udld through vtp v2-mode

udld

To enable the aggressive mode or the normal mode in the UniDirectional Link Detection (UDLD) protocol and to set the configurable message time, use the **udld** command in global configuration mode. To disable the aggressive mode or the normal mode in UDLD, use the **no** form of this command.

udld {**aggressive | enable | message time** *seconds*}

no udld {**aggressive | enable | message**}

Syntax Description

aggressive	Enables UDLD in the aggressive mode on all fiber interfaces.
enable	Enables UDLD in the normal mode on all fiber interfaces.
message time *seconds*	Sets the time, in seconds, between the UDLD probe messages on ports that are in advertisement mode and are currently determined to be bidirectional. Valid values are from 7 to 90. The default is 15.

Command Default

The UDLD is disabled on all fiber interfaces.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced.
12.2(17D)SXB	This command was integrated into Cisco IOS Release 12.2(17D)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

This command affects fiber interfaces only. Use the **udld port** command in interface configuration mode to enable UDLD on other interface types.

If you enable the aggressive mode, after all the neighbors of a port age out either in the advertisement phase or in the detection phase, UDLD restarts the linkup sequence to resynchronize with any potentially out-of-sync neighbor and shuts down the port if the message train from the link is still undetermined.

Examples

The following example shows how to enable the UDLD in the normal mode on all fiber interfaces:

```
Router(config)# udld enable
```

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD statuses.
udld port	Enables UDLD on the Ethernet interface or enables UDLD in the aggressive mode on the Ethernet interface.
udld recovery	Enables the recovery timer for the UDLD error-disabled state.
udld reset	Resets all the LAN ports that are error disabled by UDLD.

udld port

To enable the UniDirectional Link Detection (UDLD) protocol on the Ethernet interface or to enable the UDLD in the aggressive mode on the Ethernet interface, use the **udld port** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

udld port [**aggressive** | **disable**]

no udld port [**aggressive** | **disable**]

Syntax Description

aggressive	(Optional) Enables UDLD in the aggressive mode on the Ethernet interface. See the "Usage Guidelines" section for additional information.
disable	(Optional) Disables UDLD on a fiber-optic LAN port. **Note** This command is supported only on the fiber-optic LAN ports.

Command Default

If **udld port** command is not enabled on the Ethernet interfaces, UDLD will follow the global configuration settings on the fiber interfaces and UDLD will be disabled on the nonfiber interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	This command was introduced.
12.2(17D)SXB	This command was integrated into Cisco IOS Release 12.2(17D)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(2)SNG	This command was integrated into Cisco IOS Release 15.1(2)SNG.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

This command is used only on Ethernet ports.

Use the **udld port** and **udld port aggressive** commands on fiber ports to override the setting of the global **udld** (**enable** or **aggressive**) command. Use the **no** form of the **udld port** command on fiber ports to remove this setting and return the control of the UDLD-enabling task to the global **udld** command or to disable UDLD in case of the nonfiber ports.

If you enable the aggressive mode, after all the neighbors of a port age out either in the advertisement phase or in the detection phase, UDLD restarts the linkup sequence to resynchronize with any potentially out-of-sync neighbor and shuts down the port if the message train from the link is still undetermined.

If the port changes from fiber to nonfiber or vice versa, all the configurations are maintained because the platform software detects a change of module or a Gigabit Interface Converter (GBIC) change.

Examples

The following example shows how to cause a port interface to enable UDLD regardless of the current global **udld** command setting:

```
Router(config-if)# udld port
```

The following example shows how to cause a port interface to enable UDLD in the aggressive mode regardless of the current global **udld** (**enable** or **aggressive**) setting:

```
Router(config-if)# udld port aggressive
```

The following example shows how to cause a fiber port interface to disable the UDLD regardless of the current global **udld** setting:

```
Router(config-if)# udld port disable
```

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD statuses.
udld	Enables the aggressive mode or the normal mode in UDLD and sets the configurable message time.
udld recovery	Enables the recovery timer for the UDLD error-disabled state.
udld reset	Resets all the LAN ports that are error disabled by UDLD.

udld recovery

To configure the UniDirectional Link Detection (UDLD) protocol auto recovery mechanism, use the **udld recovery** command in global configuration mode. To return to the default state, use the **no** form of this command.

udld recovery [**interval** *seconds*]

no udld recovery

Syntax Description

interval *seconds*	Time, in seconds, to recover from a specified error-disabled state. The range is from 30 to 86400. The default is 300.

