

set uddl

To enable or disable the UDLD information display on specified ports or globally on all ports, use the **set uddl** command.

set uddl enable | disable [*mod/port*]

Syntax Description

enable	Enables the UDLD information display.
disable	Disables the UDLD information display.
<i>mod/port</i>	(Optional) Number of the module and port on the module.

Defaults

The defaults are as follows:

- UDLD global enable state—Globally disabled.
- UDLD per-port enable state for fiber-optic media—Enabled on all Ethernet fiber-optic ports.
- UDLD per-port enable state for twisted-pair (copper) media—Disabled on all Ethernet 10/100 and 1000BASE-TX ports.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Whenever a unidirectional connection is detected, UDLD displays a syslog message to notify you and the network management application (through SNMP) that the port on which the misconfiguration has been detected has been disabled.

If you enter the global **set uddl enable** or **disable** command, UDLD is globally configured. If UDLD is globally disabled, UDLD is automatically disabled on all interfaces, but the per-port enable (or disable) configuration is not changed. If UDLD is globally enabled, whether or not UDLD is running on an interface depends on its per-port configuration.

UDLD is supported on both Ethernet fiber and copper interfaces. UDLD can only be enabled on Ethernet fiber or copper interfaces.

Examples

This example shows how to enable the UDLD message display for port 1 on module 2:

```
Console> (enable) set uddl enable 2/1
UDLD enabled on port 2/1.
Warning:UniDirectional Link Detection
should be enabled only on ports not connected to hubs,
media converters or similar devices.
Console> (enable)
```

This example shows how to disable the UDLD message display for port 1 on module 2:

```
Console> (enable) set udd disable 2/1  
UDLD disabled on port 2/1.  
Warning:UniDirectional Link Detection  
should be enabled only on ports not connected to hubs,  
media converters or similar devices.  
Console> (enable)
```

This example shows how to enable the UDLD message display for all ports on all modules:

```
Console> (enable) set udd enable  
UDLD enabled globally.
```

```
Console> (enable)
```

This example shows how to disable the UDLD message display for all ports on all modules:

```
Console> (enable) set udd disable  
UDLD disabled globally  
Console> (enable)
```

Related Commands [show udd](#)

set udd aggressive-mode

To enable or disable the UDDL aggressive mode on specified ports, use the **set udd aggressive-mode** command.

set udd aggressive-mode enable | disable *mod/port*

Syntax Description	enable	Enables UDDL aggressive mode.
	disable	Disables UDDL aggressive mode.
	<i>mod/port</i>	Number of the module and port on the module.

Defaults The default is aggressive mode is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines You can use the aggressive mode in cases in which a port that sits on a bidirectional link stops receiving packets from its neighbor. When this happens, if aggressive mode is enabled on the port, UDDL will try to reestablish the connection with the neighbor. If connection is not reestablished after eight failed retries, the port is error disabled.

We recommend that you use this command on point-to-point links between Cisco switches only.

Examples This example shows how to enable aggressive mode:

```
Console> (enable) set udd aggressive-mode enable 2/1
Aggressive UDDL enabled on port 5/13.
Warning:Aggressive Mode for UniDirectional Link Detection
should be enabled only on ports not connected to hubs,
media converters or similar devices.
Console> (enable)
```

Related Commands [set udd](#)
[show udd](#)

set udd interval

To set the UDDL message interval timer, use the **set udd interval** command.

set udd interval *interval*

Syntax Description	<i>interval</i> Message interval in seconds; valid values are from 7 to 90 seconds.
---------------------------	---

Defaults	The default is 15 seconds.
-----------------	----------------------------

Command Types	Switch command.
----------------------	-----------------

Command Modes	Privileged.
----------------------	-------------

Examples	This example shows how to set the message interval timer:
-----------------	---

```
Console> (enable) set udd interval 90
UDLD message interval set to 90 seconds
Console> (enable)
```

Related Commands	set udd show udd
-------------------------	---

set vlan

To group ports into a VLAN, set the private VLAN type, map or unmap VLANs to or from an instance, specify an 802.1X port to a VLAN, or secure a range of VLANs on a Firewall Services Module, use the **set vlan** command.

```
set vlan {vlans} {mod/ports}
```

```
set vlan {vlans} [name name] [type type] [state state] [said said] [mtu mtu]
[bridge bridge_num] [mode bridge_mode] [stp stp_type] [translation vlan_num]
[aremaxhop hopcount] [pvlan-type pvlan_type] [mistp-instance mistp_instance]
[ring hex_ring_number] [decring decimal_ring_number] [parent vlan_num]
[backuperf {off | on}] [stemaxhop hopcount] [rspan]
```

```
set vlan {vlans} firewall-vlan {mod}
```

```
set vlan {vlan} firewall-vlan {mod} msfc-fwsm-interface
```

