VLAN Commands

clear vmps statistics

To clear the VLAN Membership Policy Server (VMPS) statistics maintained by the VLAN Query Protocol (VQP) client, use the **clear vmps statistics** command in privileged EXEC mode.

clear vmps statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

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

```
Controller# clear vmps statistics
```

You can verify that information was deleted by entering the **show vmps statistics** privileged EXEC command.

clear vtp counters

To clear the VLAN Trunking Protocol (VTP) and pruning counters, use the **clear vtp counters** command in privileged EXEC mode.

clear vtp counters

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to clear the VTP counters:

```
Controller# clear vtp counters
```

You can verify that information was deleted by entering the **show vtp counters** privileged EXEC command.

debug sw-vlan

To enable debugging of VLAN manager activities, use the **debug sw-vlan** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan {**badpmcookies**| **cfg-vlan** {**bootup**| **cli**}| **events**| **ifs**| **mapping**| **notification**| **packets**| **redundancy**| **registries**| **vtp**}

no debug sw-vlan {**badpmcookies**| **cfg-vlan** {**bootup**| **cli**}| **events**| **ifs**| **mapping**| **notification**| **packets**| **redundancy**| **registries**| **vtp**}

Syntax Description

badpmcookies	Displays debug messages for VLAN manager incidents of bad port manager cookies.
cfg-vlan	Displays VLAN configuration debug messages.
bootup	Displays messages when the switch is booting up.
cli	Displays messages when the command-line interface (CLI) is in VLAN configuration mode.
events	Displays debug messages for VLAN manager events.
ifs	Displays debug messages for the VLAN manager IOS file system (IFS). See debug sw-vlan ifs, on page 6 for more information.
mapping	Displays debug messages for VLAN mapping.
notification	Displays debug messages for VLAN manager notifications. See debug sw-vlan notification, on page 7 for more information.
packets	Displays debug messages for packet handling and encapsulation processes.
redundancy	Displays debug messages for VTP VLAN redundancy.
registries	Displays debug messages for VLAN manager registries.
vtp	Displays debug messages for the VLAN Trunking Protocol (VTP) code. See debug sw-vlan vtp, on page 9 for more information.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug sw-vlan** command is the same as the **no debug sw-vlan** command.

Examples

This example shows how to display debug messages for VLAN manager events:

```
Controller# debug sw-vlan events
```

debug sw-vlan ifs

To enable debugging of the VLAN manager IOS file system (IFS) error tests, use the **debug sw-vlan ifs** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan ifs {**open** {**read**| **write**}| **read** {**1**| **2**| **3**| **4**}| **write**}

no debug sw-vlan ifs {**open** {**read**| **write**}| **read** {**1**| **2**| **3**| **4**}| **write**}

Syntax Description

open read	Displays VLAN manager IFS file-read operation debug messages.
open write	Displays VLAN manager IFS file-write operation debug messages.
read	Displays file-read operation debug messages for the specified error test (**1**, **2**, **3**, or **4**).
write	Displays file-write operation debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

When selecting the file read operation, Operation **1** reads the file header, which contains the header verification word and the file version number. Operation **2** reads the main body of the file, which contains most of the domain and VLAN information. Operation **3** reads type length version (TLV) descriptor structures. Operation **4** reads TLV data.

Examples

This example shows how to display file-write operation debug messages:

```
Controller# debug sw-vlan ifs write
```

debug sw-vlan notification

To enable debugging of VLAN manager notifications, use the **debug sw-vlan notification** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan notification {**accfwdchange| allowedvlancfgchange| fwdchange| linkchange| modechange| pruningcfgchange| statechange**}

no debug sw-vlan notification {**accfwdchange| allowedvlancfgchange| fwdchange| linkchange| modechange| pruningcfgchange| statechange**}

Syntax Description

accfwdchange	Displays debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
allowedvlancfgchange	Displays debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
fwdchange	Displays debug messages for VLAN manager notification of spanning-tree forwarding changes.
linkchange	Displays debug messages for VLAN manager notification of interface link-state changes.
modechange	Displays debug messages for VLAN manager notification of interface mode changes.
pruningcfgchange	Displays debug messages for VLAN manager notification of changes to the pruning configuration.
statechange	Displays debug messages for VLAN manager notification of interface state changes.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

