verify

To verify the checksum of a file on a flash memory file system or compute an MD5 signature for a file, use the **verify** command.

verify {{{**/md5** *flash-filesystem*} [*expected-md5-signature*]} | {**/ios** *flash-filesystem*} | *flash-filesystem*}

Syntax Description

/md5 *flash-filesystem*	Computes an MD5 signature for a file; valid values are **bootflash:**, **disk0:**, **disk1:**, **flash:**, or **sup-bootflash:**.
expected-md5-signature	(Optional) MD5 signature.
/ios *flash-filesystem*	Verifies the compressed Cisco IOS image checksum; valid values are **bootflash:**, **disk0:**, **disk1:**, **flash:**, or **sup-bootflash:**.
flash-filesystem	Device where the flash memory resides; valid values are **bootflash:**, **disk0:**, **disk1:**, **flash:**, or **sup-bootflash:**.

Command Default

The default device is the current working device.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into the flash memory.

The Readme file, which is included with the image on the disk, lists the name, file size, and checksum of the image. Review the contents of the Readme file before loading or duplicating the new image so that you can verify the checksum when you copy it into the flash memory or onto a server.

Use the **verify /md5** command to verify the MD5 signature of a file before using it. This command validates the integrity of a copied file by comparing a precomputed MD5 signature with the signature that is computed by this command. If the two MD5 signatures match, the copied file is identical to the original file.

You can find the MD5 signature that is posted on the Cisco.com page with the image.

You can use the **verify /md5** command in one of the following ways:

- Verify the MD5 signatures manually by entering the **verify /md5** *filename* command.

  Check the displayed signature against the MD5 signature that is posted on the Cisco.com page.

- Allow the system to compare the MD5 signatures by entering the **verify /md5** {*flash-filesystem***:***filename*} {*expected-md5-signature*} command.

  After completing the comparison, the system returns with a verified message. If an error is detected, the output is similar to the following:

```
Router# verify /md5 disk0:c6msfc2-jsv-mz 0f
 ................................
 ................................
................................
 ................................
 ................................Done!
 %Error verifying disk0:c6msfc2-jsv-mz
 Computed signature  = 0f369ed9e98756f179d4f29d6e7755d3
 Submitted signature = 0f
```

To display the contents of the flash memory, enter the **show flash** command. The listing of the flash contents does not include the checksum of the individual files. To recompute and verify the image checksum after the image has been copied into the flash memory, enter the **verify** command.

A colon (:) is required after the specified device.

Examples

This example shows how to use the **verify** command:

```
Router# verify cat6k_r47_1.cbi
.....................................................
File cat6k_r47_1.cbi verified OK.
Router#
```

This example shows how to check the MD5 signature manually:

```
Router# verify /md5 c6msfc2-jsv-mz
 ..........................................
 ..........................................
..........................................
 ..........................................
 ........................................Done!
 verify /md5 (disk0:c6msfc2-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
Router#
```

This example shows how to allow the system to compare the MD5 signatures:

```
Router# verify /md5 disk0:c6msfc2-jsv-mz 0f369ed9e98756f179d4f29d6e7755d3
 ..........................................
 ..........................................
..........................................
 ..........................................
 ........................................Done!
 verified /md5 (disk0:c6sup12-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
Router#
```

This example shows how to verify the compressed checksum of the Cisco IOS image:

```
Router# verify /ios disk0:c6k222-jsv-mz
Verified compressed IOS image checksum for disk0:c6k222-jsv-mz
Router#
```

Related Commands

Command	Description
copy /noverify	Disables the automatic image verification for the current copy operation.
file verify auto	Verifies the compressed Cisco IOS image checksum.
show file systems (flash file system)	Lists available file systems.
show flash	Displays the layout and contents of flash memory.

vlan (config-VLAN submode)

To configure a specific VLAN, use the **vlan** command in config-VLAN submode. To delete a VLAN, use the **no** form of this command.

vlan *vlan-id*

no vlan *vlan*

Syntax Description

vlan-id	Number of the VLAN; valid values are from 1 to 4094.