Syntax Description

<i>vlans</i>	Number identifying the VLAN; valid values are from 1 to 4094.
<i>mod/ports</i>	Number of the module and ports on the module belonging to the VLAN.
name <i>name</i>	(Optional) Defines a text string used as the name of the VLAN; valid values are from 1 to 32 characters.
type <i>type</i>	(Optional) Identifies the VLAN type.
state <i>state</i>	(Optional) Specifies whether the state of the VLAN is active or suspended.
said <i>said</i>	(Optional) Specifies the security association identifier; valid values are from 1 to 4294967294.
mtu <i>mtu</i>	(Optional) Specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from 576 to 18190.
bridge <i>bridge_num</i>	(Optional) Specifies the identification number of the bridge; valid values are hexadecimal numbers from 0x1 to 0xF.
mode <i>bridge_mode</i>	(Optional) Specifies the bridge mode; valid values are srt and srb .
stp <i>stp_type</i>	(Optional) Specifies the STP type; valid values are ieee , ibm , and auto .
translation <i>vlan_num</i>	(Optional) Specifies a translational VLAN used to translate FDDI or Token Ring to Ethernet; valid values are from 1 to 4094.
aremaxhop <i>hopcount</i>	(Optional) Specifies the maximum number of hops for All-Routes Explorer frames; valid values are from 1 to 13.
pvlan-type <i>pvlan-type</i>	(Optional) Keyword and options to specify the private VLAN type. See the “Usage Guidelines” section for valid values.
mistp-instance <i>mistp_instance</i>	(Optional) Specifies the MISTP instance; valid values are none and from 1 to 16.
ring <i>hex_ring_number</i>	(Optional) Keyword to specify the VLAN as the primary VLAN in a private VLAN.
decring <i>decimal_ring_number</i>	(Optional) Specifies the decimal ring number; valid values are from 1 to 4095.
parent <i>vlan_num</i>	(Optional) Specifies the VLAN number of the parent VLAN; valid values are from 1 to 4094.
backuperf off on	(Optional) Specifies whether the TrCRF is a backup path for traffic.

stemaxhop <i>hopcount</i>	(Optional) Specifies the maximum number of hops for Spanning Tree Explorer frames; valid values are from 1 to 14.
rspan	(Optional) Creates a VLAN for remote SPAN.
firewall-vlan	Specifies VLANs that are secured by a Firewall Services Module; see the “Usage Guidelines” section for more information about specifying a VLAN range for a Firewall Services Module.
<i>mod</i>	Number of the Firewall Services Module.
msfc-fwsm-interface	Specifies the VLAN that is to be the interface between the MSFC and the Firewall Services Module.

Defaults

The default values are as follows:

- Switched Ethernet ports and Ethernet repeater ports are in VLAN 1.
- *said* is 100001 for VLAN 1, 100002 for VLAN 2, 100003 for VLAN 3, and so forth.
- *type* is Ethernet.
- *mtu* is 1500 bytes.
- *state* is active.
- *hopcount* is 7.
- *pvlan type* is none.
- *mistp_instance* is no new instances have any VLANs mapped. For an existing VLAN, the existing instance configuration is used.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

This command is not supported by the NAM.

If you are configuring normal-range VLANs, you cannot use the **set vlan** command until the Catalyst 6500 series switch is either in VTP transparent mode (**set vtp mode transparent**) or until a VTP domain name has been set (**set vtp domain name**). To create a private VLAN, UTP mode must be transparent.

If you set the VTP version to 3, VLAN 1 (the Cisco default VLAN) and VLANs 1002-1005 are configurable. If your switch has VTP version 1 or VTP version 2 neighbors, only default values are advertised for these VLANs. We recommend that you do not modify these VLANs if you want interoperability with older versions of VTP.

If you specify a range of VLANs, you cannot use the VLAN name.

If you enter the **mistp-instance none** command, the specified VLANs are unmapped from any instance they are mapped to.

The **set vlan *vlan_num* mistp-instance *mistp_instance*** command is available in PVST+ mode.