Command Default

The auto recovery mechanism is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

If you do not enable UDLD recovery, the interface stays in the error-disabled state until UDLD is reset. If you enable UDLD recovery, the interface is brought out of the error-disabled state and allowed to retry the unidirectional link detection process again.

Examples

The following example shows how to enable the recovery timer:

```
Router(config)# udld recovery
```

The following example shows how to set the recovery timer to 200 seconds:

```
Router(config)# udld recovery interval 200
```

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD statuses.

Command	Description
udld	Enables the aggressive mode or the normal mode in UDLD and sets the configurable message time.
udld port	Enables UDLD on the Ethernet interface or enables UDLD in the aggressive mode on the Ethernet interface.
udld reset	Resets all the LAN ports that are error disabled by UDLD.

udld reset

To reset all the ports that are error disabled by the UniDirectional Link Detection (UDLD) protocol and allow traffic to pass through them again (although other features, such as spanning tree, Port Aggregation Protocol [PAgP], and Dynamic Trunking Protocol [DTP], will behave normally if enabled), use the **udld reset** command in the privileged EXEC mode.

udld reset

Syntax Description

This command has no arguments or keywords.

Command Default

The ports that are error disabled are not reset.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)SX	This command was introduced.
12.2(17D)SXB	This command was integrated into Cisco IOS Release 12.2(17D)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

If the interface configuration is enabled for UDLD, the ports will begin to run UDLD again and may be error disabled if the reason for error disabling is not corrected.

Examples

The following example shows how to reset all the ports that are error disabled by UDLD:

```
Router# udld reset
```

Related Commands

Command	Description
show udld	Displays the administrative and operational UDLD statuses.
udld	Enables the aggressive mode or the normal mode in UDLD and sets the configurable message time.

Command	Description
udld port	Enables UDLD on the Ethernet interface or enables UDLD in the aggressive mode on the Ethernet interface.
udld recovery	Enables the recovery timer for the UDLD error-disabled state.

vlan (global)

To add a VLAN and enter config-VLAN submode, use the **vlan** command in global configuration mode. 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. See the "Usage Guidelines" section for details on configuring VLAN ID numbers.
vlan-range	Range of configured VLANs; see the "Usage Guidelines" section for details on configuring ranges of VLAN ID numbers.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

VLAN 1 parameters are factory configured and cannot be changed.

VLAN 1 and VLANs 1002-1005 are default VLANs. Default VLANs are created automatically and cannot be configured or deleted by users.

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, any configuration commands you enter in config-VLAN submode will apply to the existing VLAN. You will not create a new VLAN.

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

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

VLAN IDs in the range from 1006 to 4094 are considered "extended VLAN IDs." Beginning in Cisco IOS Release 12.4(15)T, you can configure extended VLAN IDs on the following routers:

- Cisco 800 series routers, including models 851, 857, 871, 876, 877, 878
- Cisco 1700 series routers, including models 1711, 1712, 1751, 1751V, 1760
- Cisco 1800 series routers, including models 1801, 1802, 1803, 1811, 1812, 1841
- Cisco 2600 series routers, including models 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM, 2691
- Cisco 2800 series routers, including models 2801, 2811, 2821, 2851
- Cisco 3600 series routers, including models 3620, 3640, 3640A, 3660
- Cisco 3700 series routers, including models 3725, 3745
- Cisco 3800 series routers, including models 3825, 3845

The reduced MAC address feature is required to support 4000 VLANs. Cisco IOS Release 12.1(14)E1 and later releases support chassis with 64 or 1024 MAC addresses. For chassis with 64 MAC addresses, Spanning Tree Protocol (STP) uses the extended system ID (which is the VLAN ID) plus a MAC address to make the bridge ID unique for each VLAN. (Without the reduced MAC address support, 4096 VLANs would require 4096 MAC addresses on the switch.)