Examples

This example shows how to display debug messages for VLAN manager notification of interface mode changes:

```
Controller# debug sw-vlan notification
```

debug sw-vlan vtp

To enable debugging of the VLAN Trunking Protocol (VTP) code, use the **debug sw-vlan vtp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan vtp {**events**| **packets**| **pruning** [**packets**| **xmit**]| **redundancy**| **xmit**}

no debug sw-vlan vtp {**events**| **packets**| **pruning**| **redundancy**| **xmit**}

Syntax Description

events	Displays debug messages for general-purpose logic flow and detailed VTP messages generated by the VTP_LOG_RUNTIME macro in the VTP code.
packets	Displays debug messages for the contents of all incoming VTP packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer, except for pruning packets.
pruning	Displays debug messages generated by the pruning segment of the VTP code.
packets	(Optional) Displays debug messages for the contents of all incoming VTP pruning packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer.
xmit	(Optional) Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send.
redundancy	Displays debug messages for VTP redundancy.
xmit	Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send, except for pruning packets.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug sw-vlan vtp** command is the same as the **no debug sw-vlan vtp** command.

If no additional parameters are entered after the **pruning** keyword, VTP pruning debugging messages appear. They are generated by the VTP_PRUNING_LOG_NOTICE, VTP_PRUNING_LOG_INFO, VTP_PRUNING_LOG_DEBUG, VTP_PRUNING_LOG_ALERT, and VTP_PRUNING_LOG_WARNING macros in the VTP pruning code.

Examples

This example shows how to display debug messages for VTP redundancy:

```
Controller# debug sw-vlan vtp redundancy
```

interface vlan

To create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode, use the **interface vlan** command in global configuration mode. To delete an SVI, use the **no** form of this command.

interface vlan *vlan-id*

no interface vlan *vlan-id*

Syntax Description

vlan-id	VLAN number. The range is 1 to 4094.

Command Default

The default VLAN interface is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

SVIs are created the first time you enter the **interface vlan** *vlan-id* command for a particular VLAN. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.

Note When you create an SVI, it does not become active until it is associated with a physical port.

If you delete an SVI using the **no interface vlan** *vlan-id* command, it is no longer visible in the output from the **show interfaces** privileged EXEC command.

Note You cannot delete the VLAN 1 interface.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but the previous configuration is gone.

The interrelationship between the number of SVIs configured on a switch or a switch stack and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables.

You can verify your setting by entering the **show interfaces** and **show interfaces vlan** *vlan-id* privileged EXEC commands.

Examples

This example shows how to create a new SVI with VLAN ID 23 and enter interface configuration mode:

```
Controller(config)# interface vlan 23
Controller(config-if)#
```

remote-span

To configure a VLAN as a Remote Switched Port Analyzer (RSPAN) VLAN, use the **remote-span** command in VLAN configuration mode on the switch stack or on a standalone switch. To remove the RSPAN designation from the VLAN, use the **no** form of this command.

remote-span

no remote-span

Syntax Description

This command has no arguments or keywords.

Command Default

No RSPAN VLANs are defined.

Command Modes

VLAN configuration (config-VLAN)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If VLAN Trunking Protocol (VTP) is enabled, the RSPAN feature is propagated by VTP for VLAN IDs that are lower than 1005. If the RSPAN VLAN ID is in the extended range, you must manually configure intermediate switches (those in the RSPAN VLAN between the source switch and the destination switch).

Before you configure the RSPAN **remote-span** command, use the **vlan** (global configuration) command to create the VLAN.

The RSPAN VLAN has these characteristics:

- No MAC address learning occurs on it.
- RSPAN VLAN traffic flows only on trunk ports.
- Spanning Tree Protocol (STP) can run in the RSPAN VLAN, but it does not run on RSPAN destination ports.

When an existing VLAN is configured as an RSPAN VLAN, the VLAN is first deleted and then recreated as an RSPAN VLAN. Any access ports are made inactive until the RSPAN feature is disabled.