Command Default

The defaults are as follows:

- *vlan-name* is "VLANxxxx" where "xxxx" represents four numeric digits (including leading zeroes) equal to the VLAN ID number.
- **media** *type* is **ethernet**.
- **state** is **active**.
- *said-value* is 100000 plus the VLAN ID number.
- *mtu-size* default is dependent upon the VLAN type:
  - **ethernet**—1500
  - **fddi**—1500
  - **trcrf**—1500 if V2 is not enabled, 4472 if it is enabled
  - **fd-net**—1500
  - **trbrf**—1500 if V2 is not enabled, 4472 if it is enabled
- *ring-number* is that no ring number is specified.
- *bridge-number* is that no bridge number is specified.
- *parent-vlan-id* is that no parent VLAN is specified.
- *type* is that no STP type is specified.
- *tb-vlan1* and *tb-vlan2* is 0, which means that no translational-bridge VLAN is specified.

Command Modes

config-VLAN submode

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

VLAN 1 parameters are factory configured and cannot be changed. You cannot delete VLAN 1.

Once you are in the config-VLAN submode, this syntax is available:

{**are** *hops*} {**backupcrf** *mode*} {**bridge** *type* | *bridge-num*} {**exit**} {**media** *type*} {**mtu** *mtu-size*} {**name** *vlan-name*} {**parent** *parent-vlan-id*} {**private-vlan**} {**remote-span**} {**ring** *ring-number*} {**said** *said-value*} {**shutdown**} {**state** {**suspend** | **active**}} {**stp type** *type*} {**ste** *hops*} {**tb-vlan1** *tb-vlan1-id*} {**tb-vlan2** *tb-vlan2-id*}

no {**are** | **backupcrf** | {**bridge** *type*} | **exit** | **media** | **mtu** | **name** | **parent** | **private-vlan** | **remote-span** | **ring** | **said** | **shutdown** | **state** | {**stp type** *type*} | {**ste** *hops*}}

are *hops*	Specifies the maximum number of All Route Explorer hops for this VLAN. Valid values are from 0 to 13; 0 is assumed if no value is specified.
backupcrf *mode*	Enables or disables the backup CRF mode of the VLAN; valid values are **enable** or **disable**.
bridge *type* | *bridge-num*	Specifies the bridging characteristics of the VLAN or identification number of the bridge; valid *type* values are **srb** or **srt**. Valid *bridge-num* values are from 0 to 15.
exit	Applies changes, increments the revision number, and exits config-VLAN submode.
media *type*	Specifies the media type of the VLAN; valid values are **ethernet**, **fd-net**, **fddi**, **trcrf**, and **trbrf**.
mtu *mtu-size*	Specifies the maximum transmission unit (packet size in bytes) that the VLAN can use; valid values are from 1500 to 18190.
name *vlan-name*	Defines a text string that is used as the name of the VLAN (1 to 32 characters).
parent *parent-vlan-id*	Specifies the ID number of the parent VLAN of FDDI or Token Ring-type VLANs; valid values are from 1 to 1005.
private-vlan	(Optional) Configures the VLAN as a PVLAN; see the **private-vlan** command.
remote-span	Configures the VLAN as an RSPAN VLAN.
ring *ring-number*	Specifies the ring number of FDDI or Token Ring-type VLANs; valid values are from 0 to 65535.
said *said-value*	Specifies the security-association identifier; valid values are from 1 to 4294967294.
shutdown	Shuts down VLAN switching.
state {**suspend** | **active**}	Specifies whether the state of the VLAN is active or suspended.
stp type *type*	Specifies the STP type; valid values are **ieee**, **ibm**, and **auto**.
ste *hops*	Specifies the maximum number of hops for Spanning Tree Explorer frames; valid values are from 0 to 13.
tb-vlan1 *tb-vlan1-id*	Specifies the ID number of the first translational VLAN for this VLAN. Valid values are from 1 to 1005; 0 is assumed if no value is specified.
tb-vlan2 *tb-vlan2-id*	Specifies the ID number of the second translational VLAN for this VLAN. Valid values are from 1 to 1005; 0 is assumed if no value is specified.

Caution If you enter the **shutdown** command and then the **no shutdown** command in the config-vlan mode on a PVLAN (primary or secondary), the PVLAN type and association information is deleted. You will have to reconfigure the VLAN to be a PVLAN.

The VLANs in the suspended state do not pass packets.

