table secure vlan 3
```

The following example shows how to delete a specific address from all ports in all VLANs. If the address exists in multiple VLANs or multiple ports, all the instances are deleted.

```
Switch# clear mac-address-table address 0099.7766.5544
```

The following example shows how to delete a specific address only in VLAN 2:

```
Switch# clear mac-address-table address 0099.7766.5544 vlan 2
```

The following example shows how to delete a secure MAC address associated with the ATM port in expansion slot 2:

```
Switch(config)# clear mac-address-table secure 00c0.00a0.03fa atm 2/1
```

The following example shows how to associate a static address with the ATM port in expansion slot 2:

```
Switch(config)# mac-address-table static 00c0.00a0.03fa atm 2/1
```

You can verify the previous commands by entering the **show mac-address-table** command in privileged EXEC mode.

Related Commands

show mac-address-table

clear vmps statistics

Use the **clear vmps statistics** privileged EXEC command to clear the statistics maintained by the VLAN Query Protocol (VQP) client. This command is available only in the Enterprise Edition Software.

clear vmps statistics

Syntax Description

This command has no arguments or keywords.

Default

No default is defined.

Command Mode

Privileged EXEC

Example

The following example shows how to clear VLAN Membership Policy Server (VMPS) statistics:

```
Switch# clear vmps statistics
```

You can verify the previous command by entering the **show vmps statistics** command in privileged EXEC mode.

Related Commands

show vmps statistics

clear vtp counters

Use the **clear vtp counters** privileged EXEC command to clear the VLAN Trunk Protocol (VTP) and pruning counters. This command is available only in the Enterprise Edition Software.

clear vtp counters

Syntax Description

This command has no arguments or keywords.

Default

No default is defined.

Command Mode

Privileged EXEC

Example

The following example shows how to clear the VTP counters:

```
Switch# clear vtp counters
```

You can verify the previous command by entering the **show vtp counters** command in privileged EXEC mode.

Related Commands

show vtp counters

cluster commander-address

Use the **cluster commander-address** global configuration command to add a member switch to the cluster. This command is automatically configured on a device when the command switch adds the device to the cluster. Use the **no** form of the command to remove a member switch from the cluster.

cluster commander-address [*mac-address*]
no cluster commander-address [*mac-address*]

Syntax Description

mac-address	Mac address of the member's command switch.

Default

The switch is not a member of any cluster.

Command Mode

Global configuration

Usage Guidelines

A cluster member can have only one command switch.

Use the **no** form when the command switch is unavailable. The *mac-address* parameter allows the member switch to retain the identity of the command switch during a system reload. The **no** form of the command allows a member switch to be removed from a cluster when the cluster command switch is not available.

Example

Following is sample text from the running configuration of a cluster member.

```
cluster commander-address 00E0.1E00.111
```

The following example shows how to remove a member from the cluster by using the cluster member's console.

```
switch-es3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

The following is an example of the **no** form of the command.

```
switch-es3(config)# no cluster commander-address
switch-es3(config)# exit
```

Related Commands

cluster
show cluster
show cluster candidates
show cluster view
show cluster member

cluster enable

Use the **cluster enable** global configuration command to turn on the cluster command switch. Use the **no** form of the command to remove all members and make the command switch a candidate switch.

cluster enable *name*
no cluster enable

Syntax Description

name	Name of the cluster.

Default

The switch is not a cluster command switch.

Command Mode

Global configuration

Usage Guidelines

You must name the cluster when you enable the command switch. This command fails if a device is already configured as a member of the cluster.

Example

The following example shows how to turn on the command switch for a cluster.

```
switch(config)# cluster enable Engineering-IDF4
switch(config)# exit
```

Related Commands

show cluster
show cluster candidates
show cluster view
show cluster member

cluster member

Use the **cluster member** global configuration command to add members to a cluster. Use the **no** form of the command to remove members from the cluster.

cluster member *n* **mac-address** *hw-addr* [**password** *enable-password*]
no cluster member *n*

Syntax Description

n	The number that identifies a cluster member.
mac-address	Provide the MAC address of the command switch for the cluster member.
hw-addr	Mac address of the member's command switch.
password	(Optional) The enable password on the candidate switch. This is not required if there is no password on the candidate switch. Otherwise, use this parameter.
enable-password	Password for the candidate switch.

Default

The default is **no cluster member**. A newly-enabled command switch has no members by default.

Command Mode

Global configuration

Usage Guidelines

This command is used on the command switch to add a member to or remove a member from the cluster.

You need only the password when you configure a member to join the cluster. The password is not saved in the running or startup configuration. After a candidate switch becomes a member of the cluster, it's password ceomes the same as the **enabled** password for command switch.

If a switch does not have has a configured hostname, the command switch configures its hostname to be the command switch's hostname followed by *-n>*, where *n* is the member number.

Example

The following example shows how to add a member to a cluster.

```
switch(config)# cluster member 2 mac-address 00E0.1E00.2222
switch(config)# cluster member 4 mac-address 00E0.1E00.3333 <password>
switch(config)# exit
```

Related Commands

show cluster
show cluster candidates
show cluster view
show cluster member

cluster setup

Use the **cluster setup** privileged EXEC command on the command switch to automatically build a cluster.

cluster setup

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Usage Guidelines

You can use the **cluster setup** command to add new switches to an existing cluster. The **cluster setup** command provides a high-level view of the configuration and guides you through the configuration change process. You can only see candidate switches that are one hop away from the command switch and have no IP address. To see devices farther away, use the **show cluster member** or **show cluster candidate** command.

If a candidate switch has an **enabled** password, this information will not be passed to the cluster.

Example

The following is an example of the **cluster setup** command output:

```
Switch# cluster setup

         --- Cluster Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

This switch is already configured as cluster command switch:
Command Switch Name:m217, contains 1 members

Continue with cluster configuration dialog? [yes/no]:yes
The suggested Cluster configuration is as follows:

                                                |---Upstream---|
SN MAC Address    Name         PortIf FEC Hops   SN PortIf  FEC  State
0  0050.0f08.9840 murali-217               0                     Cmdr
1* 0050.0f08.91c0 murali-99.ci Fa0/1       1     0  Fa0/9        Candidat


The following configuration command script was created:
cluster member 1 mac-address 0050.0f08.91c0
!
end


Use this configuration? [yes/no]:yes

Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.

Switch#
```

Related Commands

cluster enable
show cluster
show cluster candidates
show cluster view
show cluster member

copy tftp

Use the **copy tftp** privileged EXEC command to download a firmware file from a TFTP server to the device.

copy tftp: *//host/src_file* **slot** *number:dst_file*

Syntax Description

//host/	TFTP host name or IP address.
src_file	File to be copied to the module.
slot	Module-based file system prefix.
number	Number of the ATM interface to which to download an image.
dst_file	Name assigned to *src_file* on the module.

Command Mode

Privileged EXEC

Usage Guidelines

The slot parameter must be accompanied by a number that is followed by a colon. If you attempt to download a version of the software older than what is currently running on the interface, a warning message appears.

Examples

The following example shows how to download a new ATM module image from a host named *spaniel* to the module flash file system as *relayer_file*.

```
Switch# copy tftp://spaniel/ATM_image slot1:relayer_file
```

You can verify the previous commands by entering the **copy tftp** command in privileged EXEC mode.

Related Commands

delete

delete

Use the **delete** privileged EXEC command to delete a file from the file system of the specified module.

delete *slot number:file*

Syntax Description

slot	Module-based file-system prefix.
number:	Slot number (1 or 2).
file	Name of file.

Command Mode

Privileged EXEC

Usage Guidelines

A colon follows the number parameter.

Examples

The following example shows how to delete the file *atm_image* from the file system for ATM module 1:

```
Switch# delete slot1:atm_image
```

Related Commands

copy

duplex

Use the **duplex** interface configuration command to specify the duplex mode of operation for a Fast Ethernet port. Use the **no** form of this command to return the port to its default value.

duplex {**full** | **half** | **auto**}
no duplex

Syntax Description

full	Port is in full-duplex mode.
half	Port is in half-duplex mode.
auto	Port automatically detects whether it should run in full- or half-duplex mode.

Default

The default is **auto**.

Command Mode

Interface configuration

Usage Guidelines

Certain ports can be configured to be either full duplex or half duplex. Applicability of this command depends on the device to which the switch is attached. All ports can be configured for either full or half duplex.

For Fast Ethernet ports, setting the port to **auto** has the same effect as specifying **half** if the attached device does not autonegotiate the duplex parameter.

For Gigabit Ethernet ports, setting the port to **auto** has the same effect as specifying **full** if the attached device does not autonegotiate the duplex parameter.

Note For guidelines on setting the switch speed and duplex parameters, see the *Catalyst 2900 Series XL Installation Guide* and the *Catalyst 3500 Series XL Installation Guide*.

This command is not supported on the ATM modules.

Examples

The following example shows how to set port 1 on a Fast Ethernet module installed in slot 2 to full duplex:

```
Switch(config)# interface fastethernet2/1
Switch(config-if)# duplex full
```

The following example shows how to set port 1 on a Gigabit Ethernet module installed in slot 2 to full duplex:

```
Switch(config)# interface gigabitethernet2/1
Switch(config-if)# duplex full
```

You can verify the previous commands by entering the **show running-config** command in privileged EXEC mode.

Related Commands

show running-config
speed

enable last-resort

Use the **enable last-resort** global configuration command to specify what happens if the TACACS and Extended TACACS servers used by the **enable** command do not respond. Use the **no** form of this command to restore the default. This command is available only in the Enterprise Edition Software.

enable last-resort {password | succeed}
no enable last-resort {password | succeed}

Syntax Description

password	Allows you to enter enable mode by entering the privileged command level password. A password must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
succeed	Allows you to enter enable mode without further question.

Command Mode

Global configuration

Usage Guidelines

This secondary authentication is used only if the first attempt fails.

Note This command is not used with TACACS+, which uses the authentication, authorization, and accounting (AAA) suite of commands instead.

Examples

In the following example, if the TACACS servers do not respond to the **enable** command, the user can enable by entering the privileged-level password:

```
Switch(config)# enable last-resort <password>
```

Related Commands

enable

enable use-tacacs

Use the **enable use-tacacs** global configuration command to enable the use of TACACS to determine whether a user can access the privileged command level. Use the **no** form of this command to disable TACACS verification. This command is available only in the Enterprise Edition Software.

enable use-tacacs
no enable use-tacacs

Tips If you use the **enable use-tacacs** command, you must also use the **tacacs-server authenticate enable** command or you will be locked out of the privileged command level.

Syntax Description

This command has no arguments or keywords.

Command Mode

Global configuration

Usage Guidelines

When you add this command to the configuration file, the **enable** privilege EXEC command prompts for a new username and password pair. This pair is then passed to the TACACS server for authentication. If you are using Extended TACACS, it also sends any existing UNIX user identification code to the server.

Note This command initializes TACACS. Use the **tacacs server-extended** command to initialize Extended TACACS or use the **aaa new-model** command to initialize authentication, authorization, and accounting (AAA) and TACACS+.

Examples

The following example sets TACACS verification on the privileged EXEC-level login sequence:

```
Switch(config)# enable use-tacacs
Switch(config)# tacacs-server authenticate enable
```

Related Commands

tacacs-server authenticate enable

exit

Use the **exit** VLAN database command to implement the proposed new VLAN database, increment the database configuration number, propagate it throughout the administrative domain, and return to privileged EXEC mode. This command is available only in the Enterprise Edition Software.

exit

Syntax Description

This command has no arguments or keywords.

Default

No default is defined.

Command Mode

VLAN database

Usage Guidelines

The **exit** command implements all the configuration changes you made since you entered VLAN database mode and uses them for the running configuration. This command returns you to privileged EXEC mode.

Example

The following example shows how to implement the proposed new VLAN database and exit to privileged EXEC mode:

```
Switch(vlan)# exit
Switch#
```

You can verify the previous command by entering the **show vlan brief** command in privileged EXEC mode.

Related Commands

abort
apply
reset
show vlan
shutdown vlan
vlan database

flowcontrol

Use the **flowcontrol** interface configuration command on Gigabit Ethernet ports to control traffic rates during congestion. Use the **no** form of this command to disable flow control on the port.

flowcontrol [**asymmetric** | **symmetric**]

no flowcontrol

Syntax Description

asymmetric	Enable the local port to perform flow control of the remote port. If the local port is congested, it can request the remote port to stop transmitting. When the congestion clears, the local port requests that the remote port begin transmitting.
symmetric	Enable the local port to perform flow control only if the remote port can also perform flow control of the local port. If the remote port cannot perform flow control, the local port also will not.

Default

Asymmetric

Command Mode

Interface configuration

Example

The following example shows how to configure the local port to support any level of flowcontrol by the remote port:

```
Switch(config-if)# flowcontrol
```

The following example shows how to configure the local port to control the flow of traffic from the remote port:

```
Switch(config-if)# flowcontrol asymmetric
```

interface

Use the **interface** global configuration command to configure an interface type and enter interface configuration mode.

interface *type number*

interface *type slot/port* (for ports on an ATM module)

To configure a subinterface, use this form of the interface global configuration commands:

interface *type slot/port.subinterface-number* {**multipoint | point-to-point**}

Syntax Description

type	Type of interface.
slot	Slot number (1 or 2) for ports on an ATM module.
port	Port ID.
.subinterface-number	Subinterface number in the range 1 to 4294967293. The number that precedes the period (.) must match the number to which this subinterface belongs.
multipoint | point-to-point	(Optional) Specifies a multipoint or point-to-point subinterface. There is no default.

Command Mode

Global configuration, VLAN database

Example

The following example shows how to enable loopback mode and assign an IP network address and network mask to the interface. The loopback interface established here will always appear to be up:

```
Switch(config)# interface loopback 0
Switch(config)# ip address 131.108.1.1 255.255.255.0
```

The following example shows how to enable the switch to act on ATM interface 1/2:

```
Switch(vlan)# interface atm 1/2
Switch#
```

Related Commands

circuit
controller
mac-address
ppp
show interfaces
slip

ip address

Use the **ip address** interface configuration command to set an IP address for a switch. Use the **no** form of this command to remove an IP address or disable IP processing.

ip address *ip-address mask*
no ip address *ip-address mask*

Syntax Description

ip-address	IP address.
mask	Mask for the associated IP subnet.

Default

No IP address is defined for the switch.

Command Mode

Interface configuration

Usage Guidelines

A switch can have one IP address.

The IP address of the switch can be accessed only by nodes connected to ports that belong to VLAN 1.

Example

The following example shows how to configure the IP address for the switch on a subnetted network:

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

You can verify the previous commands by entering the **show running-config** command in privileged EXEC mode.

Related Commands

show running-config
clear ip address

login authentication

Use the **login authentication** line configuration command to enable authentication, authorization, and accounting (AAA) for logins. Use the **no** form of this command to either disable TACACS+ authentication for logins or to return to the default.

login authentication {**default** | *list-name*}
no login {**default** | *list-name*}

Syntax Description

default	Use the default list created with the AAA **authentication login** command.
list-name	Use the indicated list created with the AAA **authentication login** command.

Command Mode

Line configuration

Usage Guidelines

To create a default list that is used if **no list** is specified in the **login authentication** command, use the **default** argument followed by the methods you want used in default situations. The default method list is automatically applied to all interfaces.

Example

For example, to specify TACACS as the default method for user authentication during login, enter the following:

```
Switch# login authentication default tacacs
```

Related Commands

enable password
password
username

login

Use the **login** line configuration command to enable password checking at login. Use the **no** form of this command to disable password checking and allow connections without a password.

login [local | tacacs]
no login

Syntax Description

local	(Optional) Selects local password checking. Authentication is based on the username specified with the **username** global configuration command.
tacacs	(Optional) Selects the Terminal Access Controller Access Control System (TACACS)-style user ID and password-checking mechanism.

Default

Virtual terminals require a password. If you do not set a password for a virtual terminal, it responds to attempted connections by displaying an error message and closing the connection.

Command Mode

Line configuration

Usage Guidelines

If you specify the login command without the **local** or **tacacs** option, authentication is based on the password specified with the **password** line configuration command.

Note This command cannot be used with authentication, authorization, and accounting (AAA) and TACACS+. Use the login authentication command instead.

Example

The following example shows how to set the password *letmein* on virtual terminal line 4:

```
Switch(config-line)# line vty 4
Switch(config-line)# password letmein
Switch(config-line)# login
```

The following example shows how to enable the TACACS-style user ID and password-checking mechanism:

```
Switch(config-line)# line 0
Switch(config-line)# password <mypassword>
Switch(config-line)# login tacacs
```

Related Commands

enable password
password
username

login tacacs

Use the **login tacacs** line configuration command to configure your switch to use TACACS authentication. Use the **no** form of this command to disable TACACS user authentication for a line. This command is available only in the Enterprise Edition Software.

login tacacs
no login tacacs

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Line configuration

Usage Guidelines

You can use TACACS security if you have configured a TACACS server and you have a command control language (CCL) script that allows you to use TACACS security. For information about using files provided by Cisco Systems to modify CCL scripts to support TACACS user authentication, refer to the *Access Services Configuration Guide*.

Note This command cannot be used with authentication, authorization, and accounting (AAA) and TACACS+. Use the **login authentication** command instead.

Example

In the following example, lines 1 through 16 are configured for TACACS user authentication:

```
Switch(config-line)# line 1 16
Switch(config-line)# login tacacs
```

mac-address-table aging-time

Use the **mac-address-table aging-time** global configuration command to set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. Use the **no** form of this command to use the default aging-time interval. The aging time applies to all VLANs.

mac-address-table aging-time *age*
no mac-address-table aging-time

Syntax Description

age	Number from 10 to 1000000 (seconds).

Default

The default is 300 seconds.

Command Mode

Global configuration

Usage Guidelines

If hosts do not transmit continuously, increase the aging time to record the dynamic entries for a longer time. This can reduce the possibility of flooding when the hosts transmit again.

Example

The following example shows how to set the aging time to 200 seconds:

```
Switch(config)# mac-address-table aging-time 200
```

You can verify the previous command by entering the **show mac-address-table** command in privileged EXEC mode.