You cannot set multiple VLANs for ISL ports using this command. The VLAN name can be from 1 to 32 characters in length. If you are adding a new VLAN or modifying an existing VLAN, the VLAN number must be within the range of 1 to 4094.

If you use the **rspan** keyword for remote SPAN VLANs, you should not configure an access port (except the remote SPAN destination ports) on these VLANs. Learning is disabled for remote SPAN VLANs.

If you use the **rspan** keyword for remote SPAN VLANs, only the **name *name*** and the **state {active | suspend}** variables are supported.

The **stemaxhop *hopcount*** parameter is valid only when defining or configuring TrCRFs.

The **bridge *bridge_num***, **mode *bridge_mode***, **stp *stp_type***, and **translation *vlan_num*** keywords and values are supported only when the Catalyst 6500 series switch is used as a VTP server for Catalyst 5000 family switches in the Token Ring and FDDI networks.

You must configure a private VLAN on the supervisor engine.

Valid values for *pvlan-type* are as follows:

- **primary** specifies the VLAN as the primary VLAN in a private VLAN.
- **isolated** specifies the VLAN as the isolated VLAN in a private VLAN.
- **community** specifies the VLAN as the community VLAN in a private VLAN.
- **twoway-community** specifies the VLAN as a bidirectional community VLAN that carries the traffic among community ports and to and from community ports to and from the MSFC.
- **none** specifies that the VLAN is a normal Ethernet VLAN, not a private VLAN.

Only regular VLANs with no access ports assigned to them can be used in private VLANs. Do not use the **set vlan** command to add ports to a private VLAN; use the **set pvlan** command to add ports to a private VLAN.

VLANs 1001, 1002, 1003, 1004, and 1005 cannot be used in private VLANs.

VLANs in a suspended state do not pass packets.

To secure a range of VLANs on a Firewall Services Module, these conditions must be satisfied:

1. Port membership must be defined for the VLANs, and the VLANs must be in active state.
2. The VLANs do not have a Layer 3 interface in active state on the MSFC.
3. The VLANs are not reserved VLANs.

VLANs that do not satisfy condition number 2 in the list above are discarded from the range of VLANs that you attempt to secure on the Firewall Services Module. VLANs that meet condition number 2 and condition number 3 but do not meet condition number 1 are stored in the supervisor engine database; these VLANs are sent to the Firewall Services Module as soon as they meet condition number 1.

Starting in software release 8.4(1), the WS-X6380-NAM management port (port 2) does not have to be in the same VLAN as the sc0 interface on the switch. The **set vlan *vlan mod/port*** command can be used to put the NAM management port in any VLAN other than VLAN 1. If the **set vlan** command is not used to specify a VLAN for the NAM management port, then the NAM management port by default will be set to the same VLAN as the sc0 interface on the switch.

Examples

This example shows how to set VLAN 850 to include ports 3 through 7 on module 3:

```
Console> (enable) set vlan 850 3/3-7
VLAN 850 modified.
VLAN  Mod/Ports
-----
850   3/4-7
Console> (enable)
```

This example shows how to set VLAN 7 as a primary VLAN:

```
Console> (enable) set vlan 7 pvlan-type primary
Console> (enable)
```

This example shows how to set VLAN 901 as an isolated VLAN:

```
Console> (enable) set vlan 901 pvlan-type isolated
Console> (enable)
```

This example shows how to set VLAN 903 as a community VLAN:

```
Console> (enable) set vlan 903 pvlan-type community
Console> (enable)
```

This example shows how to unmap all instances currently mapped to VLAN 5:

```
Console> (enable) set vlan 5 mistp-instance none
Vlan 5 configuration successful
Console> (enable)
```

This example shows how to secure a range of VLANs on a Firewall Services Module:

```
Console> (enable) set vlan 2-55 firewall-module 7
Console> (enable)
```

This example shows the message that appears when VLAN port-provisioning verification is enabled:

```
Console> (enable) set vlan 10 2/1
Port Provisioning Verification is enabled on the switch.
To move port(s) into the VLAN, use 'set vlan <vlan> <port> <vlan_name>'
command.
Console> (enable)
```

Related Commands

[clear config pvlan](#)
[clear pvlan mapping](#)
[clear vlan](#)
[set pvlan](#)
[set spantree macreduction](#)
[set vlan mapping](#)
[set vlan verify-port-provisioning](#)
[show pvlan](#)
[show pvlan mapping](#)
[show vlan](#)

set vlan mapping

To map 802.1Q VLANs to ISL VLANs, use the **set vlan mapping** command.

```
set vlan mapping dot1q 1q_vlan_num isl isl_vlan_num
```

Syntax Description	dot1q <i>1q_vlan_num</i> Specifies the 802.1Q VLAN; valid values are from 1001 to 4094.
	isl <i>isl_vlan_num</i> Specifies the ISL VLAN; valid values are from 1 to 1000.