The VLANs that are created or modified are not committed until you exit config-VLAN submode.

If you define *vlan-range* in global configuration mode, you are not allowed to set the *vlan-name* in config-vlan submode.

The maximum length of a Layer 2 VLAN name is 32 characters.

Note If you attempt to add a new VLAN and the VLAN already exists, no action occurs.

For extended-range VLANs (1006 to 4094), only the **private-vlan, rspan**, and **mtu** VLAN parameters are configurable. The rest of the VLAN parameters for extended-range VLANs are set to default.

When you define *vlan-name*, the name must be unique within the administrative domain.

The SAID is documented in 802.10. When the **no** form is used, the VLAN's SAID is returned to the default. When you define the *said-value*, the name must be unique within the administrative domain.

The **bridge** *bridge-number* argument is used only for Token Ring-net and FDDI-net VLANs and is ignored in other types of VLANs. When the **no** form is used, the VLAN's source-routing bridge number returns to the default.

The parent VLAN resets to the default if the parent VLAN is deleted or the **media** keyword changes the VLAN type or the VLAN type of the parent VLAN.

The *tb-vlan1* and *tb-vlan2* are used to configure translational-bridge VLANs of a specified type of VLAN and are not allowed in other VLAN types. Translational-bridge VLANs must be different VLAN types than the affected VLAN; if two VLANs are specified, the two must be different VLAN types.

A translational-bridge VLAN resets to the default if you delete the translational-bridge VLAN or if you enter the **media** keyword to change the VLAN type or the VLAN type of the corresponding translational-bridge VLAN.

The **shutdown** keyword does not support extended-range VLANs.

To find out if a VLAN has been shut down internally, check the Status field in the **show vlan** command output. If a VLAN is shut down internally, these values appear in the Status field:

- act/ishut—VLAN status is active but shut down internally.
- sus/ishut—VLAN status is suspended but shut down internally.

Examples

This example shows how to add a new VLAN with all default parameters to the new VLAN database:

```
Router(config-vlan)# vlan 2
Router(config-vlan)#
```

This example shows how to cause the device to add a new VLAN, specify the media type and parent VLAN ID number 3, and set all other parameters to the defaults:

```
Router(config-vlan)# media ethernet parent 3
VLAN 2 modified:
    Media type ETHERNET
    Parent VLAN 3
Router(config-vlan)#
```

This example shows how to delete VLAN 2:

```
Router(config-vlan)# no vlan 2
Router(config-vlan)#
```

This example shows how to return to the default settings for the MTU for its type and translational-bridge VLANs:

```
Router(config-vlan)# no mtu tb-vlan1 tb-vlan2
Router(config-vlan)#
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

vlan (global configuration mode)

To add a VLAN and enter config-VLAN submode, use the **vlan** command. To delete the VLAN, use the **no** form of this command.

vlan {*vlan-id* | *vlan-range*}

no vlan {*vlan-id* | *vlan-range*}

Syntax Description

vlan-id	Number of the VLAN; valid values are from 1 to 4094.
vlan-range	Range of configured VLANs; see the "Usage Guidelines" section for a list of valid values.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

VLAN 1 parameters are factory configured and cannot be changed.

The specified VLAN is added or modified in the VLAN database when you exit config-VLAN submode.

When you enter the **vlan** *vlan-id* command, a new VLAN is created with all default parameters in a temporary buffer and causes the CLI to enter config-VLAN submode. If the *vlan-id* that you entered matches an existing VLAN, nothing happens except that you enter config-VLAN submode.

If you define *vlan-range*, you are not allowed to set the *vlan-name* in config-VLAN submode.

You can enter the *vlan-range* using a comma (**,**), a dash (**-**), and the number.

See the **vlan (config-VLAN submode)** command for information on the commands that are available in the config-VLAN submode.

Examples

This example shows how to add a new VLAN and enter config-VLAN submode:

```
Router (config)# vlan 2
Router (config-vlan)#
```

This example shows how to add a range of new VLANs and enter config-VLAN submode:

```
Router (config)# vlan 2,5,10-12,20,25,4000
Router (config-vlan)#
```

This example shows how to delete a VLAN:

```
Router (config)# no vlan 2
Router (config)#
```

Related Commands

Command	Description
vlan (config-VLAN submode)	Configures a specific VLAN.

vlan access-log

To configure the VACL-logging properties, including the log-table size, redirect-packet rate, and logging threshold, use the **vlan access-log** command. To return to the default settings, use the **no** form of this command.

vlan access-log {{**maxflow** *max-number*} | {**ratelimit** *pps*} | {**threshold** *pkt-count*}}

no vlan access-log {**maxflow** | **ratelimit** | **threshold**}

Syntax Description

maxflow *max-number*	Specifies the maximum log-table size. Valid values are from 0 to 2048; 0 deletes the contents of the log table.
ratelimit *pps*	Specifies the maximum redirect VACL-logging packet rate; valid values are from 0 to 5000.
threshold *pkt-count*	Specifies the logging-update threshold; valid values are from 0 to 2147483647. 0 means that the threshold is not set.

Command Default

The defaults are as follows:

- *max-number* is **500**.
- *pps* is **2000** pps.
- *pkt-count* is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Due to the rate-limiting function for redirected packets, VACL-logging counters may not be accurate.

Only denied IP packets are logged.

When the log-table size is full, the logging packets from the new flows are dropped by the software.

The packets that exceed the maximum redirect VACL-logging packet rate limit are dropped by the hardware.

A logging message is displayed if the flow threshold is reached before the 5-minute interval.

If you do not configure the maximum log-table size, maximum packet rate, or threshold, or if you enter the **no** form of the commands, the default values are assumed.

Examples

This example shows how to set the maximum log-table size:

```
Router(config)# vlan access-log maxflow 500
Router(config)#
```

This example shows how to set the maximum redirect VACL-logging packet rate after which packets are dropped:

```
Router(config)# vlan access-log ratelimit 200
Router(config)#
```

This example shows how to set the logging-update threshold:

```
Router(config)# vlan access-log threshold 3500
Router(config)#
```

Related Commands

Command	Description
show vlan access-log	Displays information about the VACL logging including the configured logging properties.

vlan access-map

To create a VLAN access map or enter VLAN access-map command mode, use the **vlan access-map** command. To remove a mapping sequence or the entire map, use the **no** form of this command.

vlan access-map *name* [*seq#*]

no vlan access-map *name* [*seq#*]

Syntax Description

name	VLAN access-map tag.
seq#	(Optional) Map sequence number; valid values are 0 to 65535.

Command Default

This command has no default settings.

Command Default

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

If you enter the sequence number of an existing map sequence, you enter VLAN access-map mode.

If you do not specify a sequence number, a number is automatically assigned. You can enter one match clause and one action clause per map sequence.

If you enter the **no vlan access-map name** [*seq#*] command without entering a sequence number, the whole map is removed.

Once you enter VLAN access-map mode, the following commands are available:

- **action**—Specifies the packet action clause; see the **action** command section.
- **default**—Sets a command to its defaults.
- **end**—Exits from configuration mode.
- **exit**—Exits from VLAN access-map configuration mode.
- **match**—Specifies the match clause; see the **match** command section.
- **no**—Negates a command or sets its defaults.

Examples

This example shows how to enter VLAN access-map mode:

```
Router(config)# vlan access-map Bob
Router(config-access-map)#
```

Related Commands

Command	Description
action	Sets the packet action clause.
match	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.
show vlan access-map	Displays the contents of a VLAN-access map.

vlan database

To enter VLAN-configuration submode, use the **vlan database** command.

vlan database

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

After you are in VLAN-configuration submode, you can access the **manipulation** commands in the VLAN-database editing buffer, including:

- **abort**—Exits mode without applying the changes.
- **apply**—Applies current changes and increments the revision number.
- **exit**—Applies changes, increments the revision number, and exits mode.
- **no**—Negates a command or sets its defaults; valid keywords are **vlan** and **vtp**.
- **reset**—Abandons current changes and releases the current database.
- **show**—Displays database information.
- **vlan**—Accesses subcommands to add, delete, or modify values that are associated with a single VLAN. For information about the **vlan** subcommands, see the **vlan (config-VLAN submode)** command.
- **vtp**—Accesses subcommands to perform VTP administrative functions. For information about the **vtp** subcommands, see the **vtp** command.

Examples

This example shows how to enter VLAN-configuration mode:

```
Router# vlan database
Router(vlan)#
```

This example shows how to exit VLAN-configuration mode without applying changes after you are in VLAN-configuration mode:

```
Router(vlan)# abort
Aborting....
Router#
```

This example shows how to delete a VLAN after you are in VLAN-configuration mode:

```
Router(vlan)# no vlan 100
Deleting VLAN 100...
Router(vlan)#
```

This example shows how to turn off pruning after you are in VLAN-configuration mode:

```
Router(vlan)# no vtp pruning
Pruning switched OFF
Router(vlan)#
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

vlan dot1q tag native

To enable dot1q tagging for all VLANs in a trunk, use the **vlan dot1q tag native** command. To clear the configuration, use the **no** form of this command.

vlan dot1q tag native

no vlan dot1q tag native

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

The **vlan dot1q tag native** command configures the switch to tag native-VLAN traffic and admit only 802.1Q-tagged frames on 802.1Q trunks, dropping any untagged traffic, including untagged traffic in the native VLAN.

Follow these configuration guidelines when configuring Layer 2-protocol tunneling:

- On all the service-provider edge switches, you must enable spanning-tree BPDU filtering on the 802.1Q-tunnel ports by entering the **spanning-tree bpdufilter enable** command.
- Ensure that at least one VLAN is available for native-VLAN tagging. If you use all the available VLANs and then enter the **vlan dot1q tag native** command, native-VLAN tagging is not enabled.
- On all the service-provider core switches, enter the **vlan dot1q tag native** command to tag native-VLAN egress traffic and drop untagged native-VLAN ingress traffic.
- On all the customer switches, either enable or disable native-VLAN tagging on each switch.

Note If you enable dot1q tagging on one switch and disable it on another switch, all traffic is dropped; you must identically configure dot1q tagging on each switch.

Examples

This example shows how to enable dot1q tagging for all VLANs in a trunk:

```
Router(config)# vlan dot1q tag native
Router(config)#
```

Related Commands

Command	Description
show vlan dot1q tag native	Displays native VLAN-tagging information.

vlan filter

To apply a VLAN access map, use the **vlan filter** command. To clear the VLAN access maps from VLANs or interfaces, use the **no** form of this command.

vlan filter *map-name* {**vlan-list** *vlan-list* | **interface** *interface number*}

no vlan filter *map-name* {**vlan-list** [*vlan-list*] | **interface** [*interface interface-number*]}

Syntax Description

map-name	VLAN access-map tag.
vlan-list	VLAN list; valid values are from 1 to 4094.
interface *interface*	Specifies the interface type; valid values are **pos**, **atm**, or **serial**. See the "Usage Guidelines" section for additional information.
interface-number	Interface number; see the "Usage Guidelines" section for additional information.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

When configuring an action clause in a VLAN access map, note the following:

- You can apply the VLAN access map to one or more VLANs or WAN interfaces.
- The *vlan-list* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges (*vlan-id-vlan-id*). Multiple entries are separated by a hyphen (-) or a comma (,).
- If you delete a WAN interface that has a VACL applied, the VACL configuration on the interface is also removed.
- You can apply only one VLAN access map to each VLAN or WAN interface.
- VACLs that are applied to VLANs are active only for VLANs with a Layer 3-VLAN interface configured. VACLs that are applied to VLANs without a Layer 3-VLAN interface are inactive. Applying a VLAN access map to a VLAN without a Layer 3-VLAN interface creates an administratively down Layer 3-VLAN interface to support the VLAN access map. If creation of the Layer 3-VLAN interface fails, the VACL is inactive.

When entering the **no** form of this command, the *vlan-list* argument is optional (but the keyword **vlan-list** is required). If you do not enter the *vlan-list* argument, the VACL is removed from all VLANs where the *map-name* argument is applied.

When entering the **no** form of this command for WAN interfaces, the *interface* argument is optional (but the **interface** keyword is required). If you do not enter the *interface* argument, the VACL is removed from interfaces where the *map-name* is applied.

The **vlan filter** *map-name* **interface** command accepts only ATM, POS, or serial interface types. If your Catalyst 6500 series switch is not configured with any of these interface types, the **interface** *interface interface-number* keyword and argument are not provided.