Related Commands

clear mac-address-table
mac-address-table dynamic
mac-address-table secure
port block
show cgmp
show mac-address-table

mac-address-table dynamic

Use the **mac-address-table dynamic** global configuration command to add dynamic addresses to the MAC address table. Dynamic addresses are automatically added to the address table and dropped from it when they are not in use. Use the **no** form of this command to remove dynamic entries from the MAC address table.

mac-address-table dynamic *hw-addr interface* [**atm** *slot/port*] [**vlan** *vlan-id*]
no mac-address-table dynamic *hw-addr* [**vlan** *vlan-id*]

Syntax Description

hw-addr
MAC address added to or removed from the table.

interface
Port to which packets destined for *hw-addr* are forwarded.

atm
(Optional) Add dynamic addresses to ATM module *slot/port*.

slot
Dynamic address is associated with slot (1 or 2) *port*.

port
Add dynamic addresses to this port. The port number is always 0 for ATM interfaces.

vlan
(Optional) The *interface* and *vlan* parameters together specify a destination to which packets destined for *hw-addr* are forwarded.

This keyword is optional if the port is a static-access or dynamic-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address.

Note When this command is executed on a dynamic-access port, queries to the VLAN Membership Policy Server (VMPS) do not occur. The VMPS cannot verify that the address is allowed or determine to which VLAN the port should be assigned. This command should only be used for testing purposes.

This keyword is required for multi-VLAN and trunk ports.

This keyword is required on trunk ports to specify to which VLAN the dynamic address is assigned.

vlan-id
ID of the VLAN to which packets destined for *hw-addr* are forwarded.

Command Mode

Global configuration

Usage Guidelines

If the variable *vlan-id* is omitted and the **no** form of the command is used, the MAC address is removed from all VLANs.

Example

The following example shows how to add a MAC address on port fa1/1 to VLAN 4:

```
Switch(config)# mac-address-table dynamic 00c0.00a0.03fa fa1/1 vlan 4
```

You can verify the previous command by entering the **show mac-address-table** command in privileged EXEC mode.

Related Commands

clear mac-address-table
mac-address-table aging-time
mac-address-table static
show mac-address-table

mac-address-table secure

Use the **mac-address-table secure** global configuration command to add secure addresses to the MAC address table. Use the **no** form of this command to remove secure entries from the MAC address table.

mac-address-table secure *hw-addr interface* [**atm** *slot/port*] [**vlan** *vlan-id*]
no mac-address-table secure *hw-addr* [**vlan** *vlan-id*]

Syntax Description

hw-addr MAC address that is added to the table.

interface Port to which packets destined for *hw-addr* are forwarded.

atm (Optional) Add secure address to ATM module *slot/port*.

slot Secure address is associated with *slot*.

port Add secure address to this port. This is always 0 for ATM interface.

vlan (Optional) The *interface* and **vlan** parameters together specify a destination to which packets destined for *hw-addr* are forwarded.

This keyword is optional if the port is a static-access VLAN port. In this case, the VLAN assigned to the port is assumed to be that of the port associated with the MAC address.

This keyword is required for multi-VLAN and trunk ports.

vlan-id ID of the VLAN to which secure entries are added.

Command Mode

Global configuration

Usage Guidelines

Secure addresses can be assigned only to one port at a time. Therefore, if a secure address table entry for the specified MAC address and VLAN already exists on another port, it is removed from that port and assigned to the specified one.

In Enterprise Edition Software, dynamic-access ports do not support secure addresses.

Example

The following example shows how to add a secure MAC address to VLAN 6 of port fa1/1:

```
Switch(config)# mac-address-table secure 00c0.00a0.03fa fa1/1 vlan 6
```

The following example shows how to add a secure MAC address to ATM port 2/1:

```
Switch(config)# mac-address-table secure 00c0.00a0.03fa atm 2/1
```

You can verify the previous command by entering the **show mac-address-table** command in privileged EXEC mode.

Related Commands

clear mac-address-table
mac-address-table aging-time
mac-address-table dynamic
mac-address-table static
show mac-address-table

mac-address-table static

Use the **mac-address-table static** global configuration command to add static addresses to the MAC address table. Use the **no** form of this command to remove static entries from the MAC address table.

mac-address-table static *hw-addr in-port out-port-list* [**atm** *slot/port*] [**vlan** *vlan-id*]
no mac-address-table static *hw-addr* [**in-port** *in-port*] [**out-port-list** *out-port-list*] [**vlan** *vlan-id*]

Syntax Description

hw-addr MAC address to add to the address table.

in-port Input port from which packets received with a destination address of *hw-addr* are forwarded to the list of ports in the *out-port-list*. The *in-port* must belong to the same VLAN as all the ports in the *out-port-list*.

out-port-list List of ports to which packets received on ports in *in-port* are forwarded. All ports in the list must belong to the same VLAN.

atm (Optional) Add dynamic addresses to ATM module *slot/port*.

slot Dynamic address is associated with slot (1 or 2) *port*.

port Add dynamic addresses to this port. The port number is always 0 for ATM interfaces.

vlan (Optional) The interface and VLAN parameters together specify a destination to which packets destined for the specified MAC address are forwarded.

This keyword is optional if all the ports specified by *in-port* and *out-port-list* are static-access VLAN ports. The VLAN assigned to the ports is assumed.

This keyword is required for multi-VLAN and trunk ports.

Dynamic-access ports cannot be included in static addresses as either the source (in-port) or destination (out-port).

This keyword is required on trunk ports to specify to which VLAN the static address is assigned.

vlan-id ID of the VLAN to which static address entries are forwarded.

Command Mode

Global configuration

Usage Guidelines

When a packet is received on the input port, it is forwarded to the VLAN of each port you specify for the *out-port-list*. Different input ports can have different output-port lists for each static address. Adding a static address already defined as one modifies the port map (*vlan* and *out-port-list*) for the input port specified.

If the variable *vlan-id* is omitted and the **no** form of the command is used, the MAC address is removed from all VLANs.

Traffic from a static address is only accepted from a port defined in the *in-port* variable.

In Enterprise Edition Software, dynamic-access ports cannot be configured as the source or destination port in a static address entry.

Example

The following example adds a static address with port 1 as an input port and ports 2 and 8 of VLAN 4 as output ports:

```
Switch(config)# mac-address-table static c2f3.220a.12f4 fa0/1 fa0/2 fa0/8 vlan 4
```

You can verify the previous command by entering the **show mac-address-table** command in privileged EXEC mode.

Related Commands

clear mac-address-table
mac-address-table aging-time
mac-address-table dynamic
mac-address-table secure
show mac-address-table

ntp access-group

Use the **ntp access-group** global configuration command to control access to the system's Network Time Protocol (NTP) services. Use the **no ntp access-group** command to remove access control to the system's NTP services.

ntp access-group {query-only | serve-only | serve | peer} *access-list-number*
no ntp access-group {query-only | serve-only | serve | peer}

Syntax Description

query-only	Allows only NTP control queries. See RFC 1305 (NTP version 3).
serve-only	Allows only time requests.
serve	Allows time requests and NTP control queries, but does not allow the system to synchronize to the remote system.
peer	Allows time requests and NTP control queries and allows the system to synchronize to the remote system.
access-list-number	Number (1 to 99) of a standard IP access list.

Command Mode

Global configuration

Usage Guidelines

The access group options are scanned in the following order from least restrictive to most restrictive:

1. peer
2. serve
3. serve-only
4. query-only

Access is granted for the first match that is found. If no access groups are specified, all access is granted to all sources. If any access groups are specified, only the specified access is granted. This facility provides minimal security for the time services of the system. However, it can be circumvented by a determined programmer. If tighter security is desired, use the NTP authentication facility.

Examples

In the following example, the system is configured to allow itself to be synchronized by a peer from access list 99.

However, the system restricts access to allow only time requests from access list 42:

```
Switch(config)# ntp access-group peer 99
Switch(config)# ntp access-group serve-only 42
```

Related Commands

access-list

ntp authenticate

Use the **ntp authenticate** global configuration command to enable Network Time Protocol (NTP) authentication. Use the **no** form of this command to disable the feature.

ntp authenticate
no ntp authenticate

Syntax Description

This command has no keywords or arguments.

Default

Authentication is not enabled.

Command Mode

Global configuration

Usage Guidelines

Use this command if you want authentication. If this command is specified, the system will not synchronize to a system unless it carries one of the authentication keys specified in the **ntp trusted-key** command.

Examples

The following example shows how to enable NTP authentication:

```
Switch(config)# ntp authenticate
```

Related Commands

ntp authentication-key
ntp trusted-key

ntp authentication-key

Use the **ntp authentication-key** global configuration command to define an authentication key for Network Time Protocol (NTP). Use the **no** form of this command to remove the authentication key for NTP.

ntp authentication-key *number* **md5** *value*
no ntp authentication-key *number*

Syntax Description

number	Key number (1 to 4294967295)
md5	Use MD5 authentication.
value	Key value (an arbitrary string of up to eight characters, with the exception of control or escape characters)

Default

No authentication key is defined.

Command Mode

Global configuration

Usage Guidelines

Use this command to define authentication keys for use with other NTP commands for greater security.

Examples

The following example sets authentication key 10 to *aNiceKey*:

```
Switch(config)# ntp authentication-key 10 md5 aNiceKey
```

Note When this command is written to NVRAM, the key is encrypted so that it is not displayed when the configuration is viewed.

Related Commands

ntp authenticate
ntp peer
ntp server
ntp trusted-key

ntp broadcast client

Use the **ntp broadcast client** interface configuration command to allow the system to receive NTP broadcast packets on an interface. Use the **no** form of the command to disable this capability.

ntp broadcast client
no ntp broadcast client

Syntax Description

This command has no arguments or keywords.

Default

Broadcast client mode is not enabled.

Command Mode

Interface configuration

Usage Guidelines

Use this command to allow the system to listen to broadcast packets on an interface-by-interface basis.

Examples

In the following example, the router synchronizes to NTP packets broadcasted on interface VLAN1:

```
Switch(config-if)# interface vlan1
Switch(config-if)# ntp broadcast client
```

Related Commands

ntp broadcast
ntp broadcastdelay

ntp broadcastdelay

Use the **ntp broadcastdelay** global configuration command to set the estimated round-trip delay between the IOS software and a Network Time Protocol (NTP) broadcast server. Use the **no** form of this command to revert to the default value.

ntp broadcastdelay *microseconds*
no ntp broadcastdelay

Syntax Description

microseconds	Estimated round-trip time (in microseconds) for NTP broadcasts. The range is from 1 to 999999.

Default

The default is 3000 microseconds.

Command Mode

Global configuration

Usage Guidelines

Use this command when the switch is configured as a broadcast client and the round-trip delay on the network is other than 3000 microseconds.

Examples

In the following example, the estimated round-trip delay between the switch and the broadcast client is set to 5000 microseconds:

```
Switch(config)# ntp broadcastdelay 5000
```

Related Commands

ntp broadcast
ntp broadcast client

ntp broadcast destination

Use the **ntp broadcast destination** interface configuration command to configure an NTP server or peer to restrict broadcast of NTP frames to the IP address of a designated client or a peer.

ntp broadcast destination *IP-address*

Syntax Description

IP-address	IP address of a designated client or a peer.

Command Mode

Interface configuration

Related Commands

ntp broadcast client
ntp broadcastdelay

ntp broadcast key

Use the **ntp broadcast key** interface configuration command to configure an Network Time Protocol (NTP) server or peer to broadcast NTP frames with the authentication key embedded into the NTP packet.

ntp broadcast key

Syntax Description

This command has no arguments.

Command Mode

Interface configuration

Related Commands

ntp broadcast client
ntp broadcastdelay

ntp broadcast version

Use the **ntp broadcast** interface configuration command to specify that a specific interface should send Network Time Protocol (NTP) broadcast packets. Use the **no** form of the command to disable this capability.

ntp broadcast [version *number***]**
no ntp broadcast

Syntax Description

version	(Optional) Indicates the NTP version.
number	Number from 1 to 3.

Default

Version 3 is the default.

Command Mode

Interface configuration

Usage Guidelines

If you are using version 2 and the NTP synchronization does not occur, use NTP version 2.

Examples

In the following example, interface VLAN1 is configured to send NTP version 2 packets:

```
Switch(config-if)# interface vlan1
Switch(config-if)# ntp broadcast version 2
```

Related Commands

ntp broadcast client
ntp broadcastdelay

ntp disable

Use the **ntp disable** interface configuration command to prevent an interface from receiving Network Time Protocol (NTP) packets. To enable receipt of NTP packets on an interface, use the **no ntp disable** command.

ntp disable
no ntp disable

Syntax Description

This command has no arguments or keywords.

Command Mode

Interface configuration

Examples

In the following example, interface VLAN1 is prevented from receiving NTP packets:

```
Switch(config-if)# interface vlan1
Switch(config-if)# ntp disable
```

ntp clock-period

Do not enter this command; it is documented for informational purposes only. The system automatically generates this command as Network Time Protocol (NTP) determines the clock error and compensates.

As NTP compensates for the error in the system clock, it keeps track of the correction factor for this error. The system automatically saves this value into the system configuration using the **ntp clock-period** global configuration command. The system uses the **no** form of this command to revert to the default.

ntp clock-period *value*
no ntp clock-period

Syntax Description

value	Amount to add to the system clock for each clock hardware tick (in units of 2 to 32 seconds).

Command Mode

Global configuration

Usage Guidelines

If a **write memory** command is entered to save the configuration to nonvolatile RAM (NVRAM), this command will automatically be added to the configuration. It is a good idea to perform this task after NTP has been running for a week or so; NTP will synchronize more quickly if the system is restarted.

ntp max-associations

Use the **ntp max-associations** global configuration command to set the maximum number of Network Time Protocol (NTP) associations that are allowed on a server. Use the **no** form of this command to disable this feature.

ntp max-associations [*number*]

no ntp max-associations

Syntax Description

number	Specifies the number of NTP associations. The range is 0 through 4294967295.

Command Mode

Global configuration

Usage Guidelines

This command provides a simple method to control the number of peers that can use the switch to synchronize to it through NTP.

After you enable a switch as NTP, use this command to set the maximum number of associations that are allowed on a server.

Examples

The following example shows how to set the maximum number of NTP associations to 44:

```
Switch(config)# ntp max-associations 44
```

ntp peer

Use the **ntp peer** global configuration command to configure the switch's system clock to synchronize a peer or to be synchronized by a peer. Use the **no ntp peer** command to disable this capability.

ntp peer *ip-address* **[version** *number***] [key** *keyid***] [source** *interface***] [prefer]**
no ntp peer *ip-address*

Syntax Description

ip-address	IP address of the peer providing, or being provided, the clock synchronization.
version	(Optional) Defines the Network Time Protocol (NTP) version number.
number	(Optional) NTP version number (1 to 3).
key	(Optional) Defines the authentication key.
keyid	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Authentication key to use when sending packets to this peer.
interface	(Optional) Name of the interface from which to pick the IP source address.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization.

Command Mode

Global configuration

Usage Guidelines

Using the **prefer** keyword will reduce switching between peers.

If you are using the default NTP version of 3 and NTP synchronization does not occur, try using NTP version 2. Many NTP servers on the Internet run version 2.

Examples

In the following example, the router is configured to allow its system clock to be synchronized with the clock of the peer (or vice versa) at IP address 131.108.22.33 using NTP version 2. The source IP address will be the address of Ethernet 0.

```
Switch(config)# ntp peer 131.108.22.33 version 2 source Ethernet 0
```

Related Commands

ntp authentication-key
ntp server
ntp source

ntp server

Use the **ntp server** global configuration command to allow the switch’s system clock to be synchronized by a time server. Use the **no ntp server** command to disable this capability.

ntp server *ip-address* **[version** *number***] [key** *keyid***] [source** *interface***] [prefer]**
no ntp server *ip-address*

Syntax Description

ip-address	IP address of the time server providing the clock synchronization.
version	(Optional) Defines the Network Time Protocol (NTP) version number.
number	(Optional) NTP version number (1 to 3).
key	(Optional) Defines the authentication key.
keyid	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Identifies the interface from which to pick the IP source address.
interface	(Optional) Name of the interface from which to pick the IP source address.
prefer	(Optional) Makes this server the preferred server that provides synchronization.

Command Mode

Global configuration

Usage Guidelines

Use this command if you want to allow this machine to synchronize with the specified server. The server will not synchronize to this machine.

Using the **prefer** keyword will reduce switching between servers.

If you are using the default NTP version of 3 and NTP synchronization does not occur, try using NTP version 2. Many NTP servers on the Internet run version 2.

Examples

In the following example, the router is configured to allow its system clock to be synchronized with the clock of the peer at IP address 128.108.22.44 using NTP version 2:

```
Switch(config)# ntp server 128.108.22.44 version 2
```

Related Commands

ntp authentication-key
ntp peer
ntp source

ntp source

Use the **ntp source** global configuration command to use a particular source address in Network Time Protocol (NTP) packets. Use the **no** form of this command to remove the specified source address.

ntp source *interface*
no ntp source

Syntax Description

interface	Any valid system interface name.

Command Mode

Global configuration

Usage Guidelines

Use this command when you want to use a particular source IP address for all NTP packets. The address is taken from the specified interface. This command is useful if the address on an interface cannot be used as the destination for reply packets. If the **source** keyword is present on an **ntp server** or **ntp peer** command, that value overrides the global value.

Examples

In the following example, the router is configured to use the IP address of VLAN1 as the source address of all outgoing NTP packets:

```
Switch(config)# ntp source vlan1
```

Related Commands

ntp peer
ntp server

ntp trusted-key

Use the **ntp trusted-key** global configuration command if you want to authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize. Use the **no** form of this command to disable authentication of the identity of the system.

ntp trusted-key *key-number*
no ntp trusted-key *key-number*

Syntax Description

key-number	Number of authentication key to be allowed.

Command Mode

Global configuration

Usage Guidelines

If authentication is enabled, use this command to define one or more key numbers that a peer NTP system must provide in its NTP packets, in order for this system to synchronize to it. The key numbers must correspond to the keys defined with the **ntp authentication-key** command. This provides protection against accidentally synchronizing the system to a system that is not allowed, since the other system must know the correct authentication key.