Defaults This command has no default settings.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines VLAN and MISTP instance mapping can be set only on the switch that is in either VTP server mode or in transparent mode.

Use this feature to map 802.1Q VLANs above 1000 to ISL VLANs.

The total of all mappings must be less than or equal to eight. Only one 802.1Q VLAN can be mapped 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.

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

If the VLAN number does not exist, then either of the following occurs:

- If the switch is in server or transparent mode, the VLAN is created with all default values.
- If the switch is in client mode, then the command proceeds without creating the VLAN. A warning will be given indicating that the VLAN does not exist.

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

The dot1q VLANs are rejected if any extended-range VLANs are present.

You cannot enable global VLAN mapping and per-port/per-ASIC VLAN mapping simultaneously.

Examples This example shows how to map VLAN 850 to ISL VLAN 1022:

```
Console> (enable) set vlan mapping dot1q 850 isl 1022
Vlan 850 configuration successful
Vlan mapping successful
Console> (enable)
```

This example shows the display if you enter a VLAN that does not exist:

```
Console> (enable) set vlan mapping dot1q 2 isl 1016  
Vlan Mapping Set  
Warning: Vlan 2 Nonexistent  
Console> (enable)
```

This example shows the display if you enter an existing mapping:

```
Console> (enable) set vlan mapping dot1q 3 isl 1022  
1022 exists in the mapping table. Please clear the mapping first.  
Console> (enable)
```

This example shows the display if the mapping table is full:

```
Console> (enable) set vlan mapping dot1q 99 isl 1017  
Vlan Mapping Table Full.  
Console> (enable)
```

Related Commands

[clear vlan mapping](#)
[show vlan](#)

set vlan verify-port-provisioning

To enable or disable VLAN port-provisioning verification on all ports, use the **set vlan verify-port-provisioning** command.

set vlan verify-port-provisioning {enable | disable}

Syntax Description	enable	Disables VLAN port-provisioning verification.
	disable	Enables VLAN port-provisioning verification.

Defaults VLAN port-provisioning verification is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When VLAN port-provisioning verification is enabled, you must specify the VLAN name in addition to the VLAN number when assigning switch ports to VLANs. Because you are required to specify both the VLAN name and the VLAN number, this verification feature helps ensure that ports are not inadvertently placed in the wrong VLAN.

When the feature is enabled, you can still create new VLANs using the **set vlan *vlan mod/port*** command, but you cannot add additional 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 SNMP, dynamic VLANs, and 802.1X.

Examples This example shows how to enable VLAN port-provisioning verification on all ports:

```
Console> (enable) set vlan verify-port-provisioning enable
Vlan verify-port-provisioning feature enabled
Console> (enable)
```

This example shows how to disable VLAN port-provisioning verification on all ports:

```
Console> (enable) set vlan verify-port-provisioning disable
vlan verify-port-provisioning feature disabled
Console> (enable)
```

Related Commands [show vlan verify-port-provisioning](#)

set vmpls auto-push-config

To enable or disable the VLAN Membership Policy Server (VMPS) autopush configuration, use the **set vmpls auto-push-config** command.

```
set vmpls auto-push-config {enable | disable}
```

Syntax Description

enable	Enables the autopush configuration of VMPS.
disable	Disables the autopush configuration of VMPS.

Defaults

VMPS autopush is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Examples

This example shows how to enable the VMPS autopush configuration:

```
Console> (enable) set vmpls auto-push-config enable  
Vlan Membership Policy Server auto-push-config enabled  
Console> (enable)
```

set vmpls config-file

To set the backup configuration file for the VLAN Membership Policy Server (VMPS), use the **set vmpls config-file** command.

```
set vmpls config-file device:[filename]
```

```
set vmpls config-file auto-save {enable | disable}
```

Syntax Description

device:	Device name where the backup configuration is stored.
filename	(Optional) Filename of the backup configuration. See the “Usage Guidelines” section for more information.
auto-save	Specifies the feature that automatically saves the VMPS configuration.
enable	Enables the auto-save feature.
disable	Disables the auto-save feature.