Examples

This example shows how to configure a VLAN as an RSPAN VLAN:

```
Controller(config)# vlan 901
Controller(config-vlan)# remote-span
```

This example shows how to remove the RSPAN feature from a VLAN:

```
Controller(config)# vlan 901
Controller(config-vlan)# no remote-span
```

You can verify your settings by entering the **show vlan remote-span** user EXEC command.

show vlan

To display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch, use the **show vlan** command in user EXEC mode.

show vlan [**brief**| **group**| **id** *vlan-id*| **group-name** *WORD user_count*| **mtu**| **name** *vlan-name*| **remote-span**| **summary**]

Syntax Description

brief	(Optional) Displays one line for each VLAN with the VLAN name, status, and its ports.
group	(Optional) Displays information about VLAN groups.
id *vlan-id*	(Optional) Displays information about a single VLAN identified by the VLAN ID number. For *vlan-id*, the range is 1 to 4094.
group-name *WORD vlan-id vlan-id*	(Optional) Displays information about a specific VLAN group.
mtu	(Optional) Displays a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.
name *vlan-name*	(Optional) Displays information about a single VLAN identified by the VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
remote-span	(Optional) Displays information about Remote SPAN (RSPAN) VLANs.
summary	(Optional) Displays VLAN summary information.

Note The **ifindex** keyword is not supported, even though it is visible in the command-line help string.

Command Default

None

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In the **show vlan mtu** command output, the MTU_Mismatch column shows whether all the ports in the VLAN have the same MTU. When yes appears in the column, it means that the VLAN has ports with different MTUs, and packets that are switched from a port with a larger MTU to a port with a smaller MTU might be dropped. If the VLAN does not have an SVI, the hyphen (-) symbol appears in the SVI_MTU column. If the MTU-Mismatch column displays yes, the names of the ports with the MinMTU and the MaxMTU appear.

Examples

This is an example of output from the **show vlan** command. See the table that follows for descriptions of the fields in the display.

```
Controller> show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24, Gi1/0/25
                                                Gi1/0/26, Gi1/0/27, Gi1/0/28
                                                Gi1/0/29, Gi1/0/30, Gi1/0/31
                                                Gi1/0/32, Gi1/0/33, Gi1/0/34
                                                Gi1/0/35, Gi1/0/36, Gi1/0/37
                                                Gi1/0/38, Gi1/0/39, Gi1/0/40
                                                Gi1/0/41, Gi1/0/42, Gi1/0/43
                                                Gi1/0/44, Gi1/0/45, Gi1/0/46
                                                Gi1/0/47, Gi1/0/48
2    VLAN0002                         active
40   vlan-40                          active
300  VLAN0300                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
300  enet  100300     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
2000 enet  102000     1500  -      -      -        -    -        0      0
3000 enet  103000     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
2000,3000

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Table 1: show vlan Command Output Fields

Field	Description
VLAN	VLAN number.

Field	Description
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.
Trans1	Translation bridge 1.
Trans2	Translation bridge 2.
Remote SPAN VLANs	Identifies any RSPAN VLANs that have been configured.

This is an example of output from the **show vlan summary** command:

```
Controller> show vlan summary
Number of existing VLANs              : 45
 Number of existing VTP VLANs         : 45
 Number of existing extended VLANS    : 0
```

This is an example of output from the **show vlan id** command:

```
Controller# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    VLAN0200                         active    Gi1/0/7, Gi1/0/8
2    VLAN0200                         active    Gi2/0/1, Gi2/0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
Disabled
```

show vlan filter

To display information about all VLAN filters or about a particular VLAN or VLAN access map, use the **show vlan filter** command in privileged EXEC mode.

show vlan filter {**access-map** *name*| **vlan** *vlan-id*}

Syntax Description

access-map *name*	(Optional) Displays filtering information for the specified VLAN access map.
vlan *vlan-id*	(Optional) Displays filtering information for the specified VLAN. The range is 1 to 4094.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This is an example of output from the **show vlan filter** command:

```
Controller# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

show vlan group

To display the VLANs that are mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

show vlan group [**group-name** *vlan-group-name* **[user_count]**]

Syntax Description

group-name *vlan-group-name*	(Optional) Displays the VLANs mapped to the specified VLAN group.
user_count	(Optional) Displays the number of users in each VLAN mapped to a specified VLAN group.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you enter the **group-name** keyword, only the members of the specified VLAN group are displayed.

Examples

This example shows how to display the members of a specified VLAN group:

show vtp

To display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters, use the **show vtp** command in EXEC mode.

show vtp {**counters**| **devices** [**conflicts**]| **interface** [*interface-id*]| **password**| **status**}

Syntax Description

counters	Displays the VTP statistics for the controller.
devices	Displays information about all VTP version 3 devices in the domain. This keyword applies only if the controller is not running VTP version 3.
conflicts	(Optional) Displays information about VTP version 3 devices that have conflicting primary servers. This command is ignored when the controller is in VTP transparent or VTP off mode.
interface	Displays VTP status and configuration for all interfaces or the specified interface.
interface-id	(Optional) Interface for which to display VTP status and configuration. This can be a physical interface or a port channel.
password	Displays the configured VTP password (available in privileged EXEC mode only).
status	Displays general information about the VTP management domain status.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you enter the **show vtp password** command when the controller is running VTP version 3, the display follows these rules:

- If the **password** *password* global configuration command did not specify the **hidden** keyword and encryption is not enabled on the controller, the password appears in clear text.