Examples

In the following example, the system is configured to synchronize only to systems providing authentication key 42 in its NTP packets:

```
Switch(config)# ntp authenticate
Switch(config)# ntp authentication-key 42 md5 aNiceKey
Switch(config)# ntp trusted-key 42
```

Related Commands

ntp authenticate
ntp authentication-key

port block

Use the **port block** interface configuration command to block the flooding of unknown unicast or multicast packets to a port. Use the **no** form of this command to resume normal forwarding.

port block {**unicast** | **multicast**}
no port block {**unicast** | **multicast**}

Syntax Description

unicast	Packets with unknown unicast addresses are not forwarded to this port.
multicast	Packets with unknown multicast addresses are not forwarded to this port.

Default

Flood unknown unicast and multicast packets to all ports.

Command Mode

Interface configuration

Usage Guidelines

The **port block** command cannot be entered for a network port.

In Enterprise Edition Software, if a trunk port is not a network port, the **unicast** keyword applies. The **multicast** keyword is supported on trunk ports. Both port block features affect all the VLANs associated with the trunk port.

Example

The following example shows how to block the forwarding of multicast and unicast packets to a port:

```
Switch(config-if)# port block unicast
Switch(config-if)# port block multicast
```

You can verify the previous commands by entering the **show port block** command in privileged EXEC mode.

Related Commands

show port block

port group

Use the **port group** interface configuration command to assign a port to a Fast EtherChannel or Gigabit EtherChannel port group. Up to 12 port groups can be created on a switch. Any number of ports can belong to a destination-based port group. Up to eight ports can belong to a source-based port group. Use the **no** form of this command to remove a port from a port group.

port group *group-number* [**distribution** {**source** | **destination**}]
no port group

Syntax Description

group-number	Port group number to which the port belongs. A number from 1 to 12 is valid.
distribution	(Optional) Forwarding method for the port group.
source	Set the port to forward traffic to a port group based on the packet source address. This is the default forwarding method.
destination	Set the port to forward traffic to a port group based on the packet destination address.

Defaults

Port does not belong to a port group.

The default forwarding method is source.

Command Mode

Interface configuration

Usage Guidelines

An ATM port is the only port that *cannot* belong to a port group. For all other ports, the following restrictions apply:

- Do not group Fast Ethernet (FE) and gigabit ports together.
- No port group member can be configured for Switched Port Analyzer (SPAN) port monitoring.
- No port group member can be enabled for port security.
- You can create up to 12 port groups of all source-based, all destination-based, or a combination of source-based and destination-based port groups. A source-based port group can have up to eight ports in its group. A destination-based port group can contain an unlimited number of ports in its group. You cannot mix source-based and destination-based ports in the same group.
- Port group members must belong to the same set of VLANs and must be all static-access, all multi-VLAN, or all trunk ports (Enterprise Edition Software only).
- In Enterprise Edition Software, dynamic-access ports cannot be grouped with any other port, not even with other dynamic-access ports.

When a group is first formed, the switch automatically sets the following parameters to be the same on all ports:

- VLAN membership of ports in the group
- VLAN mode (static, multi, trunk) of ports in the group

- Encapsulation method of the trunk
- Native VLAN configuration if the trunk uses IEEE 802.1Q
- Allowed VLAN list configuration of the trunk port (Enterprise Edition Software only)
- Spanning-Tree Protocol (STP) Port Fast
- STP port priority
- STP path cost
- Network port configuration for source-based port group

Configuration of the first port added to the group is used when setting the above parameters for other ports in the group. After a group is formed, changing any parameter in the above list changes the parameter on all other ports.

Use the distribution parameter to customize the port group to your particular environment. The forwarding method you choose depends on how your network is configured. However, source-based forwarding works best for most network configurations.

This command is not supported on the ATM modules.

Examples

The following example shows how to add a port to a port group using the default source-based forwarding:

```
Switch(config-if)# port group 1
```

The following example shows how to add a port to a group using destination-based forwarding:

```
Switch(config-if)# port group 2 distribution destination
```

You can verify the previous commands by entering the **show port group** command in privileged EXEC mode.

Related Commands

show port group

port monitor

Use the **port monitor** interface configuration command to enable Switched Port Analyzer (SPAN) port monitoring on a port. Use the **no** form of this command to return the port to its default value.

port monitor [**interface** *interface*]
no port monitor [*interface*]

Syntax Description

interface	Type of interface.
interface	(Optional) Module and port number for the SPAN to be enabled.

Default

Port does not monitor any other ports.

Command Mode

Interface configuration

Usage Guidelines

Enabling port monitoring without specifying a port causes all other ports in the same VLAN to be monitored.

ATM ports are the only ports that *cannot* be monitor ports. However, you can monitor ATM ports. The following restrictions apply for ports that have port-monitoring capability:

- A monitor port cannot be in a Fast EtherChannel or Gigabit EtherChannel port group.
- A monitor port cannot be enabled for port security.
- A monitor port cannot be a multi-VLAN port.
- A monitor port must be a member of the same VLAN as the port monitored. VLAN membership changes are disallowed on monitor ports and ports being monitored.
- In Enterprise Edition Software, a monitor port cannot be a dynamic-access port or a trunk port. However, a static-access port can monitor a VLAN on a trunk port, a multi-VLAN port, or a dynamic-access port. The VLAN monitored is the one associated with the static-access port.

Example

The following example shows how to enable port monitoring on port fa0/2:

```
Switch(config-if)# port monitor fa0/2
```

You can verify the previous command by entering the **show port monitor** command in privileged EXEC mode.

Related Commands

show port monitor

port network

Use the **port network** interface configuration command to define a port as the switch network port. All traffic with unknown unicast addresses is forwarded to the network port on the same VLAN. Use the **no** form of this command to return the port to the default value.

port network
no port network

Syntax Description

This command has no arguments or keywords.

Default

No network port is defined.

Command Mode

Interface configuration

Usage Guidelines

The following restrictions apply to network ports:

- A network port can be a static-access port, a multi-VLAN port, a port group, and/or a trunk port (Enterprise Edition Software only). Both the multi-VLAN port and the trunk port become the network port for all the VLANs associated with that port.
- A network port cannot be an ATM port, a secure port, a monitor port, or a dynamic-access port (Enterprise Edition Software only). You can assign a dynamic-access port to a VLAN in which another port is the network port.
- Each VLAN can have one network port.
- A network port cannot be in a destination-based port group.
- A network port cannot be on an ATM module.

Example

The following example shows how to set a port as a network port.

```
Switch(config-if)# port network
```

You can verify the previous command by entering the **show port network** command in privileged EXEC mode.

Related Commands

show port network

port security

Use the **port security** interface configuration command to enable port security on a port. Use the **no** form of this command to return the port to its default value.

port security [**action** {**shutdown** | **trap**}]
port security [**max-mac-count** *addresses*]
no port security

Syntax Description

action	(Optional) Action to take when an address violation occurs on this port.
shutdown	Disable the port when a security violation occurs.
trap	Generate an SNMP trap when a security violation occurs.
max-mac-count	(Optional) Maximum number of secure addresses that this port can support.
addresses	Number from 1 to 132.

Defaults

Port security is disabled.

When enabled, the default action is to generate an SNMP trap.

Command Mode

Interface configuration

Usage Guidelines

If you specify **trap**, use the **snmp-server host** command to configure the SNMP trap host to receive traps.

The following restrictions apply to secure ports:

- A secure port cannot belong to a Fast EtherChannel or Gigabit EtherChannel port group.
- A secure port cannot have Switched Port Analyzer (SPAN) port monitoring enabled on it.
- A secure port cannot be a multi-VLAN port.
- A secure port cannot be a network port.
- A secure port cannot be an ATM port.
- In Enterprise Edition Software, a secure port cannot be a dynamic-access port or a trunk port.

Examples

The following example shows how to enable port security and what action the port takes in case of an address violation (shutdown).

```
Switch(config-if)# port security action shutdown
```

The following example shows how to set the maximum number of addresses that the port can learn to 8.

```
Switch(config-if)# port security max-mac-count 8
```

You can verify the previous commands by entering the **show port security** command in privileged EXEC mode.

Related Commands

show port security

port storm-control

Use the **port storm-control** interface configuration command to enable broadcast-storm control on a port. Use the **no** form of this command to disable storm control or one of the storm-control parameters on the port.

port storm-control {**filter** | **trap** | **threshold** {**rising** *rising-number* **falling** *falling-number*}}
no port storm-control {**filter** | **trap** | **threshold**}

Syntax Description

filter	(Optional) Disable the port during a broadcast storm.
trap	(Optional) Generate an SNMP trap when the traffic on the port crosses the rising or falling threshold.
threshold	(Optional) Rising and falling threshold values to follow.
rising	Block the normal flooding of broadcast packets when the value specified for *rising-number* is reached.
rising-number	0 to 4294967295 broadcast packets per second.
falling	Restart the normal flooding of broadcast packets when the value specified for *falling-number* is reached.
falling-number	0 to 4294967295 broadcast packets per second.

Default

Broadcast storm control is not enabled.

Command Mode

Interface configuration

Example

The following example shows how to enable broadcast storm control on a port. In this example, flooding is inhibited when the number of broadcast packets arriving on the port reaches 1000 and is restarted when the number returns to 200.

```
Switch(config-if)# port storm-control threshold rising 1000 falling 200
```

You can verify the previous command by entering the **show port storm-control** command in privileged EXEC mode.

Related Commands

show port storm-control

rcommand

Use the **rcommand** user EXEC command to execute commands on a member switch from the command switch. If the user is executing on the cluster command switch at user-level, the **rcommand** command accesses the remote device at user level. If you use this command on the cluster command switch at privileged-level, the command accesses the remote device at privileged-level. If you use an intermediate enable level lower than *privileged*, access to the member switch is at user level.

rcommand *n* | **mac-address** *hw-addr* | *commander*

Syntax Description

n	Provide the number that identifies a cluster member.
mac-address	Provide the MAC address for the cluster member.
hw-addr	Mac address of the member's command switch.
commander	(Optional) Provide the name of the command switch.

Command Mode

User EXEC

Usage Guidelines

If the switch is the cluster command switch but the member switch *n* does not exist, an error message appears.

You can use this command to access a member switch from the command switch prompt or access a command switch from the member switch prompt. You will have the same access level for all switches when you use this command to access other switches.

This command will not work if the vty lines of the command switch have access-class configurations.

Example

Following is an example of the **rcommand** command without another command as a parameter. All subsequent commands will be directed to the specified member switch until you enter the **exit** command or close the session.

```
switch> rcommand 3
switch> show version
Cisco Internet Operating System Software ...
...
switch# exit
switch#
```

Related Commands

show cluster member
cluster

reset

Use the **reset** VLAN database command to abandon the proposed VLAN database and remain in VLAN database mode. This command resets the proposed database to the currently implemented VLAN database on the switch. This command is available only in the Enterprise Edition Software.

reset

Syntax Description

This command has no arguments or keywords.

Default

No default is defined.

Command Mode

VLAN database

Example

The following example shows how to abandon the proposed VLAN database and reset to the current VLAN database:

```
Switch(vlan)# reset
Switch(vlan)#
```

You can verify the previous command by entering the **show changes** and **show proposed** commands in VLAN database mode.

Related Commands

abort
apply
exit
show changes
show proposed
shutdown vlan
vlan database

session

Use the **session** privileged EXEC command to log into the ATM module operating system and start a command-line interface (CLI) session. Enter the **exit** command or **Ctrl-G** to return to the switch command-line interface.

session *number*

Syntax Description

number	Slot number (1 or 2).

Command Mode

Privileged EXEC

Examples

The following example shows how to log into the ATM module number 1:

```
Switch# session 1
```

show cgmp

Use the **show cgmp** privileged EXEC command to display the current state of the CGMP-learned multicast groups and routers.

show cgmp [**state** | **holdtime** | [**vlan** *vlan-id*] | [**group** [*address*] | **router** [*address*]]]

Syntax Description

state (Optional) Display whether CGMP is enabled or not, whether Fast Leave is enabled or not, and the router port timeout value.

holdtime (Optional) Display the router port timeout value in seconds.

vlan (Optional) Limit the display to the specified VLAN.

vlan-id ID of VLAN to which the command applies.

group (Optional) Display all known multicast groups and the destination ports. Limited to given VLAN if **vlan** keyword is entered; limited to a specific group if the *address* parameter is entered.

address MAC address of the group or router.

router (Optional) Display all routers, their ports, and expiration times. Limited to given VLAN if **vlan** keyword entered; limited to a specific router if the *address* parameter is entered.

Command Mode

Privileged EXEC

Usage Guidelines

This command displays CGMP information about known routers and groups, as well as whether CGMP is enabled, whether Fast Leave is enabled, and the current value of the router timeout. If **show cgmp** is entered with no arguments, all information is displayed.

Sample Display

The following is sample output from the **show cgmp** command.

```
Switch# show cgmp

CGMP is running.
CGMP Fast Leave is not running.
Default router timeout is 300 sec.


vLAN     IGMP MAC Address   Interfaces
------  -----------------   -----------
    1    0100.5e01.0203      Fa0/8
    1    0100.5e00.0128      Fa0/8


vLAN     IGMP Router        Expire   Interface
------  -----------------  --------  ----------
    1    0060.5cf3.d1b3     197 sec   Fa0/8
```

Related Commands

cgmp
clear cgmp

show changes

Use the **show changes** VLAN database command to display the differences between the VLAN database currently on the switch and the proposed VLAN database. You can also display the differences between the two for a selected VLAN. This command is available only in the Enterprise Edition Software.

show changes [*vlan-id*]

Syntax Description

vlan-id (Optional) ID of the VLAN in the current or proposed database. If this variable is omitted, all the differences between the two VLAN databases are displayed, including the pruning state and V2 mode. Valid IDs are from 1 to 1005.

Command Mode

VLAN database

Sample Displays

The following is sample output from the **show changes** command. It displays the differences between the current and proposed databases.

```
Switch(vlan)# show changes

DELETED:
  VLAN ISL Id: 4
    Name: VLAN0004
    Media Type: Ethernet
    VLAN 802.10 Id: 100004
    State: Operational
    MTU: 1500

DELETED:
  VLAN ISL Id: 6
    Name: VLAN0006
    Media Type: Ethernet
    VLAN 802.10 Id: 100006
    State: Operational
    MTU: 1500

MODIFIED:
  VLAN ISL Id: 7
    Current State: Operational
    Modified State: Suspended
```

The following is sample output from the **show changes 7** command. It displays the differences between VLAN 7 in the current database and the proposed database.

```
Switch(vlan)# show changes 7

MODIFIED:
  VLAN ISL Id: 7
    Current State: Operational
    Modified State: Suspended
```

Related Commands

show current
show proposed

show cluster

Use the **show cluster** user EXEC command to show a status summary of the cluster to which the switch belongs.

show cluster

Syntax Description

This command has no arguments or keywords.

Command Mode

User EXEC

Usage Guidelines

You can use this command to determine whether the switch is a command switch, member switch, candidate switch, or edge device. This command displays the following information:

- IP and MAC address of the command switch
- Cluster-member number of the switch
- State of connectivity of the member switches
- Cluster name

If a member switch cannot find its command switch, it displays any information that is available to it. Its cluster-member number is unknown.

Example

The following example shows this command being used on the command switch:

```
Tahiti-24> show cluster
Command device for cluster "default_cluster", contains 6 members.
Member state: 0 members are unreachable
Time since last status change: 5 days, 17 hours, 45 minutes
```

The following example shows this command being used on a member switch:

```
Tahiti-12> show cluster
Cluster member 5
Cluster name: default_cluster
Management ip address:  172.20.128.27
Command device mac address: 0050.5494.3c40
```

The following example shows this command being used on the command switch that is separated from member 1:

```
Tahiti-24> show cluster
Command device for cluster "default_cluster", contains 6 members.
Member state: 1 members are unreachable
Time since last status change: 5 days, 17 hours, 45 minutes
```

The following example shows this command being used on a member switch that is separated from the command switch:

```
Tahiti-12> show cluster
Cluster member <unknown>
Cluster name: default_cluster
Management ip address:  172.20.128.27
Command device mac address: 0050.5494.3c40
```

The following example shows this command being used on a member switch that is separated from the command switch and then restarted:

```
Tahiti-12> show cluster
Cluster member <unknown>
Cluster name: default_cluster
Management ip address:  172.20.128.27
Command device mac address: 0050.5494.3c40
```

Related Commands

show cluster candidates
show cluster view
show cluster members
cluster
cluster enable

show cluster candidates

Use the **show cluster candidates** user EXEC command to get a list of candidate switches. This command is available only in command-switch enabled software.

show cluster candidates [**mac-address** *hw-addr*]]

Syntax Description

mac-address Get detailed information about the specified candidate.

hw-addr MAC address for the cluster candidate.

Command Mode

User EXEC

Usage Guidelines

You can only use this command on a command switch.

This command shows a list of all cluster candidates that are one hop away from a current cluster member, and are not active members of another cluster.

Example

Following is a sample output of the **show cluster candidates** command:

```
Switch> show cluster candidates
                                                             |---Upstream---|
MAC Address    Name         Device Type      PortIf  FEC Hops SN PortIf  FEC
0050.0f08.91c0 murali-99.ci WS-C2924-XL      Fa0/1        1   0  Fa0/9
0050.0f08.a500 murali-222.c WS-C2912MF-XL    Fa0/1        1   0  Fa0/23
0050.50be.b2c0 4meg-switch  WS-C2924-XL      Fa0/1        1   0  Fa0/7

Switch> show cluster candidates mac-address 0050.0f08.91c0
Device cisco WS-C2924-XL with mac address:0050.0f08.91c0 connects to Member 0
        Candidate port Fa0/1, connects to member port Fa0/9
        Candidate is 1 hops from the command device.
Switch>
```

Related Commands

show cluster
show cluster view
show cluster members
cluster

show cluster members

Use the **show cluster members** user EXEC command to display information about the cluster members. Use the **no** form of this command to disable the command switch.

show cluster members [*n*]

Syntax Description

n	(Optional) Number that identifies a cluster member. The cluster command switch is member number 0.

Command Mode

User EXEC

Usage Guidelines

You must enter this command from the command switch.