If you configure extended VLANs, you must also enable the spanning-tree extended system-ID feature.

The legacy vlan database mode does not support extended VLAN configuration.

See the **vlan(config-VLAN)** command for information on the commands that are available under 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)	Configures a specific VLAN.

vlan (VLAN)

To configure a specific VLAN, use the **vlan** command in VLAN configuration mode. To delete a VLAN, use the **no** form of this command.

vlan *vlan-id* [**are** *hops*] [**backupcrf** *mode*] [**bridge** *type*| *bridge-number*] [**media** *type*] [**mtu** *mtu-size*] [**name** *vlan-name*] [**parent** *parent-vlan-id*] [**ring** *ring-number*] [**said** *sa-id-value*] [**state** {**suspend**| **active**}] [**stp type** *type*] [**tb-vlan1** *tb-vlan1-id*] [**tb-vlan2** *tb-vlan2-id*]

no vlan *vlan-id*

Syntax Description

vlan id	Number of the VLAN; valid values are from 2 to 1001.
are *hops*	(Optional) Specifies the maximum number of All Route Explorer hops for this VLAN. Valid values are from 0 to 13. Zero is assumed if no value is specified.
backupcrf *mode*	(Optional) Enables or disables the backup concentrator relay function (CRF) mode of the VLAN; valid values are **enable** or **disable**.
bridge *type* | *bridgenumber*	(Optional) Specifies the bridging characteristics of the VLAN or identification number of the bridge; valid type values are **srb** or **srt**. Valid *bridgenumber*values are from 0 to 15.
media *type*	(Optional) Specifies the media type of the VLAN; valid values are **ethernet**, **fd-net**, **fddi**, **trcrf**, and **trbrf**.
mtu *mtu -size*	(Optional) Specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from 576 to 18190.
name *vlan -name*	(Optional) Defines a text string used as the name of the VLAN (1 to 32 characters).
parent *parent -vlan-id*	(Optional) Specifies the ID number of the parent VLAN for FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
ring *ring -number*	(Optional) Specifies the ring number of FDDI or Token Ring-type VLANs; valid values are from 2 to 1001.
said *sa-id -value*	(Optional) Specifies the security association identifier; valid values are from 1 to 4294967294

state {**suspend** | **active**}	(Optional) Specifies whether the state of the VLAN is active or suspended. VLANs in suspended state do not pass packets.
stp type *type*	(Optional) Specifies the Spanning Tree Protocol (STP) type; valid values are **ieee**, **ibm**, and **auto**.
tb vlan1 *tb vlan1 id*	(Optional) Specifies the ID number of the first translational VLAN for this VLAN; valid values are from 2 to 1001. Zero is the default value.
tb vlan2 *tb vlan2 id*	(Optional) Specifies the ID number of the second translational VLAN for this VLAN; valid values are from 2 to 1001. Zero is the default value.

Command Default

The defaults are as follows:

- *vlan -name* --VLAN*xxxx* where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.
- **media** *type* --ethernet.
- **state** --Active.
- *said -value* --100000 plus the VLAN ID number.
- *mtu -size* --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* --No ring number is specified.
- *bridge -number* --No bridge number is specified.
- *parent -vlan -id* --No parent VLAN is specified.
- *type* --No STP type is specified.
- **tb -vlan1** and **tb-vlan2**--0, which means no translational bridge VLAN is specified.

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.1(1)E	Support for this command on the Catalyst 6000 series switch was extended to the E train.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX train.

Usage Guidelines

This command was replaced by the vlan (config-VLAN)command but is kept for backward compatibility.

This command is not supported in Cisco 7600 series routers that are configured with a Supervisor Engine 720.

This command, which is similar to the VLAN 1 parameters, are configured at the factory and cannot be changed.