Defaults

If you do not specify a *filename* argument, the filename is automatically called `vmpls-backup-config-database.1`.

The auto-save feature is disabled.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can use the **set vmpls config-file auto-save** command to automatically save the downloaded VMPS configuration in the local storage of the switch. If you enable the auto-save feature, the switch backs up the downloaded configuration file into the specified device with the specified filename.

If you do not specify a specific backup device or a specific backup configuration filename, the switch automatically saves the file in the following device with the following filename:

```
bootflash:vmpls-backup-config-database.1.
```

Examples

This example shows how to specify a backup device and a backup filename for the VMPS configuration:

```
Console> (enable) set vmpls config-file disk0:vmpls_config_engineering
Vmpls back-up file name is set to disk0:vmpls_config_engineering
Console> (enable)
```

This example shows how to enable the feature that automatically saves the VMPS configuration:

```
Console> (enable) set vmpls config-file auto-save enable
Auto save to store vmpls configuration file is enabled.
Console> (enable)
```

This example shows to disable the feature that automatically saves the VMPS configuration:

```
Console> (enable) set vmps config-file auto-save disable  
Auto save to store vmps configuration file is disabled.  
Console> (enable)
```

Related Commands [show vmps](#)

set vmps download

To specify the VLAN Membership Policy Server (VMPS) download interval, use the **set vmps download** command.

set vmps download *interval*

Syntax Description	<i>interval</i>	Download interval in minutes; values are from 1 to 35000.
---------------------------	-----------------	---

Defaults	The VMPS download interval is 0 minutes.
-----------------	--

Command Types	Switch command.
----------------------	-----------------

Command Modes	Privileged.
----------------------	-------------

Examples	This example shows how to specify the VMPS download interval to 2000 minutes:
-----------------	---

```
Console> (enable) set vmps download 2000  
vmps download interval set to 2000 minutes.  
Console> (enable)
```

set vmps downloadmethod

To specify whether to use TFTP or rcp to download the VMPS database, use the **set vmps downloadmethod** command.

```
set vmps downloadmethod {rcp | tftp} [username]
```

Syntax Description	rcp	Specifies rcp as the method for downloading the VLAN Membership Policy Server (VMPS) database.
	tftp	Specifies TFTP as the method for downloading the VMPS database.
	<i>username</i>	(Optional) Username for downloading with rcp.

Defaults If no method is specified, TFTP will be used.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The *username* option is not allowed if you specify **tftp** as the download method.

Examples This example shows how to specify the method for downloading the VMPS database:

```
Console> (enable) set vmps downloadmethod rcp jdoe
vmps downloadmethod : RCP
rcp vmps username   : jdoe
Console> (enable)
```

Related Commands

- [download](#)
- [set rcp username](#)
- [show vmps](#)

set vmps downloadserver

To specify the IP address of the TFTP or rcp server from which the VMPS database is downloaded, use the **set vmps downloadserver** command.

```
set vmps downloadserver ip_addr [filename]
```

Syntax Description	<i>ip_addr</i>	IP address of the TFTP or rcp server from which the VMPS database is downloaded.
	<i>filename</i>	(Optional) VMPS configuration filename on the TFTP or rcp server.

Defaults If *filename* is not specified, the **set vmps downloadserver** command uses the default filename vmps-config-database.1.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to specify the server from which the VMPS database is downloaded and how to specify the configuration filename:

```
Console> (enable) set vmps downloadserver 192.168.69.100 vmps_config.1
IP address of the server set to 192.168.69.100
VMPS configuration filename set to vmps_config.1
Console> (enable)
```

Related Commands

- [download](#)
- [set vmps state](#)
- [show vmps](#)

set vmpls server

To configure the VMPS, use the **set vmpls server** command.

```
set vmpls server ip_addr [primary]
```

```
set vmpls server retry count
```

```
set vmpls server reconfirminterval interval
```

Syntax Description		
	<i>ip_addr</i>	IP address of the VMPS.
	primary	(Optional) Specifies the device as the primary VMPS.
	retry count	Specifies the retry interval; valid values are from 1 to 10 minutes.
	reconfirminterval interval	Specifies the reconfirmation interval; valid values are from 0 to 120 minutes.