- If the **password** *password* command did not specify the **hidden** keyword and encryption is enabled on the controller, the encrypted password appears.
- If the **password** *password* command is included the **hidden** keyword, the hexadecimal secret key is displayed.

Examples

This is an example of output from the **show vtp devices** command. A Yes in the Conflict column indicates that the responding server is in conflict with the local server for the feature; that is, when two controllers in the same domain do not have the same primary server for a database.

```
Controller# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf controller ID      Primary Server Revision   System Name
             lict
------------ ---- --------------- --------------- ---------- ----------------------
VLAN         Yes  00b0.8e50.d000 000c.0412.6300 12354      main.cisco.com
MST          No   00b0.8e50.d000 0004.AB45.6000 24         main.cisco.com
VLAN         Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com
```

This is an example of output from the **show vtp counters** command. The table that follows describes each field in the display.

```
Controller> show vtp counters
VTP statistics:
Summary advertisements received    : 0
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 0
Subset advertisements transmitted  : 0
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Gi1/0/47              0                0                0
Gi1/0/48              0                0                0
Gi2/0/1               0                0                0
Gi3/0/2               0                0                0
```

Table 2: show vtp counters Field Descriptions

Field	Description
Summary advertisements received	Number of summary advertisements received by this controller on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this controller on its trunk ports. Subset advertisements contain all the information for one or more VLANs.

Field	Description
Request advertisements received	Number of advertisement requests received by this controller on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Summary advertisements transmitted	Number of summary advertisements sent by this controller on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this controller on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements transmitted	Number of advertisement requests sent by this controller on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Number of configuration revision errors	Number of revision errors. Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the controller increments. Revision errors increment whenever the controller receives an advertisement whose revision number matches the revision number of the controller, but the MD5 digest values do not match. This error means that the VTP password in the two controllers is different or that the controllers have different configurations. These errors indicate that the controller is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.

Field	Description
Number of configuration digest errors	Number of MD5 digest errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the controller do not match. This error usually means that the VTP password in the two controllers is different. To solve this problem, make sure the VTP password on all controllers is the same. These errors indicate that the controller is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of V1 summary errors	Number of Version 1 errors. Version 1 summary errors increment whenever a controller in VTP V2 mode receives a VTP Version 1 frame. These errors indicate that at least one neighboring controller is either running VTP Version 1 or VTP Version 2 with V2-mode disabled. To solve this problem, change the configuration of the controllers in VTP V2-mode to disabled.
Join Transmitted	Number of VTP pruning messages sent on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

This is an example of output from the **show vtp status** command. The table that follows describes each field in the display.

```
Controller> show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 2037.06ce.3580
Configuration last modified by 192.168.1.1 at 10-10-12 04:34:02
Local updater ID is 192.168.1.1 on interface LIIN0 (first layer3 interface found
)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 2
MD5 digest                        : 0xA0 0xA1 0xFE 0x4E 0x7E 0x5D 0x97 0x41
                                    0x89 0xB9 0x9B 0x70 0x03 0x61 0xE9 0x27
```

Table 3: show vtp status Field Descriptions

Field	Description
VTP Version capable	Displays the VTP versions that are capable of operating on the controller.
VTP Version running	Displays the VTP version operating on the controller. By default, the controller implements Version 1 but can be set to Version 2.
VTP Domain Name	Name that identifies the administrative domain for the controller.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
VTP Traps Generation	Displays whether VTP traps are sent to a network management station.
Device ID	Displays the MAC address of the local device.
Configuration last modified	Displays the date and time of the last configuration modification. Displays the IP address of the controller that caused the configuration change to the database.

Field	Description
VTP Operating Mode	Displays the VTP operating mode, which can be server, client, or transparent. **Server—**A controller in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The controller guarantees that it can recover all the VLAN information in the current VTP database from NVRAM after reboot. By default, every controller is a VTP server. **Note** The controller automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM and cannot return to server mode until the NVRAM is functioning. **Client—**A controller in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database. **Transparent—**A controller in VTP transparent mode is disabled for VTP, does not send or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The controller receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.
Configuration Revision	Current configuration revision number on this controller.
MD5 Digest	A 16-byte checksum of the VTP configuration.