Extended-range VLANs are not supported in VLAN configuration mode.

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

The security association ID (SAID) is documented in 802.10. When the **no**form is used, the VLAN's SAID is returned to the default value.

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

The *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 value.

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** keywords are used to configure translational bridge VLANs of a specified type and are not allowed in other types of VLANs. Translational bridge VLANs must differ in type from the affected VLAN; if two VLANs are specified, the two must be different VLAN types.

A translational bridge VLAN resets to the default if the translational bridge VLAN is deleted or the **media** keyword changes the VLAN type or the VLAN type of the corresponding translational bridge VLAN.

Examples

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

```
Router(vlan)# vlan 2
```

Note If the VLAN already exists, no action occurs.

The following 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(vlan)# vlan 2 media ethernet parent 3
VLAN 2 modified:
    Media type ETHERNET
    Parent VLAN 3
```

The following example shows how to delete VLAN 2:

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

The following example shows how to return the maximum transmission unit (MTU) to the default for its type and return translational bridging VLANs to the default:

```
Router(vlan)# no vlan 2 mtu tb-vlan1 tb-vlan2
```

Related Commands

Command	Description
show vlan	Displays VLAN information.
vlan database	Enters VLAN configuration mode.

vlan access-log

To configure the VLAN access control list (VACL)-logging properties, including the log-table size, redirect-packet rate, and logging threshold, use the **vlan access-log** command in global configuration. 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 in Cisco IOS 12.2SX releases.
- *pps* is **0** pps Cisco IOS release 12.2(50)SY and later.
- *pkt-count* is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY. Added a new default for the **ratelimit** keyword.

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
```

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
```

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

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

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 **vlanaccess-map** command in global configuration. To remove a mapping sequence or the entire map, use the **no** form of this command.

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

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

Syntax Description

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

Command Default

A VLAN access map is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 **novlanaccess-mapname** [*seq-number*] 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 tagname1
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 accounting

To configure accounting information about VLAN, use the **vlanaccounting**command in global configuration mode. To remove the accounting information, use the **no** form of this command.

vlan accounting {**input**| **output**}

no vlan accounting {**input**| **output**}

Syntax Description

input	Specifies the incoming accounting information.
output	Specifies the outgoing accounting information.

Command Default

The accounting information about VLAN is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to configure incoming accounting information about VLAN:

```
Router# enable
Router# configure terminal
Router(config)# vlan accounting input
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

vlan database

Note The **vlandatabase** command is not available in Cisco IOS Release 12.2(33)SXI5 and later Cisco IOS 12.2SX releases.

To enter VLAN configuration mode, use the**vlandatabase**command in privileged EXEC mode.

vlan database

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN configuration mode is not entered.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6500 series switches.
12.1(1)E	Support for this command on the Catalyst 6500 series switches was extended to the E release.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelin

Note If you are running in RPR+ mode on a Cisco 7600 series router or Catalyst 6500 series switch, do not configure a VLAN in VLAN-database mode. Performance problems might occur during configuration synchronization between the active and standby supervisor engines.

Once you are in VLAN configuration mode, you can access the VLAN database editing buffer manipulation commands, including:

- **abort** --Exits themode without applying the changes.
- **apply** --Applies current changes and increases the release number.
- **exit** --Applies changes, increases the release number, and exit mode.
- **no** --Negates a command or sets its defaults; valid values are **vlan** and **vtp**.
- **reset** --Abandons current changes and rereads the current database.
- **show** --Displays database information.
- **vlan** --Accesses subcommands to add, delete, or modify values associated with a single VLAN. For information about the **vlan** subcommands, see the **vlan** (VLAN) command.
- **vtp** --Accesses subcommands to perform Virtual Trunking Protocol (VTP) administrative functions. For information about the **vtp** subcommands, see the **vtpclient** command.