Defaults If no IP address is specified, the VMPS uses the local VMPS configuration.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines You can specify the IP addresses of up to three VMPSs. You can define any VMPS as the primary VMPS. If the primary VMPS is down, all subsequent queries go to a secondary VMPS. VMPS checks on the primary server's availability once every five minutes. When the primary VMPS comes back online, subsequent VMPS queries are directed back to the primary VMPS.

To use a co-resident VMPS (when VMPS is enabled in a device), configure one of the three VMPS addresses as the IP address of interface sc0.

When you specify the **reconfirminterval interval**, enter 0 to disable reconfirmation.

Examples This example shows how to define a primary VMPS:

```
Console> (enable) set vmpls server 192.168.10.140 primary
192.168.10.140 added to VMPS table as primary domain server.
Console> (enable)
```

This example shows how to define a secondary VMPS:

```
Console> (enable) set vmpls server 192.168.69.171
192.168.69.171 added to VMPS table as backup domain server.
Console> (enable)
```

■ set vmps server

Related Commands

[clear vmps server](#)
[show vmps](#)

set vmpls state

To enable or disable VMPS, use the **set vmpls state** command.

```
set vmpls state {enable | disable}
```

Syntax Description	enable	Enables VMPS.
	disable	Disables VMPS.

Defaults By default, VMPS is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines Before using the **set vmpls state** command, you must use the **set vmpls tftpserver** command to specify the IP address of the server from which the VMPS database is downloaded.

Examples This example shows how to enable VMPS:

```
Console> (enable) set vmpls state enable
Vlan membership Policy Server enabled.
Console> (enable)
```

This example shows how to disable VMPS:

```
Console> (enable) set vmpls state disable
All the VMPS configuration information will be lost and the resources released on disable.
Do you want to continue (y/n[n]):y
VLAN Membership Policy Server disabled.
Console> (enable)
```

Related Commands [download](#)
[show vmpls](#)

set vtp

To set the options for VTP, use the **set vtp** command.

set vtp domain *domain_name*

set vtp mode { **client** | **server** | **transparent** | **off** } [**vlan** | **mst** | **unknown**]

set vtp passwd *passwd* [**hidden**]

set vtp pruning { **enable** | **disable** }

set vtp version { **1** | **2** | **3** }

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

Syntax Description

domain <i>domain_name</i>	Defines the name that identifies the VLAN management domain. The <i>domain_name</i> can be from 1 to 32 characters in length.
mode { client server transparent off }	Specifies the VTP mode.
vlan	(Optional) Specifies the VLAN database.
mst	(Optional) Specifies the MST database.
unknown	(Optional) Specifies an unknown feature. See the “Usage Guidelines” section for more information.
passwd <i>passwd</i>	Defines the VTP password; the VTP password can be from 1 to 64 characters in length.
hidden	(Optional) Hides the password in the configuration. See the “Usage Guidelines” section for more information.
pruning { enable disable }	Enables or disables VTP pruning for the entire management domain in VTP versions 1 and 2. Enables or disables VTP pruning only on the local switch in VTP version 3.
version { 1 2 3 }	Specifies the VTP version.
primary	Sets the VTP version 3 primary server.
force	(Optional) Forces the switch to be the primary server.

Defaults

The defaults are as follows:

- no domain name
- server mode
- no password
- pruning disabled
- version 1

Command Types

Switch command.

Command Modes Privileged.

Usage Guidelines The following guidelines apply to VTP versions 1, 2, and 3:

- VTP supports four different modes: server, client, transparent, and off. If you make a change to the VTP or VLAN configuration on a switch in server mode, that change is propagated to all of the switches in the same VTP domain.
- If the VTP password has already been defined, entering **passwd 0** (zero) clears the VTP password. If you enter the **hidden** keyword after you specify the VTP password, the password does not appear in the configuration; an encrypted hexadecimal value appears in place of the password.
- If the receiving switch is in server mode and its revision number is higher than the sending switch, the configuration is not changed. If the revision number is lower, the configuration is duplicated.
- 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.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. Make sure to make all VTP or VLAN configuration changes on a switch in server mode.
- 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.
- When you configure the VTP off mode, the switch functions the same as in VTP transparent mode except that VTP advertisements are not forwarded.
- You cannot enable VTP pruning and MISTP at the same time.
- Use the **clear config all** command to remove the domain from the switch.



Caution

Be careful when you use the **clear config all** command. This command clears the entire switch configuration, not just the VTP domain.