Example

Following is a sample output of the **show cluster members** command:

```
Tahiti-24> show cluster members
                                                |---Upstream---|
SN MAC Address    Name         PortIf FEC Hops   SN PortIf  FEC  State
0  0050.5494.3c40 Tahiti-24                0                     Cmdr
3  00e0.1e9f.8300 Balboa       Gi2/1       2     4  Gi0/7        Up
4  0050.5494.34ff Wailea       Gi0/6       1     0  Gi0/1        Up
5  0050.5494.2ac0 Tahiti-12    Gi0/1       1     0  Gi0/2        Up
6  00e0.1e9f.7a00 Surfers-24   Fa0/5       1     0  Fa0/3        Up
7  0010.7bb6.1cc0 Ventura      Fa2/1       3     3  Fa0/24       Up

Tahiti-24> show cluster member 3
Member Number: 3        Name: es3       State: Up
        Device: cisco WS-C2924M-XL
        FEC Number:     Mac Address: 00e0.1e9f.8300
        Link port: Gi2/1        Hops to command device: 2
Connected to member number 4
        Mac address: 0050.5494.34ff     Link port: Gi0/7
```

Related Commands

cluster member
show cluster
show cluster candidates
show cluster view

show cluster view

Use the **show cluster view** command to show all current members of and candidates for neighbors of the cluster.

show cluster view

Syntax Description

This command has no arguments.

Command Mode

User EXEC

Example

Following is a sample output of the **show cluster view** command:

```
Tahiti-24> show cluster view
                                                                |---Upstream---|
SN MAC Address    Name         Device Type      PortIf  FEC Hops SN PortIf  FEC
0  0050.5494.3c40 Tahiti-24    WS-C3524-XL                   0
3  00e0.1e9f.8300 Balboa       WS-C2924M-XL     Gi2/1        2   4  Gi0/7
4  0050.5494.34ff Wailea       WS-C3508G-XL     Gi0/6        1   0  Gi0/1
5  0050.5494.2ac0 Tahiti-12    WS-C3512-XL      Gi0/2        2   4  Gi0/8
6  00e0.1e9f.7a00 Surfers-24   WS-C2924-XL      Fa0/5        1   0  Fa0/3
7  0010.7bb6.1cc0 Ventura      WS-C2912MF-XL    Fa2/1        3   3  Fa0/24
   0010.0de0.75d4 zuma-alpha-2 WS-C2924-XL      Fa0/20       1   0  Fa0/24
   00e0.1e9f.8c00 Tahiti-24-2  WS-C2912-XL      Fa0/4        1   0  Fa0/7
   00e0.1e9f.8c40 Surfers-12-1 WS-C2912-XL      Fa0/1        1   0  Fa0/9
```

Related Commands

show cluster candidates

show current

Use the **show current** VLAN database command to display the current VLAN database on the switch or a selected VLAN from it. This command is available only in the Enterprise Edition Software.

show current [*vlan-id*]

Syntax Description

vlan-id	(Optional) ID of the VLAN in the current database. If this variable is omitted, the entire VLAN database displays, included the pruning state and V2 mode. Valid IDs are from 1 to 1005.

Command Mode

VLAN database

Sample Displays

The following is sample output from the **show current** command. It displays the current VLAN database.

```
Switch(vlan)# show current

VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 2
    Name: VLAN0002
    Media Type: Ethernet
    VLAN 802.10 Id: 100002
    State: Operational
    MTU: 1500

  VLAN ISL Id: 3
    Name: VLAN0003
    Media Type: Ethernet
    VLAN 802.10 Id: 100003
    State: Operational
    MTU: 4000

VLAN ISL Id: 4
    Name: VLAN0004
    Media Type: Ethernet
    VLAN 802.10 Id: 100004
    State: Operational
    MTU: 1500

  VLAN ISL Id: 5
    Name: VLAN0005
    Media Type: Ethernet
    VLAN 802.10 Id: 100005
    State: Operational
    MTU: 1500

  VLAN ISL Id: 6
    Name: VLAN0006
    Media Type: Ethernet
    VLAN 802.10 Id: 100006
    State: Operational
    MTU: 1500
```

The following is sample output from the **show current 2** command. It displays only VLAN 2 of the current database.

```
Switch(vlan)# show current 2

VLAN ISL Id: 2
    Name: VLAN0002
    Media Type: Ethernet
    VLAN 802.10 Id: 100002
    State: Operational
    MTU: 1500
```

Related Commands

show changes
show proposed

show file systems

Use the **show file systems** privileged EXEC command to show file system information.

show file systems

Syntax Description

The command has no arguments.

Command Mode

Privileged EXEC

Example

The following is sample output from the **show file systems** command:

```
System# show file systems

File Systems:

Size(b)     Free(b)      Type  Flags  Prefixes
     -           -     opaque     rw  null:
     -           -     opaque     rw  system:
     -           -     opaque     ro  xmodem:
     -           -        rcp     rw  rcp:
     -           -       tftp     rw  tftp:
3612672     1507328     flash     rw  flash:
3612672     1507328   unknown     rw  zflash:
     -           -     opaque     rw  bs:
```

show interface

Use the **show interface** privileged EXEC mode command to display the administrative and operational status of a switching (nonrouting) port.

show interface *interface-id* [**switchport** [**allowed-vlan** | **prune-elig**]]

Syntax Description

interface-id	ID of the module and port number.
switchport	(Optional) Display the administrative and operational status of a switching (nonrouting) port.
allowed-vlan	(Optional) Display the VLAN IDs that receive and transmit all types of traffic on the trunk port. By default, all VLAN IDs are included.
prune-elig	(Optional) Display the VLAN ID whose flood traffic can be pruned. VLAN 1 and VLANs 1002 through 1005 are not eligible for pruning. By default, no VLANs are pruning eligible on the trunk.

Command Mode

Privileged EXEC

Sample Display

The following is sample output from the **show interface fa0/2 switchport** command. Table 2-1 describes each field in the display.

```
Switch# show interface fa0/2 switchport
Name: fa0/2
Switchport: Enabled
Administrative Mode: Static Access
Operational Mode: Static Access
Administrative Trunking Encapsulation: ISL
Operational Trunking Encapsulation: ISL
Negotiation of Trunking: Disabled
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1-30, 50, 100-1005
Pruning VLANs Enabled: NONE
```

Table 2-1 Show Interface Ethernet2/2 Switchport Field Descriptions

Field	Description
Name	Displays the port name.
Switchport	Displays the administrative and operational status of the port. In this display, the port is in switchport mode.
Administrative Mode Operational Mode	Displays the administrative and operational mode.

Table 2-1 Show Interface Ethernet2/2 Switchport Field Descriptions (continued)

Field	Description
Administrative Trunking Encapsulation Operation Trunking Encapsulation Negotiation of Trunking	Displays the administrative and operational encapsulation method. Also displays whether trunking negotiation is enabled.
Access Mode VLAN	VLAN ID.
Trunking Native Mode Trunking VLANs Enabled Trunking VLANs Active	Lists the VLAN ID of the trunk that is in native mode. Lists the active VLANs on the trunk.
Pruning VLANs Enabled	Lists the VLANs that are pruning eligible.

Related Commands

switchport access
switchport mode
switchport multi
switchport trunk

show mac-address-table

Use the **show mac-address-table** privileged EXEC command to display the MAC address table.

show mac-address-table [**static** | **dynamic** | **secure** | **self** | **aging-time** | **count**]
[**address** *hw-addr*] [**interface** *interface*] [**atm** *slot/port*][**vlan** *vlan-id*]

Syntax Description

static	(Optional) Display only the static addresses.
dynamic	(Optional) Display only the dynamic addresses.
secure	(Optional) Display only the secure addresses.
self	(Optional) Display only addresses added by the switch itself.
aging-time	(Optional) Display aging-time for dynamic addresses for all VLANs.
count	(Optional) Display a count for different kinds of MAC addresses.
address	(Optional) Display information for a specific address.
hw-addr	Display information for this address.
interface	(Optional) Display addresses for a specific port.
interface	Display addresses for this port.
atm	(Optional) Add dynamic addresses to ATM module *slot/port*.
slot	Dynamic address is associated with slot (1 or 2) *port*.
port	Add dynamic addresses to this port. The port number is always 0 for ATM interfaces.
vlan	(Optional) Display addresses for a specific VLAN.
vlan-id	Display addresses for this VLAN.

Command Mode

Privileged EXEC

Usage Guidelines

This command displays the MAC address table for the switch. Specific views can be defined by using the optional keywords and values. If more than one optional keyword is used, then all of the conditions must be true in order for that entry to be displayed.

Sample Display

The following is sample output from the **show mac-address-table** command:

```
Switch# show mac-address-table

Dynamic Addresses Count:               9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:           41
Total MAC addresses:                   50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0010.0de0.e289       Dynamic          1  FastEthernet0/1
0010.7b00.1540       Dynamic          2  FastEthernet0/5
0010.7b00.1545       Dynamic          2  FastEthernet0/5
0060.5cf4.0076       Dynamic          1  FastEthernet0/1
0060.5cf4.0077       Dynamic          1  FastEthernet0/1
0060.5cf4.1315       Dynamic          1  FastEthernet0/1
0060.70cb.f301       Dynamic          1  FastEthernet0/1
00e0.1e42.9978       Dynamic          1  FastEthernet0/1
00e0.1e9f.3900       Dynamic          1  FastEthernet0/1
```

Related Commands

clear mac-address-table

show ntp associations

Use the **show ntp associations** privileged EXEC command to show the status of Network Time Protocol (NTP) associations.

show ntp associations [**detail**]

Syntax Description

detail	(Optional) Shows detailed information about each NTP association.

Command Mode

Privileged EXEC

Examples

Detailed descriptions of the information displayed by this command can be found in the NTP specification (RFC 1305).

The following is sample output from the **show ntp associations** command:

```
Switch# show ntp associations
     address         ref clock     st  when  poll reach  delay  offset    disp
 ~160.89.32.2      160.89.32.1       5    29  1024  377     4.2   -8.59     1.6
+~131.108.13.33    131.108.1.111     3    69   128  377     4.1    3.48     2.3
*~131.108.13.57    131.108.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
Switch#
```

show ntp status

Use the **show ntp status** EXEC command to show the status of Network Time Protocol (NTP).

show ntp status

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Usage Guidelines

This command deletes entries from the global MAC address table. Specific subsets can be deleted by using the optional keywords and values. If more than one optional keyword is used, all of the conditions in the argument must be true for that entry to be deleted.

Examples

The following is sample output from the **show ntp status** command:

```
Switch# show ntp status
Clock is synchronized, stratum 4, reference is 131.108.13.57
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is AFE2525E.70597B34 (00:10:22.438 PDT Mon Jul 5 1993)
clock offset is 7.33 msec, root delay is 133.36 msec
root dispersion is 126.28 msec, peer dispersion is 5.98 msec
Switch#
```

show port block

Use the **show port block** privileged EXEC command to display the blocking of unicast or multicast flooding to a port.

show port block {**unicast** | **multicast**} [*interface*]

Syntax Description

unicast	Display whether or not ports are blocking unicast packets.
multicast	Display whether or not ports are blocking multicast packets.
interface	(Optional) Display whether the port specified is blocking unicast or multicast packets.

Command Mode

Privileged EXEC

Usage Guidelines

If the variable *interface* is omitted, the **show port block unicast** and **show port block multicast** commands display packet blocking information on all ports.

Sample Display

The following is sample output from the **show port block** command:

```
Switch# show port block unicast fa0/8

FastEthernet0/8 is blocked from unknown unicast addresses
```

Related Commands

port block

show port group

Use the **show port group** privileged EXEC command to list the ports that belong to a port group.

show port group [*group-number*]

Syntax Description

group-number	(Optional) Port group to which the port is assigned.

Command Mode

Privileged EXEC

Usage Guidelines

If the variable *group-number* is omitted, the **show port group** command displays all port groups on the switch.

Sample Display

The following is sample output from the **show port group** command:

```
Switch# show port group 1

Group  Interface
-----  ---------------
    1  FastEthernet0/1
    1  FastEthernet0/4
```

Related Commands

port group

show port monitor

Use the **show port monitor** privileged EXEC command to display the ports for which Switched Port Analyzer (SPAN) port monitoring is enabled.

show port monitor [*interface*]

Syntax Description

interface	(Optional) Module and port number enabled for SPAN.

Command Mode

Privileged EXEC

Usage Guidelines

If the variable *interface* is omitted, the **show port monitor** command displays all monitor ports on the switch.

Sample Display

The following is sample output from the **show port monitor** command:

```
Switch# show port monitor fa0/8

Monitor Port        Port Being Monitored
------------------  --------------------
FastEthernet0/8     FastEthernet0/1
FastEthernet0/8     FastEthernet0/2
FastEthernet0/8     FastEthernet0/3
FastEthernet0/8     FastEthernet0/4
```

Related Commands

port monitor

show port network

Use the **show port network** privileged EXEC command to display the network port defined for the switch or VLAN.

show port network [*interface*]

Syntax Description

interface	(Optional) Port to be displayed.

Command Mode

Privileged EXEC

Usage Guidelines

If the variable *interface* is omitted, the **show port network** command displays all network ports on the switch.

Sample Display

The following is sample output from the **show port network** command:

```
Switch# show port network

Network Port      VLAN ID
------------      -------
FastEthernet0/11  1
```

Related Commands

port network

show port security

Use the **show port security** privileged EXEC command to show the port security parameters defined for the port.

show port security [*interface*]

Syntax Description

interface	(Optional) Port to be displayed.

Command Mode

Privileged EXEC

Usage Guidelines

If the variable *interface* is omitted, the **show port security** command displays all secure ports on the switch.

Sample Display

The following is sample output from the **show port security** command for fixed port 07:

```
Switch# show port security fa0/7

Secure Port      Secure Addr    Secure Addr  Security   Security Action
                 Cnt (Current)  Cnt (Max)    Reject Cnt
---------------  -------------  -----------  ---------- ----------------
FastEthernet0/7  0              132          0          Send Trap
```

Related Commands

port security

show port storm-control

Use the **show port storm-control** privileged EXEC command to display the rising and falling thresholds for broadcast storm control. This command also displays the action that the switch takes when the thresholds are reached.

show port storm-control [*interface*]

Syntax Description

interface (Optional) Port to be displayed.

Command Mode

Privileged EXEC

Usage Guidelines

If the variable *interface* is omitted, the **show port storm-control** command displays broadcast storm control settings on all ports on the switch.

Sample Display

The following is sample output from the **show port storm-control** command:

```
Switch# show port storm-control

Interface  Filter State   Trap State     Rising  Falling  Current  Traps Sent
---------  -------------  -------------  ------  -------  -------  ----------
Fa0/1      <inactive>     <inactive>       1000      200        0           0
Fa0/2      <inactive>     <inactive>        500      250        0           0
Fa0/3      <inactive>     <inactive>        500      250        0           0
Fa0/4      <inactive>     <inactive>        500      250        0           0
```

Related Commands

port storm-control

show proposed

Use the **show proposed** VLAN database command to display the proposed VLAN database or a selected VLAN from it. This command is available only in the Enterprise Edition Software.

show proposed [*vlan-id*]

Syntax Description

vlan-id	(Optional) ID of the VLAN in the proposed database. If this variable is omitted, the entire VLAN database displays, included the pruning state and V2 mode. Valid IDs are from 1 to 1005.

Command Mode

VLAN database

Usage Guidelines

If the variable *vlan-id* is omitted, the **show proposed** command displays the entire proposed VLAN database.

The proposed VLAN database is not the running configuration until you use the **exit** or **apply** command.

Sample Display

The following is sample output from the **show proposed** command:

```
Switch(vlan)# show proposed

VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 2
    Name: VLAN0002
    Media Type: FDDI Net
    VLAN 802.10 Id: 100002
    State: Operational
    MTU: 1500
    STP Type: IBM

VLAN ISL Id: 1002
    Name: fddi-default
    Media Type: FDDI
    VLAN 802.10 Id: 101002
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1003

VLAN ISL Id: 1003
    Name: trcrf-default
    Media Type: TRCRF
    VLAN 802.10 Id: 101003
    State: Operational
    MTU: 4472
    Bridge Type: SRB
    Ring Number: 3276
    Bridge Number: 1
    Parent VLAN: 1005
    Maximum ARE Hop Count: 7
    Maximum STE Hop Count: 7
    Backup CRF Mode: Disabled
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1002

  VLAN ISL Id: 1004
    Name: fddinet-default
    Media Type: FDDI Net
    VLAN 802.10 Id: 101004
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Bridge Number: 1
    STP Type: IBM

VLAN ISL Id: 1005
    Name: trbrf-default
    Media Type: TRBRF
    VLAN 802.10 Id: 101005
    State: Operational
    MTU: 4472
```

```
Bridge Type: SRB
Bridge Number: 15
STP Type: IBM
```

Related Commands

show changes
show proposed

show spanning-tree

Use the **show spanning-tree** privileged EXEC command to show spanning-tree information for the specified spanning-tree instances.

show spanning-tree [**vlan** *stp-list*] [**interface** *interface-list*]

Syntax Description

vlan (Optional) Specify VLAN IDs for the *stp-list* variable when displaying information about spanning-tree instances.

stp-list (Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Enter each VLAN ID separated by a space. Ranges are not supported.

interface (Optional) Specify ports for which spanning-tree instances are displayed.

interface-list List of ports for which spanning-tree information is displayed. Enter each port separated by a space. Ranges are not supported.

Command Mode

Privileged EXEC

Usage Guidelines

If the variable *stp-list* is omitted, the command applies to the STP instance associated with VLAN 1.