Examples

The following example shows how to enter VLAN configuration mode:

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

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

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

The following 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 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 (802.1Q) tagging for all VLANs in a trunk, use the **vlandot1qtagnative**command in global configuration mode. 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

Dot1q (802.1Q) tagging for all VLANs in a trunk is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **vlandot1qtagnative** 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 bridge protocol data unit (BPDU) filtering on the 802.1Q-tunnel ports by entering the **spanning-treebpdufilterenable** command.
- Ensure that at least one VLAN is available for native-VLAN tagging. If you use all the available VLANs and then enter the **vlandot1qtagnative**command, native-VLAN tagging is not enabled.
- On all the service-provider core switches, enter the **vlandot1qtagnative** 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 **vlanfilter** command in global configuration mode. 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 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. See the "Usage Guidelines" section for additional information on the *vlan-list*argument.
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

A VLAN access map is not applied.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 VLAN access control list (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 **vlanfilter***map-name***interface** command accepts only ATM, POS, or serial interface types. If your Cisco 7600 series router is not configured with any of these interface types, the **interface***interfaceinterface-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 ifdescr detail

To enable the Cisco device to provide detailed display information for VLAN subinterfaces in ifDescr format, use the **vlanifdescrdetail**command in global configuration mode. To disable this functionality, use the **no** form of this command.

vlan ifdescr detail

no vlan ifdescr detail

Syntax Description

This command has no arguments or keywords.

Command Default

Information about VLAN subinterfaces is not displayed.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to enable the display information for VLAN interfaces:

```
Router# configure terminal
Router(config)# vlan ifdescr detail
```

Related Commands

Command	Description
show vlan	Displays VLAN information.

vlan internal allocation policy

To configure the allocation direction of the internal VLAN, use the **vlaninternalallocationpolicy** command in global configuration mode. To the default setting, use the **no** form of this command to return.

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(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.(2)SNG	This command was implemented on Cisco ASR 901Series Aggregation Service Routers.

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 come, first served” policy is used in allocating these spaces.

You must perform a system reboot before the **vlaninternalallocationpolicy** 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 **writemem** 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 Inter-Switch Link (ISL) VLAN, use the **vlanmappingdot1q** command in global configuration mode. 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(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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 (VLAN)	Configures a specific VLAN.
vlan database	Enters VLAN-configuration submode.

vlan port provisioning

To enable VLAN port provisioning verification, use the **vlanportprovisioning** command in global configuration mode. To disable VLAN port provisioning verification, use the **no** form of this command.

vlan port provisioning

no vlan port provisioning

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN port provisioning verification is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

When you enable the VLAN port provisioning, you must specify the VLAN name in order to change a port from one VLAN to another.

When VLAN port provisioning is enabled, you can still create new VLANs, but you cannot add ports to the VLAN without specifying both the VLAN number and the VLAN name. The feature does not affect assigning ports to VLANs using other features such as Simple Network Management Protocol (SNMP), dynamic VLANs, and 802.1X.

Examples

The following example shows how to enable VLAN port provisioning on all ports:

```
Router(config)# vlan port provisioning
```

The following example shows how to disable VLAN port provisioning on all ports:

```
Router(config)# no vlan port provisioning
```

Related Commands

Command	Description
show vlan port provisioning	Displays the VLAN port provisioning status.

vtp (global)

To configure the global VLAN Trunking Protocol (VTP) state, use the **vtp** command in global configuration mode. To return to the default value, use the **no** form of this command.

vtp {**domain** *domain-name*| **file** *filename*| **interface** *interface-name* **[only]**| **mode** {**client**| **off**| **server**| **transparent**}| **password** *password-value*| **pruning**| **version** {**1**| **2**}}

no vtp

vtp {**domain** *domain-name*| **file** *filename*| **interface** *interface-name* **[only]**| **mode** {**client**| **off**| **server** [**mst**| **unknown**| **vlan**]| **transparent**}| **password** *password-value* [**hidden**| **secret**]| **pruning**| **version** {**1**| **2**| **3**}}

no vtp

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 off	Sets the type of VTP-device mode to off 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 administrative-domain password.
pruning	Enables the administrative domain to permit pruning.
Catalyst 6500 Series Switch	
hidden	(Optional) Configures the password with a secret key saved in hexadecimal format in the running configuration. Supported on the Catalyst 6500 series switch only.
secret	(Optional) Allows the password secret key to be directly configured. Supported on the Catalyst 6500 series switch only.

mst	Sets the mode for Multiple Spanning-Tree (MST) VTP instance.
unknown	Sets the mode for unknown VTP features.
vlan	Sets the mode for VLAN VTP instance.
version {1 | 2 | 3}	Specifies the administrative-domain VTP-version number.