The *interface-number* format can be *mod*/*port* or *slot*/*port-adapter*/*port*; it can include a subinterface or channel-group descriptor.

Examples

This example shows how to apply a VLAN access map on VLANs 7 through 9:

```
Router(config)# vlan filter ganymede vlan-list 7-9
Router(config)#
```

Related Commands

Command	Description
action	Sets the packet action clause.
match	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.
show vlan filter	Displays information about the VLAN filter.

vlan internal allocation policy

To configure the allocation direction of the internal VLAN, use the **vlan internal allocation policy** command. To return to the default settings, use the **no** form of this command.

vlan internal allocation policy {**ascending** | **descending**}

no vlan internal allocation policy

Syntax Description

ascending	Allocates internal VLANs from 1006 to 4094.
descending	Allocates internal VLANs from 4094 to 1006.

Command Default

ascending

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

You can configure internal VLAN allocation to be from 1006 and up or from 4094 and down.

Internal VLANs and user-configured VLANs share the 1006 to 4094 VLAN spaces. A first in, first out (FIFO) policy is used in allocating these spaces.

You must perform a system reboot before the **vlan internal allocation policy** command changes can take effect. During system bootup, internal VLANs that are required for features in the startup-config file are allocated first. The user-configured VLANs in the startup-config file are configured next. If you configure a VLAN that conflicts with an existing internal VLAN, the VLAN that you configured is put into a nonoperational status until the internal VLAN is freed and becomes available.

After you enter the **write memory** command and the system reloads, the reconfigured allocation is used by the port manager.

Examples

This example shows how to configure VLANs in a descending order as the internal VLAN-allocation policy:

```
Router(config)# vlan internal allocation policy descending
Router(config)#
```

Related Commands

Command	Description
show vlan internal usage	Displays information about the internal VLAN allocation.

vlan mapping dot1q

To map an 802.1Q VLAN to an ISL VLAN, use the **vlan mapping dot1q** command. To remove a specified mapping or all 802.1Q VLAN-to-ISL VLAN mappings, use the **no** form of this command.

vlan mapping {**dot1q** *dot1q-vlan-id*} {**isl** *isl-vlan-id*}

no vlan mapping {**dot1q** *dot1q-vlan-id* | **all**}

Syntax Description

dot1q *dot1q-vlan-id*	Specifies the VLAN ID of the 802.1Q VLAN from which the mapping occurs as traffic leaves and enters 802.1Q trunks on the local device; valid values are from 1 to 4094.
isl *isl-vlan-id*	Specifies the VLAN ID of the ISL VLAN onto which the mapping occurs as traffic leaves and enters 802.1Q trunks on the local device and specifies the VLAN ID of the 802.1Q VLAN for which to discard traffic as it arrives at a local device; valid values are from 1 to 4094.
all	Removes all 802.1Q VLAN-to-ISL VLAN mappings.

Command Default

The default for 802.1Q VLAN IDs 1 to 4094 is an identity mapping.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

VLAN 1 parameters are factory configured and cannot be changed.

You can map up to eight VLANs. You can map only one 802.1Q VLAN to an ISL VLAN. For example, if 802.1Q VLAN 800 has been automatically mapped to ISL VLAN 800, do not manually map any other 802.1Q VLANs to ISL VLAN 800.

You cannot overwrite existing 802.1Q-VLAN mapping. If the 802.1Q-VLAN number already exists, the command is aborted. You must first clear that mapping.

If the table is full, the command is aborted with an error message indicating that the table is full.

Examples

This example shows how to map traffic arriving on 802.1Q trunks on VLAN 1001 to ISL VLAN 888 on the local device, discard traffic arriving on 802.1Q trunks on VLAN 888, and map traffic on ISL VLAN 888 on the local device to 802.1Q VLAN 1001 as it leaves the device:

```
Router(config)# vlan mapping dot1q 1001 isl 888
Router(config)#
```

This example shows how to clear the mapping of 802.1Q VLAN 1001 to ISL VLAN 888. The result is that 802.1Q VLAN 1001 traffic is discarded when it arrives on the local device, and 802.1Q VLAN 888 traffic is mapped to ISL VLAN 888 (both are their default states):

```
Router(config)# no vlan mapping dot1q 1001
No mapping for 1022
Router(config)#
```