Sample Display

The following is sample output from the **show spanning-tree** command for VLAN 1:

```
Switch# show spanning-tree vlan 1

Spanning tree 1 is executing the IEEE compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 00e0.1eb2.ddc0
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0010.0b3f.ac80
  Root port is 5, cost of root path is 10
  Topology change flag not set, detected flag not set, changes 1
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0

Interface Fa0/1  in Spanning tree 1 is down
   Port path cost 100, Port priority 128
   Designated root has priority 32768, address 0010.0b3f.ac80
   Designated bridge has priority 32768, address 00e0.1eb2.ddc0
   Designated port is 1, path cost 10
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 0, received 0
...
```

The following is sample output from the **show spanning-tree interface** command for port 3:

```
Switch# show spanning-tree interface fa0/3

Interface Fa0/3 (port 3) in Spanning tree 1 is down
   Port path cost 100, Port priority 128
   Designated root has priority 6000, address 0090.2bba.7a40
   Designated bridge has priority 32768, address 00e0.1e9f.4abf
   Designated port is 3, path cost 410
   Timers: message age 0, forward delay 0, hold 0
   BPDU: sent 0, received 0
```

Related Commands

spanning-tree
spanning-tree forward-time
spanning-tree max-age
spanning-tree port-priority
spanning-tree protocol

show tacacs

Use the **show tacacs** command to display various TACACS+ server statistics.

show tacacs

Syntax Description

This command has no arguments.

Command Mode

Privileged EXEC

show version

Use the **show version** privileged EXEC command to display version information for the hardware and firmware.

show version

Syntax Description

The command has no arguments

Command Mode

Privileged EXEC

Examples

The following is sample output from the **show version** command:

```
Switch# show version

Cisco Internetwork Operating System Technology Software
IOS Technology(tm) C2900XL Software (C2900XL-H-M), Version 11.2
Copyright (c) 1986-1998 by cisco Systems, Inc.
Compiled Fri 24-Apr-98 10:51 by mollyn
Image text-base: 0x00003000, data-base: 0x001A582C

ROM: Bootstrap program is C2900XL boot loader

Switch uptime is 1 hour, 32 minutes
System restarted by power-on
System image file is “flash:boot”, booted via

cisco WS-C2916M-XL (PowerPC403GA) processor (revision 0x11) with 4096K/1024K bytes of
memory.
Processor board ID 0x06, with hardware revision 0x00
Cluster command switch capable
Cluster member switch capable
Last reset from power-on

Processor is running Enterprise Edition Software
16 Ethernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:53:45:00:02:00
Motherboard assembly number: 73-2193-07
Motherboard serial number: FAA02060647
System serial number: FAA0209Z06U

Module Ports  Model        Hw Version Sw Version
------ -----  -----        ---------- ----------
1      1      WS-X2951-XL  0          12.0   (19990209:004908)

Configuration register is 0xF
```

show vlan

Use the **show vlan** privileged EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) in the administrative domain.

Standard Edition Software:

show vlan {**brief** | **id** *vlan-id*}

Enterprise Edition Software:

show vlan [**brief** | **id** *vlan-id* | **name** *vlan-name*]

Syntax Description

brief (Optional) Display one line for each VLAN with the VLAN name, status, and its ports.

id (Optional) Display VLAN status by VLAN ID.

vlan-id ID of the VLAN displayed. Valid IDs are from 1 to 1005.

name (Optional) Display VLAN status by VLAN name. This keyword is available only in the Enterprise Edition Software.

vlan-name Name of the VLAN displayed. The VLAN name is an ASCII string from 1 to 32 characters. This option is available only in the Enterprise Edition Software.

Command Mode

Privileged EXEC

Sample Displays

The following is sample output from the **show vlan** command (Enterprise Edition Software only):

```
Switch# show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/8, Fa0/10, Fa0/11,
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15,
                                                Fa0/16, Fa1/1, Fa1/2
2    VLAN0002                         active    Fa0/2
3    VLAN0003                         active    Fa0/3
4    VLAN0004                         active    Fa0/4
5    VLAN0005                         suspended Fa0/5
6    VLAN0006                         active    Fa0/6
7    VLAN0007                         active
10   VLAN0010                         act/lshut
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- ------ ------
1    enet  100001     1500  -      -      -        -    1002   1003
6    fdnet 100006     1500  -      -      -        ieee 0      0
7    trnet 100007     1500  -      -      5        ieee 0      0
1002 fddi  101002     1500  -      -      -        -    1      1003
1003 tr    101003     1500  1005   3276   -        -    1      1002
1004 fdnet 101004     1500  -      -      1        ibm  0      0
1005 trnet 101005     1500  -      -      15       ibm  0      0
```

Note This command is not available in the standard edition software.

The following is sample output from the **show vlan brief** command (Enterprise Edition Software only):

```
Switch# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/5, Fa0/6,
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10,
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14,
                                                Fa0/15, Fa0/16, Fa1/1, Fa1/2,
                                                Fa1/3, Fa1/4, Fa2/3, Fa2/4
2    VLAN0002                         active
3    VLAN0003                         active
6    VLAN0006                         active
7    VLAN0007                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Note This command does not show information for VLANs 1002 to 1005 in the standard edition software.

The following is sample output from the **show vlan id 6**or **show vlan name VLAN006** command (Enterprise Edition Software only):

```
Switch# show vlan id 6

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
6    VLAN0006                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- ------ ------
6    fdnet 100006     1500  -      -      -        ieee 0      0
```

Note This command does not show VTP-specific information in the standard edition software.

Related Commands

switchport
vlan

show vmps

Use the **show vmps** privileged EXEC command to display the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, and the current and primary servers. This command is available only in the Enterprise Edition Software.

show vmps

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Sample Display

The following is sample output from the **show vmps** command:

```
Switch# show vmps

VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                    172.20.128.87

Reconfirmation status
---------------------
VMPS Action:         No Dynamic Port
```

Related Commands

vmps reconfirm
vmps retry
vmps server

show vmps statistics

Use the **show vmps statistics** privileged EXEC command to display the VLAN Query Protocol (VQP) client-side statistics and counters. This command is available only in the Enterprise Edition Software.

show vmps statistics

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Sample Display

This following is sample output from the **show vmps statistics** command. Table 2-2 describes each field in the display.

```
Switch# show vmps statistics

VMPS Client Statistics
----------------------
VQP  Queries:              0
VQP  Responses:            0
VMPS Changes:              0
VQP  Shutdowns:            0
VQP  Denied:               0
VQP  Wrong Domain:         0
VQP  Wrong Version:        0
VQP  Insufficient Resource: 0
```

Table 2-2 Field Descriptions

Field	Description
VQP Queries	Number of queries sent by the client to the VLAN Membership Policy Server (VMPS).
VQP Responses	Number of responses sent to the client from the VMPS.
VMPS Changes	Number of times that the VMPS changed from one server to another.
VQP Shutdowns	Number of times the VMPS sent a response to shutdown the port. The client disables the port and removes all dynamic addresses on this port from the address table. You must administratively reenable the port to restore connectivity.
VQP Denied	Number of times the VMPS denied the client request for security reasons. When the VMPS response says to deny an address, no frame is forwarded to or from the workstation with that address (broadcast or multicast frames are delivered to the workstation if the port has been assigned to a VLAN). The client keeps the denied address in the address table as a blocked address to prevent further queries from being sent to the VMPS for each new packet received from this workstation. The client ages the address if no new packets are received from this workstation on this port within the aging time period.
VQP Wrong Domain	Number of times the management domain in the request does not match the one for the VMPS. Any previous VLAN assignments of the port are not changed. Receipt of this response indicates that the server and the client have not been configured with the same VTP management domain.

Table 2-2 Field Descriptions (continued)

Field	Description
VQP Wrong Version	Number of times the version field in the query packet contains a value that is higher than the version supported by the VMPS. Previous VLAN assignment of the port is not changed. The switches send only VMPS version 1 requests.
VQP Insufficient Resource	Number of times the VMPS is unable to answer the request because of a resource availability problem. If the retry limit has not yet been reached, the client repeats the request with the same server or with the next alternate server, depending on whether the per-server retry count has been reached.

Related Commands

clear vmps statistics

show vtp

Use the **show vtp** privileged EXEC command to display general information about the VLAN Trunk Protocol (VTP) management domain, status, and counters. This command is available only in the Enterprise Edition Software.

show vtp {**counters** | **status**}

Syntax Description

counters	Display the VTP counters for the switch.
status	Display general information about the VTP management domain.

Command Mode

Privileged EXEC

Sample Displays

The following is sample output from the **show vtp counters** command. Table 2-3 describes each field in the display.

```
Switch# show vtp counters

VTP statistics:
summary advts received        : 0
subset advts received         : 0
request advts received        : 0
summary advts transmitted     : 0
subset advts transmitted      : 0
request advts transmitted     : 0
No. of config revision errors : 0
No. of config digest errors   : 0
No. of V1 summary errors      : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Fa2/1               242              0                0
```

Table 2-3 Field Descriptions

Field	Description
Summary Advts Received	Number of summary advertisements received by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset Advts Received	Number of subset advertisements received by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request Advts Received	Number of advertisement requests received by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.

Table 2-3 Field Descriptions (continued)

Field	Description
Summary Advts Transmitted	Number of summary advertisements sent by this switch on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset Advts Transmitted	Number of subset advertisements sent by this switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request Advts Transmitted	Number of advertisement requests sent by this switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
No. of Configuration Revision Errors	Number of revision errors. Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the switch increments. Revision errors increment whenever the switch receives an advertisement whose revision number matches the revision number of the switch, but the MD5 digest values do not match. This error indicates that the VTP password in the two switches is different, or the switches have different configurations. These errors indicate that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
No. of Configuration Digest Errors	Number of MD5 digest errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually indicates that the VTP password in the two switches is different. To solve this problem, make sure the VTP password on all switches is the same. These errors indicate that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
No. of V1 Summary Errors	Number of version 1 errors. Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP version 1 frame. These errors indicate that at least one neighboring switch is either running VTP version 1 or VTP version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.
Join Transmitted	Number of VTP pruning messages transmitted on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

The following is sample output from the **show vtp status** command. Table 2-4 describes each field in the display.

```
Switch# show vtp status

VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 68
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 : test1
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x3D 0x02 0xD4 0x3A 0xC4 0x46 0xA1 0x03
Configuration last modified by 172.20.130.52 at 3-4-93 22:25:
```

Table 2-4 Field Descriptions

Field	Description
VTP Version	Displays the VTP version operating on the switch. By default, Catalyst 2900 and 3500 XL switches implement version 1 but can be set to version 2.
Configuration Revision	Number of configuration revisions on this switch.
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.
VTP Operating Mode	Displays the VTP operating mode, which can be server, client, or transparent. Server: a switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot. By default, every switch is a VTP server. Client: a switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not transmit VTP advertisements until it receives advertisements to initialize its VLAN database. Transparent: a switch in VTP transparent mode is disabled for VTP, does not transmit advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. The configuration of multi-VLAN ports causes the switch to automatically enter transparent mode. **Note** Catalyst 2912MF XL, 2924 M XL, 3508G XL, 3512 XL, and 3524 XL switches support up to 250 VLANs. Catalyst 2916M XL, 2924 XL, 2924C XL, and 2908 XL switches support up to 250 or 64 VLANs, respectively. If you define more than 250 or 64 or if the switch receives an advertisement that contains more than 250 or 64 VLANs, the switch automatically enters VTP transparent mode and operates with the VLAN configuration preceding the one that sent it into transparent mode.
VTP Domain Name	Name that identifies the administrative domain for the switch.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.

Table 2-4 Field Descriptions (continued)

Field	Description
VTP V2 Mode	Displays if VTP version 2 mode is enabled. All VTP version 2 switches operate in version 1 mode by default. Each VTP switch automatically detects the capabilities of all the other VTP devices. A network of VTP devices should be configured to version 2 only if all VTP switches in the network can operate in version 2 mode.
VTP Traps Generation	Displays whether VTP traps are transmitted to a network management station.
MD5 Digest	A 16-byte checksum of the VTP configuration.
Configuration Last Modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.

Related Commands

clear vtp counters
vtp

shutdown

Use the **shutdown** interface configuration command to disable a port. Use the **no** form of this command to restart a disabled port.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Mode

Interface configuration

Usage Guidelines

The **shutdown** command for a port causes it to stop forwarding. You can enable the port with the **no shutdown** command.

In the Enterprise Edition Software, the **no shutdown** command has no effect if the port is a static-access port assigned to a VLAN that has been deleted, suspended, or shutdown. The port must first be a member of an active VLAN before it can be reenabled.

Examples

The following examples show how to disable fixed port fa0/8 and how to reenable it:

```
Switch(config)# interface fa0/8
Switch(config-if)# shutdown

Switch(config-if)# no shutdown
```

You can verify the previous commands by entering the **show interface** command in privileged EXEC mode.

shutdown vlan

Use the **shutdown vlan** global configuration command to shutdown (suspend) local traffic on the specified VLAN. Use the **no** form of this command to restart local traffic on the VLAN. This command is available only in the Enterprise Edition Software.

shutdown vlan *vlan-id*
no shutdown vlan *vlan-id*

Syntax Description

vlan-id	ID of the VLAN to be locally shut down. Valid IDs are from 2 to 1001, excluding VLANs defined as default VLANs under the VLAN Trunk Protocol (VTP). The default VLANs are 1 and 1002–1005.

Default

No default is defined.

Command Mode

Global configuration

Usage Guidelines

The **shutdown vlan** command does not change the VLAN information in VTP database. It shuts down traffic locally, but the switch still advertises VTP information.

Example

The following example shows how to shutdown traffic on VLAN 2:

```
Switch(config)# shutdown vlan 2
```

You can verify the previous command by entering the **show vlan** command in privileged EXEC mode.

Related Commands

abort
apply
exit
reset
vlan database

snmp-server enable traps vlan-membership

Use the **snmp-server enable traps vlan-membership** global configuration command to enable SNMP notification for VLAN Membership Policy Server (VMPS) changes. Use the **no** form of this command to disable the VMPS trap notification. This command is available only in the Enterprise Edition Software.

snmp-server enable traps vlan-membership
no snmp-server enable traps vlan-membership

Syntax Description

This command has no arguments or keywords.

Default

SNMP traps for VMPS are disabled.

Command Mode

Global configuration

Usage Guidelines

Specify the host that receives the traps by using the **snmp-server host** command.

Example

The following example shows how to enable VMPS to send trap notifications:

```
Switch(config)# snmp-server enable trap vlan-membership
```

You can verify the previous command by entering the **show running-config** command in privileged EXEC mode.

Related Commands

show running-config
snmp-server host

snmp-server enable traps vtp

Use the **snmp-server enable traps vtp** global configuration command to enable SNMP notification for VLAN Trunk Protocol (VTP) changes. Use the **no** form of this command to disable VTP trap notification. This command is available only in the Enterprise Edition Software.

snmp-server enable traps vtp
no snmp-server enable traps vtp

Syntax Description

This command has no arguments or keywords.

Default

SNMP traps for VTP are disabled.

Command Mode

Global configuration

Usage Guidelines

Specify the host that receives the traps by using the **snmp-server host** command.

Example

The following example shows how to enable VTP to send trap notifications:

```
Switch(config)# snmp-server enable trap vtp
```

You can verify the previous command by entering the **show vtp status** or **show running-config** command in privileged EXEC mode.

Related Commands

show running-config
show vtp status
snmp-server host

snmp-server host

Use the **snmp-server host** global configuration command to specify the host that receives SNMP traps. Use the **no** form of this command to remove the specified host.

snmp-server host *host-address community-string* [**c2900/c3500** | **config** | **snmp** | **tty** | **udp-port** *port-number* | **vlan-membership** | **vtp**]
no snmp-server host *host-address*

Syntax Description

host-address	IP address or name of the SNMP trap host.
community-string	Password-like community string sent with the trap operation.
c2900	Send SNMP Catalyst 2900 series traps.
c3500	Send SNMP Catalyst 3500 series traps.
config	Send SNMP configuration traps.
snmp	Send SNMP-type traps.
tty	Send Cisco enterprise-specific traps when a Transmission Control Protocol (TCP) connection closes.
udp-port {*port-number*}	UDP port of the host to use. The default is 162.
vlan-membership	Send SNMP VLAN Membership Policy Server (VMPS) traps. This option is available only in the Enterprise Edition Software.
vtp	Send SNMP VLAN Trunk Protocol (VTP) traps. This option is available only in the Enterprise Edition Software.

Command Mode

Global configuration

Defaults

The SNMP trap host address and community string are not defined.

Traps are disabled.

Example

The following example shows how to configure an SNMP host to receive VTP traps:

```
Switch(config)# snmp-server host 172.20.128.178 traps vtp
```

Related Commands

snmp-server enable traps vlan-membership
snmp-server enable traps vtp

spanning-tree

Use the **spanning-tree** global configuration command to enable Spanning-Tree Protocol (STP) on a VLAN. Use the **no** form of the command to disable STP on a VLAN.

spanning-tree [**vlan** *stp-list*]
no spanning-tree [**vlan** *stp-list*]

Syntax Description

vlan	(Optional) Include VLAN IDs in the *stp-list* variable when enabling STP.
stp-list	(Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Enter each VLAN ID separated by a space. Ranges are not supported.

Default

STP is enabled.

Command Mode

Global configuration

Usage Guidelines

Disabling STP causes the VLAN or list of VLANs to stop participating in STP. Ports that are administratively down remain down. Received Bridge Protocol Data Units (BPDUs) are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.

STP can be disabled on a VLAN that is not currently active. The setting takes effect when the VLAN is activated.

If the variable *stp-list* is omitted, the command applies to the STP instance associated with VLAN 1.

You can enable STP on a VLAN that has no ports assigned to it.

Example

The following example shows how to disable STP on VLAN 5:

```
Switch(config)# no spanning-tree vlan 5
```

You can verify the previous command by entering the **show spanning-tree** command in privileged EXEC mode. In this instance, VLAN 5 does not appear in the list.

Related Commands

show spanning-tree
spanning-tree forward-time
spanning-tree max-age
spanning-tree port-priority
spanning-tree protocol

spanning-tree cost

Use the **spanning-tree cost** interface configuration command to set the path cost for Spanning-Tree Protocol (STP) calculations. Use the **no** form of this command to return to the default value.

spanning-tree [**vlan** *stp-list*] **cost** *cost*
spanning-tree portfast
no spanning-tree [**vlan** *stp-list*] **cost**

Syntax Description

vlan	(Optional) Include VLAN IDs in the *stp-list* variable when setting the path cost.
stp-list	(Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Enter each VLAN ID separated by a space. Ranges are not supported.
cost	Set a cost.
cost	Path cost can range from 1 to 65535, with higher values indicating higher costs. This range applies whether or not the IEEE or DEC STP has been specified.

Defaults

The default path cost is computed from the interface bandwidth setting. The following are IEEE default path cost values:

- 10 Mbps – 100
- 100 Mbps – 19
- 155 Mbps – 14
- 1 Gbps – 4
- 10 Gbps – 2
- Speeds greater than 10 Gbps – 1

Command Mode

Interface configuration

Usage Guidelines

If the variable *stp-list* is omitted, the command applies to the STP instance associated with VLAN 1.

You can set a cost for a port or on a VLAN that does not exist. The setting takes effect when the VLAN exists.

Example

The following example shows how to set a path cost value of 250 for VLAN 1:

```
Switch(config-if)# spanning-tree vlan 1 cost 250
```

You can verify the previous command by entering the **show spanning-tree** command in privileged EXEC mode.

Related Commands

show spanning-tree
spanning-tree portfast
spanning-tree priority

spanning-tree forward-time

Use the **spanning-tree forward-time** global configuration command to set the forwarding-time for the specified spanning-tree instances. Use the **no** form of this command to return to the default value.

spanning-tree [**vlan** *stp-list*] **forward-time** *seconds*
no spanning-tree [**vlan** *stp-list*] **forward-time**

Syntax Description

vlan (Optional) Include VLAN IDs in the *stp-list* variable when setting the forwarding-time.

stp-list (Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Enter each VLAN ID separated by a space. Ranges are not supported.

seconds Forward-delay interval from 4 to 200 seconds.

Defaults

The default configuration IEEE Spanning-Tree Protocol (STP) is 15 seconds. The default for IBM STP is 4 seconds, and the default for DEC STP is 30 seconds.

Command Mode

Global configuration

Usage Guidelines

If the variable *stp-list* is omitted, the command applies to the STP instance associated with VLAN 1.

You can set the forwarding-time on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to it.

Example

The following example shows how to set the spanning-tree forwarding time to 18 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 forward-time 18
```

You can verify the previous command by entering the **show spanning-tree** command in privileged EXEC mode.