Command Default

The defaults are as follows:

- **vtp domain** and **vtpinterface** co mmands have no default settings.
- *filename* is const-nvram:vlan.dat .
- VTP mode is **modeserver**.
- No password is configured.
- Pruning is disabled.
- Administrative-domain VTP-version number 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The **modeoff**keyword combination was added.
12.2(33)SXI	The following changes were made for the Catalyst 6500 series switch: • **vtp mode** {**client** | **off** | **server** [**mst** | **unknown** | **vlan**] | **transparent**]} • **vtp password** *password-value* [**hidden** | **secret** • **vtp version** {**1** | **2**|**3**}
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelin

Note The **vtppruning**, **vtppassword**, and **vtpversion** 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 version 1 and version 2. Extended range VLANs are supported in VTP version 3.

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

The *filename* and *interface-name*values 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 an applicable device 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 **vtppassword**, **vtppruning**, and **vtpversion** commands are not placed in startup memory but are included in the VTP transparent-mode startup configuration file.

Extended-range VLANs are not supported by VTP.

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

The password-value argument 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 applicable devices in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on applicable devices in the same VTP domain.

If all applicable devices in a domain are VTP version 2-capable, you need only to enable VTP version 2 on one applicable devices; the version number is then propagated to the other version 2-capable applicable devices in the VTP domain.

If you toggle the version 2 mode, certain default VLAN parameters are modified.

If you enter the **vtpmodeoff** command, it sets the device to off. If you enter the **novtpmodeoff** command, it resets the device to the VTP server mode.

Catalyst 6500 Series Switch

VTP version 3 supports all the features in version 1 and version 2. VTP version 3 also supports the following features not supported in version 1 and version 2:

- Enhanced authentication--In VTP version 3, you can configure the authentication password to be hidden using the **vtppassword** command. When you configure the authentication password to be hidden, it does not appear in plain text in the configuration. Instead, the secret associated with the password is saved in hexadecimal format in the running configuration. The password-string argument is an ASCII string from 8 to 64 characters identifying the administrative domain for the device. The following syntax is available:

password *password-string* [**hidden** | **secret**]

password *password-string* --Specifies the administrative domain password.

hidden --(Optional) Configures the password with a secret key saved in hexadecimal format in the running configuration.

secret --(Optional) Allows the password secret key to be directly configured in hexadecimal format.

The **hidden** keyword for the VTP password is supported only in VTP version 3. If converting to VTP version 2 from VTP version 3, you must remove the **hidden** keyword prior to the conversion.

- Support for extended-range VLAN database propagation--VTP version 1 and version 2 support VLANs 1 to 1000 only. In VTP version 3, the entire VLAN range is supported (VLANs 1 to 4096). The pruning of VLANs still applies to VLANs 1 to 1000 only. Extended-range VLANs are supported in VTP version 3 only. If converting from VTP version 3 to VTP version 2, VLANs in the range 1006 to 4094 are removed from VTP control.
- Support for propagation of any database in a domain--In VTP version 1 and version 2, a VTP server is used to backup the database to the NVRAM and allows you to change the database information. In VTP version 3, there is a VTP-primary server and a VTP-secondary server. A primary server allows you to alter the database information, and the database updates sent out are honored by all the devices in the system. A secondary server can only back up the updated VTP configuration received from the primary server in the NVRAMs. The status of the primary and secondary servers is a runtime status and is not configurable.