Related Commands

Command	Description
show vlan	Displays VLAN information.
vlan (config-VLAN submode)	Configures a specific VLAN.
vlan database	Enters VLAN-configuration submode.

vtp

To configure the global VTP state, use the **vtp** command. To return to the default value.

vtp {**domain** *domain-name*}

vtp {**file** *filename*}

vtp {**interface** *interface-name*} [**only**]

vtp {**mode** {**client** | **server** | **transparent**}}

vtp {**password** *password-value*}

vtp pruning

vtp {**version** {**1** | **2**}}

Syntax Description

domain *domain-name*	Sets the VTP-administrative domain name.
file *filename*	Sets the ASCII name of the IFS-file system file where the VTP configuration is stored.
interface *interface-name*	Sets the name of the preferred source for the VTP-updater ID for this device.
only	(Optional) Specifies to use only this interface's IP address as the VTP-IP updater address.
mode client	Sets the type of VTP-device mode to client mode.
mode server	Sets the type of VTP-device mode to server mode.
mode transparent	Sets the type of VTP-device mode to transparent mode.
password *password-value*	Specifies the adminstrative-domain password.
pruning	Enables the adminstrative domain to permit pruning.
version 1 | 2	Specifies the adminstrative-domain VTP-version number.

Command Default

The defaults are as follows:

- **vtp domain** and **vtp interface** commands have no default settings.
- *filename* is **const-nvram:vlan.dat**.
- VTP mode is **mode server**.
- No password is configured.
- Pruning is disabled.
- **version 1**.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Note The **vtp pruning**, **vtp password**, and **vtp version** commands are also available in privileged EXEC mode. We recommend that you use these commands in global configuration mode only; do not use these commands in privileged EXEC mode.

Extended-range VLANs are not supported by VTP.

When you define the *domain-name*, the domain name is case sensitive and can be from 1 to 32 characters.

The *filename* and *interface-name* are ASCII strings from 1 to 255 characters.

You must configure a password on each network device in the management domain when the switch is in secure mode.

Caution If you configure VTP in secure mode, the management domain does not function properly if you do not assign a management domain password to each network device in the domain.

A VTP version 2-capable network device can operate in the same VTP domain as a network device running VTP version 1 if VTP version 2 is disabled on the VTP version 2-capable network device (VTP version 2 is disabled by default).

Do not enable VTP version 2 on a network device unless all of the network devices in the same VTP domain are version 2 capable. When you enable VTP version 2 on a network device, all of the version 2-capable network devices in the domain enable VTP version 2.

In a Token Ring environment, you must enable VTP version 2 for VLAN switching to function properly.

Enabling or disabling VTP pruning on a VTP server enables or disables VTP pruning for the entire management domain.

Configuring VLANs as pruning eligible or pruning ineligible on a Catalyst 6500 series switch affects pruning eligibility for those VLANs on that switch only; it does not affect pruning eligibility on all network devices in the VTP domain.

The **vtp password**, **vtp pruning**, and **vtp version** commands are not placed in NVGEN but are included in the VTP transparent-mode startup configuration file.

Extended-range VLANs are not supported by VTP.

You can configure **pruning** in VTP-server mode; **version** is configurable in VTP-server mode or VTP transparent mode.

The *password-value* is an ASCII string from 8 to 64 characters identifying the administrative domain for the device.

VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.

All Catalyst 6500 series switches in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on Catalyst 6500 series switches in the same VTP domain.

If all Catalyst 6500 series switches in a domain are VTP version 2 capable, you need to enable VTP version 2 on one Catalyst 6500 series switch; the version number is then propagated to the other version 2-capable Catalyst 6500 series switch in the VTP domain.

If you toggle the version 2 mode, certain default VLAN parameters are modified. See the *Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide—Release 12.2ZY* for additional information.