Related Commands

show spanning-tree
spanning-tree forward-time
spanning-tree max-age
spanning-tree port-priority
spanning-tree protocol

spanning-tree hello-time

Use the **spanning-tree hello-time** global configuration command to specify the interval between hello Bridge Protocol Data Units (BPDUs). Use the **no** form of this command to return to the default interval.

spanning-tree [**vlan** *stp-list*] **hello-time** *seconds*
no spanning-tree [**vlan** *stp-list*] **hello-time**

Syntax Description

vlan	(Optional) Include VLAN IDs in the *stp-list* variable when specifying the hello-time.
stp-list	(Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Enter each VLAN ID separated by a space. Ranges are not supported.
seconds	Interval from 1 to 10 seconds.

Defaults

The default configuration IEEE Spanning-Tree Protocol (STP) is 2 seconds. The default for IBM STP is 2 seconds, and the default for DEC STP is 1 second.

Command Mode

Global configuration

Usage Guidelines

If the variable *stp-list* is omitted, the command applies to the STP instance associated with VLAN 1.

You can set the hello time on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to it.

Example

The following example shows how to set the spanning-tree hello-delay time to 3 seconds for VLAN 20:

```
Switch (config) # spanning-tree vlan 20 hello-time 3
```

You can verify the previous command by entering the **show spanning-tree** command in privileged EXEC mode.

Related Commands

show spanning-tree
spanning-tree
spanning-tree port-priority
spanning-tree protocol

spanning-tree max-age

Use the **spanning-tree max-age** global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a Bridge Protocol Data Unit (BPDU) message from the root switch within this interval, it recomputes the STP topology. Use the **no** form of this command to return to the default interval.

spanning-tree [**vlan** *stp-list*] **max-age** *seconds*
no spanning-tree [**vlan** *stp-list*] **max-age**

Syntax Description

vlan (Optional) Include VLAN IDs in the *stp-list* variable when changing the interval that switch waits to hear BPDUs from the root switch.

stp-list (Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Enter each VLAN ID separated by a space. Ranges are not supported.

seconds Interval the switch waits between receiving BPDUs from the root switch. Enter a number from 6 to 200.

Defaults

The default configuration (IEEE STP) is 20 seconds. The default for DEC STP is 15 seconds, and the default for IBM STP is 10 seconds.

Command Mode

Global configuration

Usage Guidelines

The **max-age** setting must be greater than the **hello-time** setting.

If the variable *stp-list* is omitted, the command applies to the STP instance associated with VLAN 1.

You can set the **max-age** on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to it.

Examples

The following example shows how to set **spanning-tree max-age** to 30 seconds for VLAN 20:

```
Switch (config)# spanning-tree vlan 20 max-age 30
```

The following example shows how to reset the **max-age** parameter to the default value for spanning-tree instances 100 through 102:

```
Switch (config)# no spanning-tree vlan 100 101 102 max-age
```

You can verify the previous commands by entering the **show spanning-tree** command in privileged EXEC mode.

Related Commands

show spanning-tree
spanning-tree forward-time
spanning-tree hello-time
spanning-tree priority
spanning-tree protocol

spanning-tree portfast

Use the **spanning-tree portfast** interface configuration command to enable the Port Fast feature on a port in all its associated VLANs. When the Port Fast feature is enabled, the port changes directly from a blocking state to a forwarding state without making the intermediate Spanning-Tree Protocol (STP) status changes. Use the **no** form of this command to return the port to default operation.

spanning-tree portfast *interface*
no spanning-tree portfast

Syntax

interface	Module and port number enabled for the Port Fast feature.

Default

The Port Fast feature is disabled.

Command Mode

Interface configuration

Usage Guidelines

This feature is not supported on the ATM modules.

This feature should be used only on ports that connect to end stations.

This feature affects all VLANs on the port.

A port with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state.

In Enterprise Edition Software, the Port Fast feature is automatically enabled on dynamic-access ports.

Example

The following example shows how to enable the Port Fast feature on fixed port 2.

```
Switch(config-if)# spanning-tree portfast fa0/2
```

Related Commands

spanning-tree portfast
spanning-tree port-priority

spanning-tree port-priority

Use the **spanning-tree port-priority** interface configuration command to set a port priority that is used when two switches tie for position as the root switch. Use the **no** form of this command to return to the default value.

spanning-tree [**vlan** *stp-list*] **port-priority** *port-priority*
no spanning-tree [**vlan** *stp-list*] **port-priority**

Syntax Description

vlan (Optional) Include VLAN IDs in the *stp-list* variable when setting the port priority.

stp-list (Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Enter each VLAN ID separated by a space. Ranges are not supported.

port-priority Number from 0 to 255.

Defaults

The default configuration (IEEE STP) is 128. The default for IBM STP and DEC STP is also 128.

Command Mode

Interface configuration

Usage Guidelines

If the variable *stp-list* is omitted, the command applies to the STP instance associated with VLAN 1.

You can set the port priority on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to it.

Example

The following example shows how to increase the likelihood that the spanning-tree instance 20 is chosen as the root switch on port fa0/2:

```
Switch(config)# interface fa0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

You can verify the previous commands by entering the **show spanning-tree** command in privileged EXEC mode.

Related Commands

show spanning-tree
spanning-tree port-priority
spanning-tree protocol

spanning-tree priority

Use the **spanning-tree priority** global configuration command to configure the switch priority for the specified spanning-tree instance. This will change the likelihood that the switch is selected as the root switch. Use the **no** form of this command to revert to the default value.

spanning-tree [**vlan** *stp-list*] **priority** *bridge-priority*
no spanning-tree [**vlan** *stp-list*] **priority**

Syntax Description

vlan (Optional) Include VLAN IDs in the *stp-list* variable when configuring the switch priority.

stp-list (Optional) List of STP instances. Each spanning-tree instance is associated with a VLAN ID. Enter each VLAN ID separated by a space. Ranges are not supported.

bridge-priority A number from 0 to 65535. The lower the number, the more likely the switch will be chosen as root.

Defaults

The default configuration (IEEE STP) is 32768. The default value for IBM STP and DEC STP is also 32768.

Command Mode

Global configuration

Usage Guidelines

If the variable *stp-list* is omitted, the command applies to the STP instance associated with VLAN 1.

You can configure the switch priority on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to it.

Example

The following example shows how to set the spanning-tree priority to 125 for a list of VLANs:

```
Switch (config)# spanning-tree vlan 20 100 101 102 priority 125
```

You can verify the previous command by entering the **show spanning-tree** command in privileged EXEC mode.

Related Commands

show spanning-tree
spanning-tree forward-time
spanning-tree hello-time
spanning-tree max-age
spanning-tree protocol

spanning-tree protocol

Use the **spanning-tree protocol** global configuration command to specify the Spanning-Tree Protocol (STP) to be used for specified spanning-tree instances. Use the **no** form to use the default protocol.

spanning-tree [**vlan** *stp-list*] **protocol** {**ieee** | **dec** | **ibm**}
no spanning-tree [**vlan** *stp-list*] **protocol**

Syntax Description

vlan	(Optional) Include VLAN IDs in the *stp-list* variable when specifying the protocol.
stp-list	(Optional) List of spanning-tree instances. Each spanning-tree instance is associated with a VLAN ID. Enter each VLAN ID separated by a space. Ranges are not supported.
ieee	IEEE Ethernet STP.
dec	DEC STP.
ibm	IBM STP.

Default

The default protocol is **ieee**.

Command Mode

Global configuration

Usage Guidelines

Changing the spanning-tree protocol causes STP parameters to change to default values of the new protocol.

If the variable *stp-list* is omitted, this command applies to the STP instance associated with VLAN 1.

You can change the protocol on a VLAN that has no ports assigned to it. The setting takes effect when you assign ports to it.

Example

The following example shows how to change the STP protocol for VLAN 20 to the DEC version of STP:

```
Switch(config)# spanning-tree vlan 20 protocol dec
```

You can verify the previous command by entering the **show spanning-tree** command in privileged EXEC mode.

Related Commands

show spanning-tree
spanning-tree
spanning-tree forward-time
spanning-tree max-age
spanning-tree port-priority

stp uplinkfast

Use the **stp uplinkfast** global configuration command to accelerate the choice of a new root port when a link or switch fails or when Spanning-Tree Protocol (STP) reconfigures itself. This command is available only in the Enterprise Edition Software.

stp uplinkfast [**max-update-rate** *pkts-per-second*]

Syntax Description

max-update-rate	The maximum update rate for packets per seconds.
pkts-per-second	The number of packets per second for multicast traffic. The range is 0 to 1000.

Command Mode

Global configuration

Usage Guidelines

When you enable UplinkFast, it is enabled for the entire switch and cannot be enabled for individual VLANs.

Example

Enter this command in global configuration mode to configure UplinkFast:

```
Switch(config)# spanning-tree uplinkfast
```

speed

Use the **speed** interface configuration command to specify the speed of a Fast Ethernet port. Use the **no** form of this command to return the port to its default value.

speed {**10** | **100** | **auto**}
no speed

Syntax Description

10	Port runs at 10 Mbps.
100	Port runs at 100 Mbps.
auto	Port automatically detects whether it should run at 10 or 100 Mbps.

Defaults

The default is **auto**.

For Gigabit Ethernet ports, the speed is 1000 Mbps and not configurable.

Command Mode

Interface configuration

Usage Guidelines

Certain ports can be configured to be either 10 or 100 Mbps. Applicability of this command is hardware-dependent.

Note For guidelines on setting the switch speed and duplex parameters, see the *Catalyst 2900 Series XL Installation and Configuration Guide*.

Example

The following example shows how to set port 1 on module 2 to 100 Mbps:

```
Switch(config)# interface fastethernet2/1
Switch(config-if)# speed 100
```

Related Commands

duplex

switchport access

Use the **switchport access** interface configuration command to configure a port as a static-access or dynamic-access port. If the mode is set to access, the port operates as a member of the configured VLAN. If set to dynamic, the port starts discovery of VLAN assignment based on the incoming packets it receives. Use the **no** form of this command to reset the access mode to the default VLAN for the switch.

switchport access vlan {*vlan-id* | **dynamic**}
no switchport access vlan {*vlan-id* | **dynamic**}

Syntax Description

vlan	Assign a VLAN to the port.
vlan-id	ID of the VLAN. Valid IDs are from 1 to 1001.
dynamic	Port is assigned to a VLAN based on the source MAC address of a host (or hosts) connected to that port. The switch sends every new source MAC address received to the VLAN Membership Policy Server (VMPS) to obtain the VLAN name to which the dynamic-access port should be assigned. If the port already has a VLAN assigned and the source has already been approved by the VMPS, the switch forwards the packet to the VLAN. This keyword is only supported in the Enterprise Edition Software.

Defaults

All ports are in static-access mode in VLAN 1.

A dynamic-access port is initially a member of no VLAN and receives its assignment based on the packets it receives.

Command Mode

Interface configuration

Usage Guidelines

The port must be in access mode before the **switchport access vlan** *vlan-id* or **switchport access vlan dynamic** command can take effect. For more information, see the “switchport mode” section on page 2-128.

An access port can be assigned to only one VLAN.

When the **no switchport access vlan** form is used, the access mode is reset to static access on VLAN 1.

The following restrictions apply to dynamic-access ports:

- Enterprise Edition Software implements the VLAN Query Protocol (VQP) client, which can query a VMPS such as the Catalyst 5000. Catalyst 2900 series switches are not VMPS servers. The VMPS server must be configured before a port is configured as dynamic.
- Use dynamic-access ports to connect end stations only. Connecting them to switches or routers (that are bridging protocols) can cause a loss of connectivity.
- Configure the network so that STP does not put the dynamic-access port into an STP blocking state. The Port Fast feature is automatically enabled on dynamic-access ports.

- Dynamic-access ports can only be in one VLAN and do not use VLAN tagging.
- Dynamic-access ports cannot be configured as:
  - — The source or destination port in a static address entry.
  - — A network port (dynamic-access ports can be assigned to a VLAN in which one of the other ports is a network port).
  - — A port group (dynamic-access ports cannot be grouped with any other port including other dynamic ports).
  - — A secure port.
  - — A port with a secure address.
  - — A monitor port.

Examples

The following example shows how to assign a port already in access mode to VLAN 2 (instead of the default VLAN 1):

```
Switch(config-if)# switchport access vlan 2
```

The following example shows how to assign a port already in access mode to dynamic:

```
Switch(config-if)# switchport access vlan dynamic
```

The following example shows how to reconfigure a dynamic-access port to a static-access port:

```
Switch(config-if)# no switchport access vlan dynamic
```

You can verify the previous commands by entering the **show interface** *interface-id* **switchport** command in privileged EXEC mode and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

switchport mode
switchport multi
switchport trunk

switchport mode

Use the **switchport mode** interface configuration command to configure the VLAN membership mode of a port. Use the **no** form of this command to reset the mode to the appropriate default for the device.

switchport mode {**access** | **multi** | **trunk**}
no switchport mode {**access** | **multi** | **trunk**}

Syntax Description

access	Set the port to access mode (either static-access or dynamic-access depending on the setting of the **switchport access vlan** command). The port operates as a nontrunking, single VLAN interface that transmits and receives nonencapsulated frames. An access port can be assigned to only one VLAN.
multi	Set the port to multi-VLAN port mode. The port operates as a nontrunking VLAN interface that transmits and receives nonencapsulated frames. A multi-VLAN port can be assigned to one or more VLANs.
trunk	Set the port to a trunking VLAN Layer-2 interface. The port transmits and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router. This keyword is supported only in the Enterprise Edition Software.

Default

All ports are static-access ports in VLAN 1.

Command Mode

Interface configuration

Usage Guidelines

Configuration using the **access**, **multi**, or **trunk** keywords takes effect only when the port is changed to the corresponding mode by using the **switchport mode** command. The static-access, multi-VLAN, and trunk (Enterprise Edition Software only) configurations are saved, but only one configuration is active at a time.

The **no switchport mode** form resets the mode to static access.

Only these combinations of port modes can appear on a single switch:

- Multi-VLAN and access ports
- Trunk and access ports

Trunk and multi-VLAN ports cannot coexist on the same switch. If you want to change a multi-VLAN or trunk port into another mode, you must first change it to an access port and then reassign it to the new mode.

Examples

The following example shows how to configure a port for access mode:

```
Switch(config-if)# switchport mode access
```

The following example shows how to configure a port for multi-VLAN mode:

```
Switch(config-if)# switchport mode multi
```

The following example shows how to configure a port for trunk mode:

```
Switch(config-if)# switchport mode trunk
```

You can verify the previous commands by entering the **show interface** *interface-id* **switchport** command in privileged EXEC mode and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

switchport access
switchport multi
switchport trunk

switchport multi

Use the **switchport multi** interface configuration command to configure a list of VLANs to which the port is associated. If the mode is set to multi, the port operates as a member of all VLANs in the list. Use the **no** form of this command to reconfigure the port as an access port.

switchport multi vlan {**add** *vlan-list* | **remove** *vlan-list*}
no switchport multi vlan

Syntax Description

vlan	Indicate the VLAN to which the port is associated.
add	Add specified VLAN IDs to the list.
vlan-list	List of VLAN IDs. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are from 1 to 1001.
remove	Remove the specified VLAN IDs.

Default

The default for VLAN membership of a multi-VLAN port is VLAN 1.

Command Mode

Interface configuration

Usage Guidelines

The **switchport mode multi** command must be entered before the **switchport multi vlan** *vlan-list* command can take effect.

In the variable *vlan-list*, separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.

A multi-VLAN port cannot be a secure port or a monitor port.

A multi-VLAN port cannot coexist with a trunk port on the same switch.

Caution To avoid loss of connectivity, do not connect multi-VLAN ports to hubs or switches. Connect multi-VLAN ports to routers or servers.

Examples

The following example shows how to assign a multi-VLAN port already in multi mode to two VLANs:

```
Switch(config-if)# switchport multi vlan 2,4
```

The following example shows how to assign a multi-VLAN port already in multi mode to a range of VLANs:

```
Switch(config-if)# switchport multi vlan 5-10
```

The following example shows how to reset the VLAN list of a multi-VLAN port to the default (VLAN 1 only):