By default, all devices come up as secondary servers. You can enter the **vtpprimary** privileged EXEC mode command to specify a primary server. The following syntax is available:

vtp primary [**vlan** | **mst**] [**force**

vlan --(Optional) Specifies this device as the primary server for the VTP VLAN feature.

mst-- (Optional) Specifies this device as the primary server for the VTP MST feature.

force-- (Optional) Forces this device to become the primary server.

The primary-server status is needed only when database changes have to be performed and is obtained when the administrator issues a takeover message in the domain. The primary-server status is lost when you reload, switch over, or the domain parameters change. The secondary servers back up the configuration and continue to propagate the database. You can have a working VTP domain without any primary servers.

In VTP version 3, there is no longer a restriction to propagate only VLAN database information. You can use VTP version 3 to propagate any database information across the VTP domain. A separate instance of the protocol is running for each application that uses VTP.

- CLI to turn off/on VTP on a per-trunk basis--You can disable VTP on a per-trunk basis using the **novtp**command in interface configuration mode . When you disable VTP on the trunking port, all the VTP instances for that port are disabled. You will not be provided with the option of setting VTP to OFF for the MST database and ON for the VLAN database. You can enable VTP on a per-trunk basis using the **vtp**command in interface configuration mode .

VTP on a global basis--When you set VTP mode to OFF globally, this applies to all the trunking ports in the system. Unlike the per-port configuration, you can specify the OFF option on a per-VTP instance basis. For example, the system could be configured as VTP-server for the VLAN database and as VTP-off for the MST database. In this case, VLAN databases are propagated by VTP, MST updates are sent out on the trunk ports in the system, and the MST updates received by the system are discarded.

Examples

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

```
Router(config)#
vtp domain DomainName1
```

The following 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.
```

The following example shows how to set the VTP mode to client:

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

The following example shows how to disable VTP mode globally:

```
Router(config)# vtp mode off
Setting device to VTP OFF mode.
```

The following example shows how to reset the device to the VTP server mode:

```
Router(config)# no vtp mode off
Setting device to VTP OFF mode.
```

Related Commands

Command	Description
show vtp	Displays the VTP statistics and domain information.
vtp (interface)	Enables VTP on a per-port basis.

vtp (interface)

To enable VLAN Trunking Protocol (VTP) on a per-port basis, use the **vtp** command in interface configuration mode. To disable VTP on a per-port basis, use the **no** form of this command.

vtp

no vtp

Syntax Description

This command has no arguments or keywords.

Command Default

VTP on a per-port basis is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

The VTP enable value is applied only when a port becomes a switched port and is in trunk mode.

Examples

This example shows how to enable VTP on a per-port basis:

```
Router(config-if)# vtp
```

This example shows how to disable VTP on a per-port basis:

```
Router(config-if)# no vtp
```

Related Commands

Command	Description
vtp mode	Globally configures VTP mode.

vtp client

To place the device in Virtual Trunking Protocol (VTP) client mode, use the **vtpclient** command in VLAN configuration mode. To return to VTP server mode, use the **no** form of this command.

vtp client

no vtp client

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN mode

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, be sure to make all VTP or VLAN configuration changes on a switch in server mode.

The **vtpserver** command is the functional equivalent of **novtpclient**command except that it does not return an error if the device is not in client mode.

Examples

The following example shows how to place the device in VTP client mode:

```
Router(vlan)# vtp client
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global)	Modifies the name of the VTP configuration storage file.
vtp server	Places a device in VTP server mode.
vtp transparent	Places a device in VTP transparent mode.

vtp domain

To create the administrative domain name for the device, use the **vtpdomain** command in VLAN configuration mode. To delete the administrative domain name, use the **no** form of this command.

vtp domain *domain-name*

no vtp domain

Syntax Description

domain -name	Domain name. Domain names can be a maximum of 32 characters.

Command Default

The administrative domain name is not created.

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you define the *domainname* argument, the domain name is case-sensitive.

Until a domain name is set, the device is in the no-management-domain state. In this state, the device does not transmit any VLAN Trunking Protocol (VTP) advertisements regardless of changes to local VLAN configuration. The device leaves the no-management-domain state upon receiving the first VTP summary packet on any port that is currently trunking or when it receives a domain name configured by the **vtpdomain** command. If the device receives its domain from a summary packet, it resets its configuration revision number to 0.