This is an example of output from the **show vtp status** command for a controller running VTP version 3:

spanning-tree vlan

To configure spanning tree on a per-VLAN basis, use the **spanning-tree vlan** command in global configuration mode on the switch stack or on a standalone switch. To return to the default setting, use the **no** form of this command.

spanning-tree vlan *vlan-id* [**forward-time** *seconds*| **hello-time** *seconds*| **max-age** *seconds*| **priority** *priority*| **root** {**primary**| **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]]

no spanning-tree vlan *vlan-id* [**forward-time**| **hello-time**| **max-age**| **priority**| **root**]

Syntax Description

vlan-id	VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
forward-time *seconds*	(Optional) Sets the forward-delay time for the specified spanning-tree instance. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds.
hello-time *seconds*	(Optional) Sets the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds.
max-age *seconds*	(Optional) Sets the interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds.
priority *priority*	(Optional) Sets the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. The range is 0 to 61440 in increments of 4096. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
root primary	(Optional) Forces this switch to be the root switch.
root secondary	(Optional) Sets this switch to be the root switch should the primary root switch fail.
diameter *net-diameter*	(Optional) Sets the maximum number of switches between any two end stations. The range is 2 to 7.

Command Default

Spanning tree is enabled on all VLANs.

The forward-delay time is 15 seconds.

The hello time is 2 seconds.

The max-age is 20 seconds.

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. Interfaces that are administratively down remain down. Received BPDUs are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.

You can disable the STP on a VLAN that is not currently active and verify the change by using the **show running-config** or the **show spanning-tree vlan** *vlan-id* privileged EXEC command. The setting takes effect when the VLAN is activated.

When disabling or reenabling the STP, you can specify a range of VLANs that you want to disable or enable.

When a VLAN is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign interfaces to it.

When setting the **max-age** *seconds*, if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The max-age setting must be greater than the hello-time setting.

The **spanning-tree vlan** *vlan-id* **root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan** *vlan-id* **root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan** *vlan-id* **root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

Examples

This example shows how to disable the STP on VLAN 5:

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

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

This example shows how to set the spanning-tree forwarding time to 18 seconds for VLANs 20 and 25:

```
Controller(config)# spanning-tree vlan 20,25 forward-time 18
```

This example shows how to set the spanning-tree hello-delay time to 3 seconds for VLANs 20 to 24:

```
Controller(config)# spanning-tree vlan 20-24 hello-time 3
```

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

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

This example shows how to reset the max-age parameter to the default value for spanning-tree instance 100 and 105 to 108:

```
Controller(config)# no spanning-tree vlan 100, 105-108 max-age
```

This example shows how to set the spanning-tree priority to 8192 for VLAN 20:

```
Controller(config)# spanning-tree vlan 20 priority 8192
```

This example shows how to configure the switch as the root for VLAN 10 with a network diameter of 4:

```
Controller(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Controller(config)# spanning-tree vlan 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree vlan** *vlan-id* privileged EXEC command.

wlan

To create a wireless LAN, use the **wlan** command. To disable a wireless LAN, use the **no** form of this command.

wlan [*wlan-name*| *wlan-name wlan-id*| *wlan-name wlan-id wlan-ssid*]

no wlan [*wlan-name*| *wlan-name wlan-id*| *wlan-name wlan-id wlan-ssid*]

Syntax Description

wlan-name	WLAN profile name. The name is from 1 to 32 alphanumeric characters.
wlan-id	Wireless LAN identifier. The range is from 1 to 512.
wlan-ssid	SSID. The range is from 1 to 32 alphanumeric characters.

Command Default

WLAN is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you do not specify an SSID, the profile name parameter is used for both the profile name and the SSID. If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager (Access Point Manager) interfaces are assigned to different VLANs, you do not need to disable the WLAN.

An error message appears if you try to delete a WLAN that is assigned to an access point group. If you proceed, the WLAN is removed from the access point group and from the access point's radio.

Examples

This example shows how to create a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config)# wlan test-wlan-cr 67 test-wlan-cr-ssid
```

This example shows how to delete a WLAN:

```
Controller# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Controller(config)# wlan wlan1
Controller(config)# no wlan test-wlan-cr 67 test-wlan-cr-ssid
```