```
Switch(config-if)# no switchport multi vlan
```

You can verify the previous commands by entering the **show interface** *interface-id* **switchport** command in privileged EXEC mode and examining information in the Administrative Mode and Operational Mode rows.

Related Commands

switchport access
switchport mode
switchport trunk

switchport trunk allowed vlan

Use the **switchport trunk allowed vlan** interface configuration command to control which VLANs can receive and transmit traffic on the trunk. Use the **no** form of this command to reset the allowed list to the default value. This command is available only in the Enterprise Edition Software.

switchport trunk allowed vlan {**add** *vlan-list* | **all** | **except** *vlan-list* | **remove** *vlan-list*}
no switchport trunk allowed vlan

Syntax Description

add	Add specified VLAN IDs to the list.
vlan-list	List of VLAN IDs. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are from 1 to 1001.
all	Add all VLAN IDs to the list.
except	Add VLAN IDs except the specified ones.
remove	Remove the specified VLAN IDs.

Default

All VLANs are included in the allowed list.

Command Mode

Interface configuration

Usage Guidelines

When the **no switchport trunk allowed vlan** form is used, the allowed list is reset to the default list, which allows all VLANs.

In the variable *vlan-list*, separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs. You cannot remove VLAN 1 or 1002 to 1005 from the list.

A trunk port cannot be a secure port or a monitor port. However, a static-access port can monitor a VLAN on a trunk port. The VLAN monitored is the one associated with the static-access port.

If a trunk port is identified as a network port, the trunk port becomes the network port for all the VLANs associated with the port.

Example

The following example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

You can verify the previous command by entering the **show interface** *interface-id* **switchport** command in privileged EXEC mode.

Related Commands

switchport mode
switchport trunk encapsulation
switchport trunk native

switchport trunk encapsulation

Use the **switchport trunk encapsulation** interface configuration command to set the encapsulation format on the trunk port. Use the **no** form of this command to reset the format to the default. This command is available only in the Enterprise Edition Software.

switchport trunk encapsulation {**isl** | **dot1q**}
no switchport trunk encapsulation

Syntax Description

isl	Set the encapsulation format to Inter-Switch Link (ISL). The switch encapsulates all received and transmitted packets with an ISL header. The switch filters native frames received from an ISL trunk port.
dot1q	Set the tagging format to IEEE 802.1Q. With this format, the switch supports simultaneous tagged and untagged traffic on a port.

Default

The default encapsulation format is ISL.

Command Mode

Interface configuration

Usage Guidelines

You cannot configure one end of the trunk as an 802.1Q trunk and the other end as an ISL or nontrunk port. However, you can configure one port as an ISL trunk and another port on the same switch as a 802.1Q trunk.

This command is only applicable on switch platforms and port hardware that support both formats.

Example

The following example shows how to configure the encapsulation format to 802.1Q:

```
Switch(config-if)# switchport trunk encapsulation dot1q
```

You can verify the previous command by entering the **show interface** *interface-id* **switchport** command in privileged EXEC mode.

Related Commands

switchport mode
switchport trunk allowed vlan
switchport trunk native

switchport trunk native

Use the **switchport trunk native** interface configuration command to set the native VLAN for untagged traffic when in 802.1Q trunking mode. Use the **no** form of this command to reset the native VLAN to the default. This command is available only in the Enterprise Edition Software.

switchport trunk native vlan *vlan-id*
no switchport trunk native

Syntax Description

vlan	Indicate the VLAN to which the port is associated.
vlan-id	ID of the VLAN that is sending and receiving untagged traffic on the trunk port. Valid IDs are from 1 to 1001.

Default

VLAN 1 is the default native VLAN ID on the port.

Command Mode

Interface configuration

Usage Guidelines

All untagged traffic received on the 802.1Q trunk port is forwarded with the native VLAN configured for the port.

If a packet has a VLAN ID equal to the outgoing port's native VLAN ID, the packet is transmitted untagged; otherwise, the switch transmits the packet with a tag.

Example

The following example shows how to configure VLAN 3 as the default port to send all untagged traffic:

```
Switch(config-if)# switchport trunk native vlan 3
```

You can verify the previous command by entering the **show interface** *interface-id* **switchport** command in privileged EXEC mode.

Related Commands

switchport mode
switchport trunk allowed vlan
switchport trunk encapsulation

tacacs-server attempts

Use the **tacacs-server attempts** global configuration command to control the number of login attempts that can be made on a line set up for TACACS, Extended TACACS, or TACACS+ verification. Use the **no** form of this command to disable this feature and restore the default. This command is available only in the Enterprise Edition Software.

tacacs-server attempts *count*
no tacacs-server attempts

Syntax Description

count	Integer that sets the number of attempts. The default is 3.

Command Mode

Global configuration

Examples

The following example changes the login attempt to just one:

```
Switch(config)# tacacs-server attempts 1
```

Related Commands

enable (use-tacacs)
login (tacacs)
show (tacacs)
tacacs-server (directed-request)
tacacs-server (host)
tacacs-server (key)
tacacs-server (last-resort)
tacacs-server (timeout)

tacacs-server directed-request

Use the **tacacs-server directed-request** global configuration command to send only a username to a specified server when a direct request is issued in association with TACACS, Extended TACACS, and TACACS+. Use the **no** form of this command to disable the direct-request feature. This command is available only in the Enterprise Edition Software.

tacacs-server directed-request
no tacacs-server directed-request

Syntax Description

This command has no arguments or keywords.

Command Mode

Global configuration

Usage Guidelines

This command sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with the directed-request feature enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Using **no tacacs-server directed-request** causes the whole string, both before and after the "@" symbol, to be sent to the default TACACS server. When the directed-request feature is disabled, the router queries the list of servers, starting with the first one in the list. It sends the whole string, and accepts the first response it gets from the server. The **tacacs-server directed-request** command is useful for sites that have developed their own TACACS server software that parses the whole string and makes decisions based on it.

With **tacacs-server directed-request** enabled, only configured TACACS servers can be specified by the user after the "@" symbol. If the host name specified by the user does not match the IP address of a TACACS server configured by the administrator, the user input is rejected.

Use **no tacacs-server directed-request** to disable the ability of the user to choose between configured TACACS servers and to cause the entire string to be passed to the default server.

Examples

The following example shows how to pass the entire user input to the default TACACS server **tacacs-server directed-request**:

```
Switch(config)# no tacacs-server directed-request
```

Related Commands

enable (use-tacacs)
login (tacacs)
show (tacacs)
tacacs-server (directed-request)
tacacs-server (host)
tacacs-server (key)
tacacs-server (last-resort)
tacacs-server (timeout)

tacacs-server dns-alias-lookup

Use the **tacacs-server dns-alias-lookup** global configuration command to enable IP Domain Name System alias lookup for TACACS+. Use the **no** form of this command to disable this feature. This command is available only in the Enterprise Edition Software.

tacacs-server dns-alias-lookup
no tacacs-server dns-alias-lookup

Syntax Description

This command has no keywords or arguments.

Command Mode

Global configuration

Usage Guidelines

This command enables IP Domain Name System alias lookup for TACACS servers.

tacacs-server extended

Use the **tacacs-server extended** global configuration command to enable an extended TACACS mode. Use the **no** form of this command to disable the mode. This command is available only in the Enterprise Edition Software.

t**acacs-server extended**
no tacacs-server extended

Syntax Description

This command has no arguments or keywords.

Command Mode

Global configuration

Usage Guidelines

This command initializes extended TACACS. To initialize AAA/TACACS+, use the **aaa new-model** command.

Examples

The following example shows how to enable extended TACACS mode:

```
Switch(config)# tacacs-server extended
```

tacacs-server host

Use the **tacacs-server host** global configuration command to specify a TACACS, Extended TACACS, or TACACS+ host. Use the **no** form of this command to delete the specified name or address. This command is available only in the Enterprise Edition Software.

tacacs-server host *hostname* **[single-connection] [port *integer*] [timeout *integer*] [key *string*]**
no tacacs-server host *hostname*

Syntax Description

hostname	Name or IP address of the host.
single-connection	Specify that the switch maintain a single open connection for confirmation from a AAA/TACACS+ server (CiscoSecure Release 1.0.1 or later). This command contains no autodetect and fails if the specified host is not running a CiscoSecure daemon.
port	Specify a server port number.
integer	Port number of the server (in the range 1 to 10,000).
timeout	Specify a timeout value. This overrides the global timeout value set with the **tacacs-server timeout** command for this server only.
integer	Integer value, in seconds, of the timeout interval.
key	Specify an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command tacacs-server key for this server only.
string	Character string specifying authentication and encryption key.

Command Mode

Global configuration

Usage Guidelines

You can use multiple **tacacs-server host** commands to specify additional hosts. The Cisco IOS software searches for hosts in the order in which you specify them. Use the **single-connection**, **port**, **timeout**, and **key** options only when running a AAA/TACACS+ server.

Because some of the parameters of the **tacacs-server host** command override global settings made by the **tacacs-server timeout** and **tacacs-server key** commands, you can use this command to enhance security on your network by uniquely configuring individual switches.

Examples

The following example specifies a TACACS host named *Sea_Change*:

```
Switch(config)# tacacs-server host Sea_Change
```

The following example specifies that, for AAA confirmation, the switch consult the CiscoSecure TACACS+ host named *Sea_Cure* on port number 51. The timeout value for requests on this connection is 3 seconds; the encryption key is *a_secret*.

```
Switch(config)# tacacs-server host Sea_Cure single-connection port 51 timeout 3 key
a_secret
```

Related Commands

login tacacs
ppp
slip
tacacs-server key
tacacs-server timeout

tacacs-server key

Use the **tacacs-server key** global configuration command to set the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon. Use the **no** form of the command to disable the key. This command is available only in the Enterprise Edition Software.

tacacs-server key *key*
no tacacs-server key [*key*]

Syntax Description

key	Key used to set authentication and encryption. This key must match the key used on the TACACS+ daemon.

Command Mode

Global configuration

Usage Guidelines

After enabling AAA with the **aaa new-model** command, you must set the authentication and encryption key using the **tacacs-server key** command.

The key entered must match the key used on the TACACS+ daemon. All leading spaces are ignored; spaces within and at the end of the key are not. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Examples

The following example illustrates how to set the authentication and encryption key to *dare to go*:

```
Switch(config)# tacacs-server key dare to go
```

Related Commands

aaa new-model
tacacs-server host

tacacs-server last-resort

Use the **tacacs-server last-resort** global configuration command to cause the network access server to request the privileged password as verification for TACACS or Extended TACACS or to allow successful login without further input from the user. Use the **no tacacs-server last-resort** command to restore the system to the default behavior. This command is available only in the Enterprise Edition Software.

tacacs-server last-resort {password | succeed}
no tacacs-server last-resort {password | succeed}

Syntax Description

password	Allows the user to access the privileged EXEC command mode by entering the password set by the **enable** command.
succeed	Allows the user to access the privileged EXEC command mode without further question.

Command Mode

Global configuration

Usage Guidelines

Use the **tacacs-server last-resort** command to be sure that you can login; for example, a systems administrator would use this command to log in to troubleshoot TACACS servers that might be down.

Note This command is not used in AAA/TACACS+.

Examples

The following example shows how to force successful login:

```
Switch(config)# tacacs-server last-resort succeed
```

Related Commands

enable password
login (EXEC)

tacacs-server login-timeout

Use the **tacacs-server login-timeout** global configuration command to cause the network access server to request the privileged password as verification for TACACS or Extended TACACS, or to allow successful login without further input from the user. Use the **no tacacs-server login-timeout** command to restore the system to the default behavior. This command is available only in the Enterprise Edition Software.

tacacs-server login-timeout {password | succeed}
no tacacs-server login-timeout {password | succeed}

Syntax Description

password	Allow the user to access the privileged EXEC command mode by entering the password set by the enable command.
succeed	Allow the user to access the privileged EXEC command mode without further question.

Command Mode

Global configuration

Usage Guidelines

Use the **tacacs-server login-timeout** command to be sure that you can login; for example, a systems administrator would use this command to log in to troubleshoot TACACS servers that might be down.

Note This command is not used in authentication, authorization, and accounting (AAA)/TACACS+.

Examples

The following example shows how to force successful login:

```
Switch(config)# tacacs-server login-timeout succeed
```

Related Commands

enable password
login (EXEC)

tacacs-server optional-passwords

Use the **tacacs-server optional-passwords** global configuration command to specify that the first TACACS request to a TACACS or Extended TACACS server be made without password verification. Use the **no** form of this command to restore the default. This command is available only in the Enterprise Edition Software.

tacacs-server optional-passwords
no tacacs-server optional-passwords

Syntax Description

This command has no arguments or keywords.

Command Mode

Global configuration

Usage Guidelines

When the user enters in the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the TACACS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The TACACS server must support authentication for users without passwords to make use of this feature. This feature supports all TACACS requests--login, SLIP, enable, and so on.

Note This command is not used by AAA/TACACS+.

Examples

The following example shows how to configure the first login to bypass TACACS verification:

```
Switch(config)# tacacs-server optional-passwords
```

tacacs-server retransmit

Use the **tacacs-server retransmit** global configuration command to specify the number of times the Cisco IOS software searches the list of TACACS or Extended TACACS server hosts before giving up. Use the **no** form of this command to disable retransmission. This command is available only in the Enterprise Edition Software.

tacacs-server retransmit *retries*
no tacacs-server retransmit

Syntax Description

retries	Integer that specifies the retransmit count.

Command Mode

Global configuration

Usage Guidelines

The Cisco IOS software will try all servers, allowing each one to time out before increasing the retransmit count.

Examples

The following example shows how to specify a retransmit counter value of 5:

```
Switch(config)# tacacs-server retransmit 5
```

tacacs-server timeout

Use the **tacacs-server timeout** global configuration command to set the interval that the server waits for a TACACS, Extended TACACS, or TACACS+ server to reply. Use the **no** form of this command to restore the default. This command is available only in the Enterprise Edition Software.

tacacs-server timeout *seconds*
no tacacs-server timeout

Syntax Description

seconds	Integer that specifies the timeout interval in seconds (between 1 and 300).

Command Mode

Global configuration

Usage Guidelines

None.

Examples

The following example shows how to change the interval timer to 10 seconds:

```
Switch(config)# tacacs-server timeout 10
```

Related Commands

tacacs-server host

vlan

Use the **vlan** VLAN database command to configure VLAN characteristics. Use the **no** form of this command to delete a VLAN and its configured characteristics. This command is available only in the Enterprise Edition Software.

vlan *vlan-id* [**name** *vlan-name*] [**media** {**ethernet** | **fddi** | **fdi-net** | **tokenring** | **tr-net**}]
[**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*]
[**bridge** *bridge-number* | **type** {**srb** | **srt**}] [**parent** *parent-vlan-id*] [**stp type** {**ieee** | **ibm** | **auto**}]
[**are** *are-number*] [**ste** *ste-number*] [**backupcrf** {**enable** | **disable**}]
[**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

no vlan *vlan-id* [**name** *vlan-name*] [**media** {**ethernet** | **fddi** | **fdi-net** | **tokenring** | **tr-net**}]
[**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*]
[**bridge** *bridge-number* | **type** {**srb** | **srt**}] [**parent** *parent-vlan-id*] [**stp type** {**ieee** | **ibm** | **auto**}]
[**are** *are-number*] [**ste** *ste-number*] [**backupcrf** {**enable** | **disable**}]
[**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

Note Catalyst 2900 and Catalyst 3500 XL switches support only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunk Protocol (VTP) global advertisements to other switches. These VLANs are locally suspended.

Table 2-5 lists the valid syntax for each media type.

Table 2-5 Valid Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	**vlan** *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
FDDI	**vlan** *vlan-id* [**name** *vlan-name*] **media fddi** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*] [**parent** *parent-vlan-id*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
FDDI-NET	**vlan** *vlan-id* [**name** *vlan-name*] **media fdi-net** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**bridge** *bridge-number*] [**stp type** {**ieee** | **ibm** | **auto**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*] If VTP V2 mode is disabled, do not set the stp type to auto.
Token Ring	VTP V2 mode is disabled. **vlan** *vlan-id* [**name** *vlan-name*] **media tokenring** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*] [**parent** *parent-vlan-id*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
Token Ring concentrator relay function (TRCRF)	VTP V2 mode is enabled. **vlan** *vlan-id* [**name** *vlan-name*] **media tokenring** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**ring** *ring-number*] [**parent** *parent-vlan-id*] [**bridge type** {**srb** | **srt**}] [**are** *are-number*] [**ste** *ste-number*] [**backupcrf** {**enable** | **disable**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]
Token Ring-NET	VTP V2 mode is disabled. **vlan** *vlan-id* [**name** *vlan-name*] **media tr-net** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**bridge** *bridge-number*] [**stp type** {**ieee** | **ibm**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

Table 2-5 Valid Syntax for Different Media Types (continued)

Media Type	Valid Syntax
Token Ring bridge relay function (TRBRF)	VTP V2 mode is enabled. **vlan** *vlan-id* [**name** *vlan-name*] **media tr-net** [**state** {**suspend** | **active**}] [**said** *said-value*] [**mtu** *mtu-size*] [**bridge** *bridge-number*] [**stp type** {**ieee** | **ibm** | **auto**}] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

VLAN Configuration Rules

Table 2-6 describes the rules for configuring VLANs.

Table 2-6 VLAN Configuration Rules

Configuration	Rule
VTP V2 mode is enabled, and you are configuring a TRCRF VLAN media type.	Specify a parent VLAN ID of a TRBRF that already exists in the database. Specify a ring number. Do not leave this field blank. Specify unique ring numbers when TRCRF VLANs have the same parent VLAN ID. Only one backup CRF can be enabled.
VTP V2 mode is enabled, and you are configuring VLANs other than TRCRF media type.	Do not specify a backup CRF.
VTP V2 mode is enabled, and you are configuring a TRBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.
VTP V2 mode is disabled.	No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

Syntax Description

vlan-id	ID of the configured VLAN. Valid IDs are from 1 to 1005 and must be unique within the administrative domain.
name	(Optional) Name of the VLAN to follow.
vlan-name	ASCII string from 1 to 32 characters that must be unique within the administrative domain.
media	(Optional) VLAN media type to follow.
ethernet	Ethernet media type.
fddi	FDDI media type.
fdi-net	FDDI network entity title (NET) media type.
tokenring	Token Ring media type if the VTP V2 mode is disabled. TRCRF media type if the VTP V2 mode is enabled.
tr-net	Token Ring network entity title (NET) media type if the VTP V2 mode is disabled. TRBRF media type if the VTP V2 mode is enabled.
state	(Optional) State of the VLAN to follow.
active	VLAN is operational.
suspend	VLAN is suspended. Suspended VLANs do not pass packets.
said	(Optional) The security association identifier (SAID) as documented in IEEE 802.10 to follow.
said-value	Integer from 1 to 4294967294 that must be unique within the administrative domain.
mtu	(Optional) Maximum transmission unit (packet size in bytes) to follow.
mtu-size	Packet size in bytes from 1500 to 18190 that the VLAN can use.
ring	(Optional) Logical ring for an FDDI, Token Ring, or TRCRF VLAN to follow.
ring-number	Integer from 1 to 4095.
bridge	(Optional) Logical distributed source-routing bridge to follow. This bridge that interconnects all logical rings having this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TRBRF VLANs.
bridge-number	Integer from 0 to 15.
type	Bridge type to follow. Applies only to TRCRF VLANs.
srb	Source-route bridging VLAN.

srt	Source-route transparent bridging VLAN.
parent	(Optional) Parent VLAN of an existing FDDI, Token Ring, or TRCRF VLAN to follow. This parameter identifies the TRBRF to which a TRCRF belongs and is required when defining a TRCRF.
parent-vlan-id	Integer from 0 to 1005.
stp type	(Optional) Spanning-tree type for FDDI-NET, Token Ring-NET, or TRBRF VLAN to follow.
ieee	IEEE Ethernet STP running source-route transparent (SRT) bridging.
ibm	IBM STP running source-route bridging (SRB).
auto	STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).
are	Number of all-routes explorer (ARE) hops to follow. This keyword applies only to TRCRF VLANs.
are-number	Integer from 0 to 13 that defines the maximum number of ARE hops for this VLAN.
ste	Number of spanning-tree explorer (STE) hops to follow. This keyword applies only to TRCRF VLANs.
ste-number	Integer from 0 to 13 that defines the maximum number of STE hops for this VLAN.
backupcrf	Backup CRF mode to follow. This keyword applies only to TRCRF VLANs.
enable	Enable backup CRF mode for this VLAN.
disable	Disable backup CRF mode for this VLAN.
tb-vlan1 and **tb-vlan2**	(Optional) First and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example.
tb-vlan1-id and *tb-vlan2-id*	Integer that ranges from 0 to 1005.

Defaults

The *vlan-name* variable is *VLANxxxx*, where *xxxx* represents four numeric digits (including leading zeroes) equal to the VLAN ID number.

The media type is **ethernet**.

The state is **active**.

The SAID value is 100000 plus the VLAN ID.

The MTU size for Ethernet, FDDI, and FDDI-NET VLANs is 1500 bytes. The MTU size for Token Ring and Token Ring-NET VLANs is 1500 bytes. The MTU size for TRBRF and TRCRF VLANs is 4472 bytes.

The ring number for Token Ring VLANs is zero. For FDDI VLANs, there is no default. For TRCRF VLANs, you must specify a ring number.

The bridge number is zero (no source-routing bridge) for FDDI-NET and Token Ring-NET VLANs. For TRBRF VLANs, you must specify a bridge number.

The parent VLAN ID is zero (no parent VLAN) for FDDI and Token Ring VLANs. For TRCRF VLANs, you must specify a parent VLAN ID. For both Token Ring and TRCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TRBRF VLAN.

The STP type is **ieee** for FDDI-NET VLANs. For Token Ring-NET and TRBRF VLANs, the default is **ibm**.

The ARE value is 7.

The STE value is 7.

Backup CRF is disabled.

The *tb-vlan1-id* and *tb-vlan2-id* variables are zero (no translational bridging).

Command Mode

VLAN database

Usage Guidelines

When the **no vlan** *vlan-id* form is used, the VLAN is deleted. Deleting VLANs automatically resets to zero any other parent VLANs and translational bridging parameters that refer to the deleted VLAN.

When the **no vlan** *vlan-id* **name** *vlan-name* form is used, the VLAN name returns to the default name (*VLANxxxx*, where *xxxx* represent four numeric digits (including leading zeroes) equal to the VLAN ID number).

When the **no vlan** *vlan-id* **media** form is used, the media type returns to the default (**ethernet**). Changing the VLAN media type (including the **no** form) resets the VLAN MTU to the default MTU for the type (unless the **mtu** keyword is also present in the command). It also resets the VLAN parent and translational bridging VLAN to the default (unless the **parent**, **tb-vlan1**, and/or **tb-vlan2** are also present in the command).

When the **no vlan** *vlan-id* **state** form is used, the VLAN state returns to the default (**active)**.

When the **no vlan** *vlan-id* **said** form is used, the VLAN SAID returns to the default (100,000 plus the VLAN ID).

When the **no vlan** *vlan-id* **mtu** form is used, the VLAN MTU returns to the default for the applicable VLAN media type. You can also modify the MTU using the **media** keyword.

When the **no vlan** *vlan-id* **ring** form is used, the VLAN logical ring number returns to the default (0).

When the **no vlan** *vlan-id* **bridge** form is used, the VLAN source-routing bridge number returns to the default (0). The **vlan** *vlan-id* **bridge** command is only used for FDDI-NET and Token Ring-NET VLANs and is ignored in other VLAN types.

When the **no vlan** *vlan-id* **parent** form is used, the parent VLAN returns to the default (0). The parent VLAN resets to the default if the parent VLAN is deleted or if the **media** keyword changes the VLAN type or the VLAN type of the parent VLAN.

When the **no vlan** *vlan-id* **stp type** form is used, the VLAN spanning-tree type returns to the default (ieee).

When the **no vlan** *vlan-id* **tb-vlan1** or **no vlan** *vlan-id* **tb-vlan2** form is used, the VLAN translational bridge VLAN (or VLANs, if applicable) returns to the default (0). Translational bridge VLANs must be a different VLAN type than the affected VLAN, and if two are specified, the two must be different VLAN types from each other. A translational bridge VLAN resets to the default if the translational bridge VLAN is deleted, if the **media** keyword changes the VLAN type, or if the **media** keyword changes the VLAN type of the corresponding translation bridge VLAN.

Examples

The following example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of *VLANxxx*, where *xxxx* represents four numeric digits (including leading zeroes) equal to the VLAN ID number. The default **media** option is **ethernet**; the **state** option is **active**. The default *said-value* variable is 100000 plus the VLAN ID; the *mtu-size* variable is 1500; the **stp-type** option is **ieee**. The VLAN is added if it did not already exist; otherwise, this command does nothing.

```
Switch(vlan)# vlan 2
```

The following example shows how to modify an existing VLAN by changing its name and MTU size:

```
Switch(vlan)# no vlan name engineering mtu 1200
```

You can verify the previous commands by entering the **show vlan** command in privileged EXEC mode.

Related Commands

show vlan

vlan database

Use the **vlan database** privileged EXEC command to enter VLAN database mode from the command-line interface (CLI). From the CLI, you can add, delete, and modify VLAN configurations and globally propagate these changes using the VLAN Trunk Protocol (VTP). This command is available only in the Enterprise Edition Software.

vlan database

Syntax Description

This command has no arguments or keywords.

Default

No default is defined.

Command Mode

Privileged EXEC

Usage Guidelines

To return to the privileged EXEC mode from the VLAN database mode, enter the **exit** command.

Note This command mode is different from other modes because it is session oriented. When you add, delete, or modify VLAN parameters, the changes are not applied until you exit the session by entering the **apply** or **exit** commands. When the changes are applied, the VTP configuration version is incremented. You can also not apply the changes to the VTP database by entering **abort**.

Example

The following example shows how to enter the VLAN database mode from the privileged EXEC mode:

```
Switch# vlan database
Switch(vlan)#
```

Related Commands

abort
apply
exit
reset
shutdown vlan

vmps reconfirm (Privileged EXEC)

Use the **vmps reconfirm** privileged EXEC command to immediately send VLAN Query Protocol (VQP) queries to reconfirm all dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS). This command is available only in the Enterprise Edition Software.

vmps reconfirm

Syntax Description

This command has no arguments or keywords.

Default

No default is defined.

Command Mode

Privileged EXEC

Example

The following example shows how to immediately send VQP queries to the VMPS:

```
Switch# vmps reconfirm
```

You can verify the previous command by entering the **show vmps** command in privileged EXEC mode and examining the VMPS Action row of the Reconfirmation Status section. The **show vmps** command shows the result of the last time the assignments were reconfirmed either as a result of reconfirmation timer expiring or because the **vmps reconfirm** command was issued.

Related Commands

show vmps
vmps reconfirm

vmps reconfirm (Global Configuration)

Use the **vmps reconfirm** global configuration command to change the reconfirmation interval for the VLAN Query Protocol (VQP) client. This command is available only in the Enterprise Edition Software.

vmps reconfirm *interval*

Syntax Description

interval	Reconfirmation interval for VQP client queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments. The interval range is from 1 to 120 minutes.

Default

The default reconfirmation interval is 60 minutes.

Command Mode

Global configuration

Example

The following example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:

```
Switch(config)# vmps reconfirm 20
```

You can verify the previous command by entering the **show vmps** command in privileged EXEC mode and examining information in the Reconfirm Interval row.

Related Commands

show vmps
vmps reconfirm

vmps retry

Use the **vmps retry** global configuration command to configure the per-server retry count for the VLAN Query Protocol (VQP) client. This command is available only in the Enterprise Edition Software.

vmps retry *count*

Syntax Description

count Number of attempts to contact the VLAN Membership Policy Server (VMPS) by the client before querying the next server in the list. The retry range is from 1 to 10.

Default

The default retry count is 3.

Command Mode

Global configuration

Example

The following example shows how to set the retry count to 7:

```
Switch(config)# vmps retry 7
```

You can verify the previous command by entering the **show vmps** command in privileged EXEC mode and examining information in the Server Retry Count row.

Related Commands

show vmps

vmps server

Use the **vmps server** global configuration command to configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers. Use the **no** form of this command to remove a VMPS server. This command is available only in the Enterprise Edition Software.

vmps server *ipaddress* [**primary**]
no vmps server [*ipaddress*]

Syntax Description

ipaddress	IP address or host name of the primary or secondary VMPS servers. If you specify a host name, the Domain Name System (DNS) server must be configured.
primary	(Optional) Determines whether primary or secondary VMPS servers are being configured.

Default

No primary or secondary VMPS servers are defined.

Command Mode

Global configuration

Usage Guidelines

The first server entered is automatically selected as the primary server whether or not **primary** is entered. The first server address can be overridden by using **primary** in a subsequent command.

If a member switch in a cluster configuration does not have an IP address, the cluster does not use the VMPS server configured for that member switch. Instead, the cluster uses the VMPS server on the command switch, and the command switch proxies the VMPS requests. The VMPS server treats the cluster as a single switch and uses the IP address of the command switch to respond to requests.

When using the **no** form without specifying the *ipaddress*, all configured servers are deleted. If you delete all servers when dynamic-access ports are present, the switch cannot forward packets from new sources on these ports because it cannot query the VMPS.

Examples

The following example shows how to configure the server with IP address 191.10.49.20 as the primary VMPS server, and the servers with IP addresses 191.10.49.21 and 191.10.49.22 as secondary servers:

```
Switch(config)# vmps server 191.10.49.20 primary
Switch(config)# vmps server 191.10.49.21
Switch(config)# vmps server 191.10.49.22
```

The following example shows how to delete the server with IP address 191.10.49.21:

```
Switch(config)# no vmps server 191.10.49.21
```

You can verify the previous commands by entering the **show vmps** command in privileged EXEC mode and examining information in the VMPS Domain Server row.

Related Commands

show vmps

vtp

Use the **vtp** VLAN database command to configure the VLAN Trunk Protocol (VTP) mode. Use the **no** form of this command to return to the default setting. This command is available only in the Enterprise Edition Software.

vtp {**server** | **client** | **transparent**}
no vtp {**server** | **client** | **transparent**}

Syntax Description

server Place the switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.

client Place the switch in VTP client mode. A switch in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not transmit VTP advertisements until it receives advertisements to initialize its VLAN database.

transparent Place the switch in VTP transparent mode. A switch in VTP transparent mode is disabled for VTP, does not transmit advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. The configuration of multi-VLAN ports causes the switch to automatically enter transparent mode.

Note The switch supports up to 250 VLANs on the Catalyst 2912MF XL, Catalyst 2924M XL, Catalyst 3508G, and Catalyst 3524 XL switches. All other switches support up to 64 VLANs. If you define more than 250 or 64, respectively, or if the switch receives an advertisement that contains more than 250 or 64 VLANs, the switch automatically enters VTP transparent mode and operates with the VLAN configuration preceding the one that put it into transparent mode. The count of 250 or 64 VLANs always includes VLAN 1 but never includes VLANs 1002 to 1005. The switch can have 250 or 64 active VLANs, plus VLANs 1002 through 1005, which are inactive.

Default

Server mode is the default mode.

Command Mode

VLAN database

Usage Guidelines

The **no vtp client** and **no vtp transparent** forms of the command return the switch to VTP server mode.

The **vtp server** command is the same as **no vtp client** or **no vtp transparent** except that it does not return an error if the switch is not in client or transparent mode.

Example

The following example shows how to place the switch in VTP transparent mode:

```
Switch(vlan)# vtp transparent
```

You can verify the previous commands by entering the **show vtp status** command in privileged EXEC mode.

Related Commands

show vtp status

vtp domain

Use the **vtp domain** VLAN database command to configure the VLAN Trunk Protocol (VTP) administrative domain. This command is available only in the Enterprise Edition Software.

vtp domain *domain-name*

Syntax Description

domain-name	ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.

Default

No domain name is defined.

Command Mode

VLAN database

Usage Guidelines

The switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not transmit any VTP advertisements even if changes occur to the local VLAN configuration. The switch leaves the no-management-domain state after receiving the first VTP summary packet on any port that is currently trunking or after configuring a domain name using the **vtp domain** command. If the switch receives its domain from a summary packet, it resets its configuration revision number to zero. After the switch leaves the no-management-domain state, it can never be configured to reenter it until you clear the NVRAM and reload the software.

Domain names are case sensitive.

Once you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

Example

The following example shows how to set the administrative domain for the switch:

```
Switch(vlan)# vtp domain OurDomainName
```

You can verify the previous commands by entering the **show vtp status** command in privileged EXEC mode.

Related Commands

show vtp status
vtp password

vtp file

Use the **vtp file** global configuration command to modify the VLAN Trunk Protocol (VTP) configuration storage filename. Use the **no** form of this command to return the filename to its default name. This command is available only in the Enterprise Edition Software.

vtp file *ifsfilename*
no vtp file

Syntax Description

ifsfilename	The IOS IFS filename where the VTP VLAN configuration is stored.

Default

The default filename is *flash:vlan.dat*.

Command Mode

Global configuration

Usage Guidelines

This command cannot be used to load a new database; it only renames the file in which the existing database is stored.

Example

The following example shows how to rename the filename for VTP configuration storage to *vtpfilename*:

```
Switch(config)# vtp file vtpfilename
```

Related Commands

vtp

vtp password

Use the **vtp password** VLAN database command to configure the VLAN Trunk Protocol (VTP) administrative domain password. Use the **no** form of this command to remove the password. This command is available only in the Enterprise Edition Software.

vtp password *password-value*
no vtp password *password-value*

Syntax Description

password Set the password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements.

password-value ASCII string from 8 to 64 characters. The password is case sensitive.

Default

No password is defined.

Command Mode

VLAN database

Usage Guidelines

Passwords are case sensitive. Passwords should match on all switches in the same domain.

When the **no vtp password** form of the command is used, the switch returns to the no password state.

Example

The following example shows how to configure the VTP domain password:

```
Switch(vlan)# vtp password ThisIsOurDomain’sPassword
```

Related Commands

vtp domain

vtp pruning

Use the **vtp pruning** VLAN database command to enable pruning in the VLAN Trunk Protocol (VTP) administrative domain. Use the **no** form of this command to disable pruning. This command is available only in the Enterprise Edition Software.

vtp pruning
no vtp pruning

Syntax Description

pruning	Enable pruning in the VTP administrative domain. If you enable pruning on the VTP server, it is enabled for the entire management domain. Only VLANs included in the pruning-eligible list can be pruned. For Catalyst 2900 series switches, no VLANs are pruning eligible on the trunk port.

Default

Pruning is disabled.

Command Mode

VLAN database

Example

The following example shows how to enable pruning in the proposed new VLAN database:

```
Switch(vlan)# vtp pruning
```

You can verify the previous commands by entering the **show vtp status** command in privileged EXEC mode.

Related Commands

show vtp status
vtp
vtp v2-mode

vtp v2-mode

Use the **vtp v2-mode** VLAN database command to enable VLAN Trunk Protocol (VTP) version 2 in the administrative domains. Use the **no** form of this command to disable V2 mode. This command is available only in the Enterprise Edition Software.

vtp v2-mode
no vtp v2-mode

Syntax Description

v2-mode Enable V2 mode in the VTP administrative domain. Each VTP switch automatically detects the capabilities of all the other VTP devices. To use V2 mode, all VTP switches in the network must support version 2; otherwise, you must configure them to operate in VTP version 1 mode (no vtp v2-mode).

If you are using VTP in a Token Ring environment, VTP V2 mode must be enabled.

If you are configuring a Token Ring bridge relay function (TRBRF) or Token Ring concentrator relay function (TRCRF) VLAN media type, you must use version 2.

If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use version 1.

Default

VTP version 2 is disabled.

Command Mode

VLAN database

Usage Guidelines

Toggling the V2 mode state modifies certain parameters of certain default VLANs.

Example

The following example shows how to enable V2 mode in the proposed new VLAN database:

```
Switch(vlan)# vtp v2-mode
```

You can verify the previous commands by entering the **show vtp status** command in privileged EXEC mode.

Related Commands

show vtp status
vtp
vtp pruning