When the device leaves the no-management-domain state, it can never be configured to reenter it, except by the cleaning of NVRAM and the reloading of the device.

Examples

The following example shows how to set the device's administrative domain to DomainChandon:

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

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global)	Modifies the name of the VTP configuration storage file.

vtp password

To create a Virtual Trunking Protocol (VTP) domain password, use the **vtppassword**command in VLAN configuration mode. To delete the password, use the **no** form of this command.

vtp password *password-value*

no vtp password

Syntax Description

password value	The password. The value is an ASCII string from 1 to 32 characters.

Command Default

The default is no password.

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.1(1)E	Support for this command on the Catalyst 6000 series switches was extended to the E train.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The value of the *passwordvalue* argument is an ASCII string from 1 to 32 characters.

Examples

The following example shows how to create the VTP domain password for DomainChandon:

```
Router(vlan)# vtp password DomainChandon
```

The following example shows how to delete the VTP domain password:

```
Router(vlan)# no vtp password
Clearing device VLAN database password.
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global)	Modifies the name of the VTP configuration storage file.

vtp server

To place the device in Virtual Trunking Protocol (VTP) server mode, use the **vtpserver** command in VLAN configuration mode.

vtp server

Syntax Description

This command has no arguments or keywords.

Command Default

The default is VTP server mode.

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.1(1)E	Support for this command on the Catalyst 6000 series switches was extended to the E train.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all the switches in the same VTP domain.

VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

If the receiving switch is in server mode, the configuration is not changed.

The **vtpserver** command is the functional equivalent of the **novtpclient** command, except that it does not return an error if the device is not in client mode.

Examples

The following example shows how to place the device in VTP server mode:

```
Router(vlan)# vtp server
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global)	Modifies the name of the VTP configuration storage file.
vtp client	Places a device in VTP client mode.
vtp transparent	Places a device in VTP transparent mode.

vtp transparent

To place the device in Virtual Trunking Protocol (VTP) transparent mode, use the **vtptransparent** command in VLAN configuration mode. To return to VTP server mode, use the **no** form of this command.

vtp transparent

no vtp transparent

Syntax Description

This command has no arguments or keywords.

Command Default

The default is VTP server mode.

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.1(1)E	Support for this command on the Catalyst 6000 series switches was extended to the E train.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The**vtptransparent**command disables VTP from the domain but does not remove the domain from the switch.

If the receiving switch is in transparent mode, the configuration is not changed. Switches in transparent mode do not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to the other switches in the network.

The **vtpserver** command is similar to the **novtptransparent**command, except that it does not return an error if the device is not in transparent mode.

Examples

The following example shows how to place the device in VTP transparent mode:

```
Router(vlan)# vtp transparent
```

The following example shows how to return the device to VTP server mode:

```
Router(vlan)# no vtp transparent
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global)	Modifies the name of the VTP configuration storage file.
vtp client	Places a device in VTP client mode.
vtp server	Places a device in VTP server mode.

vtp v2-mode

To enable Virtual Trunking Protocol (VTP) version 2 mode, use the**vtpv2-mode** command in VLAN configuration mode. To disable version 2 mode, use the **no** form of this command.

vtp v2-mode

no vtp v2-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Version 2 mode is disabled.

Command Modes

VLAN configuration (vlan)

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 series switches.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1) E on the Catalyst 6000 series switches.
12.2(2)XT	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

If you toggle the version 2 mode, parameters of certain default VLANs are modified.

Examples

The following example shows how to enable version 2 mode in the VLAN database:

```
Router(vlan)# vtp v2-mode
```

The following example shows how to disable version 2 mode in the VLAN database:

```
Router(vlan)# no vtp v2-mode
```

Related Commands

Command	Description
show vtp	Displays VTP statistics and domain information.
vtp (global)	Modifies the name of the VTP configuration storage file.