Examples

This example shows how to set the device's management domain:

```
Router(config)# vtp domain DomainChandon
Router(config)#
```

This example shows how to specify the file in the IFS-file system where the VTP configuration is stored:

```
Router(config)# vtp file vtpconfig
Setting device to store VLAN database at filename vtpconfig.
Router(config)#
```

This example shows how to set the VTP mode to client:

```
Router(config)# vtp mode client
Setting device to VTP CLIENT mode.
Router(config)#
```

Related Commands

Command	Description
show vtp	Displays the VTP statistics and domain information.

wrr-queue

To allocate the bandwidth between the standard transmit SRR, DWRR, or WRR queues, use the **wrr-queue** command. To return to the default settings, use the **no** form of this command.

wrr-queue [**bandwidth** | **shape**] {**percent** *low-priority-queue-percentage* [*intermediate-priority-queue-percentages*] *high-priority-queue-percentage*}

wrr-queue [**bandwidth** | **shape**] {**percent** *low-priority-queue-weight* [*intermediate-priority-queue-weight*] *high-priority-queue-weight*}

no wrr-queue [**bandwidth** | **shape**]

Syntax Description

bandwidth	(Optional) Enters the **bandwidth** keyword to configure DWRR or WRR.
shape	(Optional) Enters the **shape** keyword to configure SRR.
percent *low-priority-queue-percentage*	(Optional) Specifies the minimum percentage; valid values are from 1 to 100.
intermediate-priority-queue-percentage	(Optional) Intermediate percentage; valid values are from 1 to 100.
high-priority-queue-percentage	Maximum percentage; valid values are from 1 to 100.
low-priority-queue-weight	Minimum weight; valid values are from 1 to 255.
intermediate-priority-queue-weight	(Optional) Intermediate weight; valid values are from 1 to 255.
high-priority-queue-weight	Maximum weight; valid values are from 1 to 255.

Command Default

The defaults are listed in Table 2-96.

Table 2-96 Bandwidth Default Values

Port Types	Default Value
2q8t	90:10
8q4t	90:0:0:0:0:0:0:10
8q8t	90:0:0:0:0:0:0:10
1p7q8t	22:33:45:0:0:0:0
1p2q1t	100:255
2q2t, 1p2q2t, and 1p2q1t	5:255
1p3q1t	100:150:255

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.

Usage Guidelines

Shaped round robin (SRR) allows a queue to use only the allocated bandwidth. SRR is supported as an option on Supervisor Engine 32 SFP 1p3q8t ports and on 1p7q4t ports. Use of SRR prevents use of the strict priority queue. To configure SRR, any CoS or DSCP values mapped to a strict-priority queue must be remapped to a standard queue.

DWRR keeps track of any lower-priority queue under-transmission caused by traffic in a higher-priority queue and compensates in the next round. DWRR is the dequeuing algorithm on 1p3q1t, 1p2q1t, 1p3q8t, 1p7q4t, and 1p7q8t ports.

WRR allows a queue to use more than the allocated bandwidth if the other queues are not using any, up to the total bandwidth of the port. WRR is the dequeuing algorithm on all other ports.

The higher the percentage or weight that is assigned to a queue, the more transmit bandwidth is allocated to it. If you enter weights, the ratio of the weights divides the total bandwidth of the queue. For example, for three queues on a Gigabit Ethernet port, weights of 25:25:50 provide this division:

- Queue 1—250 Mbps
- Queue 2—250 Mbps
- Queue 3—500 Mbps

WRR allows bandwidth sharing at the egress port. This command defines the bandwidths for egress WRR through scheduling weights.

The WRR weights are used to partition the bandwidth between the queues if all queues are nonempty. For example, entering weights of 1:3 means that one queue gets 25 percent of the bandwidth and the other queue gets 75 percent.

Entering weights of 1:3 do not necessarily lead to the same results as entering weights at 10:30. Weights at 10:30 mean that more data is serviced from each queue and the latency of packets being serviced from the other queue goes up. You should set the weights so that at least one packet (maximum size) can be serviced from the lower priority queue at a time. For the higher priority queue, set the weights so that multiple packets are serviced at any one time.

Percentages should add up to 100. You must enter percentages for all the standard transmit queues on the port.

The valid values for weight range from 1 to 255. You must enter weights for all the standard transmit queues on the port.

Examples

This example shows how to allocate a three-to-one bandwidth ratio:

```
Router(config-if)# wrr-queue bandwidth 3 1
Router(config-if)#
```

Related Commands

Command	Description
show queueing interface	Displays queueing information.
wrr-queue queue-limit	Sets the transmit-queue size ratio on an interface.