- The **set vtp** command is not supported by the NAM.

The following guidelines apply only to VTP versions 1 and 2:

- 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 domain.
- If all switches in a VTP domain are VTP version 2-capable, you only need to enable VTP version 2 on one switch by using the **set vtp version 2** command. The version number is then propagated to other version 2-capable switches in the VTP domain.
- The **pruning** keyword is used to enable or disable VTP pruning for the entire VTP domain. VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN out a particular switch port. Use the **set vtp pruneeligible** and **clear vtp pruneeligible** commands to specify which VLANs should or should not be pruned when pruning is enabled for the domain.

The following guidelines apply only to VTP version 3:

- VTP version 3 works concurrently with VTP versions 1 and 2. VTP version 3 is implemented independently because it only distributes a list of databases over an administrative domain. VTP version 3 does not directly handle VLANs.

- The **unknown** keyword allows you to configure the behavior of the switch databases that it cannot interpret. (These databases will be features handled by future extensions of VTP version 3). If you enter **set vtp mode transparent unknown**, packets for unknown features are flooded through the switch. If you enter **set vtp mode off unknown**, packets are dropped.
- VTP version 3 is a local configuration for the switch. Pruning does not propagate throughout the domain but only the local switch.
- MST mapping is propagated only if the switch is running VTP version 3 in software release 8.3(1). If the switch is running VTP version 3 without the MST feature and receives an MST database, it takes action based on the unknown database mode. If the unknown database mode is transparent, the switch relays the VTP version 3 packet that carries the MST database. If the unknown database mode is off, the switch drops the packet.



Note A switch running VTP version 1 or version 2 ignores the MST database that is sent by the VTP version 3 switch in the network.



Note A switch can commit any new MST mapping only if it is a primary server for the MST feature.

Examples

This example shows how to set the VTP domain name:

```
Console> (enable) set vtp domain Lab_Network
VTP domain Lab_Network modified
Console> (enable)
```

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

```
Console> (enable) set vtp mode server
Changing VTP mode for all features
VTP3 domain Lab_Network modified
Console> (enable)
```

This example shows what happens if you try to change VTP to server or client mode and dynamic VLAN creation is enabled:

```
Console> (enable) set vtp mode server
Failed to Set VTP to Server. Please disable Dynamic VLAN Creation First.
Console> (enable)
```

This example shows how to set VTP to off mode:

```
Console> (enable) set vtp mode off
VTP domain modified
Console> (enable)
```

This example shows how to set the VTP password:

```
Console> (enable) set vtp passwd Sa7r12ah
Generating the secret associated to the password.
VTP domain pubs modified
Console> (enable)
```

This example shows how to set the VTP password and hide it in the configuration:

```
Console> (enable) set vtp passwd Sa7r12ah hidden  
Generating the secret associated to the password.  
The VTP password will not be shown in the configuration.  
VTP domain pubs modified  
Console> (enable)
```

This example shows how to set the VTP mode for the MST feature:

```
Console> (enable) set vtp mode server mst  
Changing VTP mode for mst feature  
VTP3 domain map1 modified  
Console> (enable)
```

This example shows how to set the primary server for the MST feature:

```
Console> (enable) set vtp primary mst  
This switch is becoming primary server for feature mst.  
Do you want to continue (y/n) [n]? y  
Console> (enable)
```

Related Commands

[clear vlan](#)
[clear vtp pruneeligible](#)
[set vlan](#)
[set vtp pruneeligible](#)
[show vlan](#)
[show vtp domain](#)

set vtp pruneeligible

To specify which VTP domain VLANs are pruning eligible, use the **set vtp pruneeligible** command.

set vtp pruneeligible *vlan*s

Syntax Description	<i>vlan</i> s	Range of VLAN numbers; valid values are from 2 to 1000.
---------------------------	---------------	---

Defaults	The default is VLANs 2 through 1000 are eligible for pruning.
-----------------	---

Command Types	Switch command.
----------------------	-----------------

Command Modes	Privileged.
----------------------	-------------

Usage Guidelines	VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN out a particular switch port. Use the set vtp command to enable VTP pruning.
-------------------------	--

By default, VLANs 2 through 1000 are pruning eligible. You do not need to use the **set vtp pruneeligible** command unless you have previously used the **clear vtp pruneeligible** command to make some VLANs pruning ineligible. If VLANs have been made pruning ineligible, use the **set vtp pruneeligible** command to make them pruning eligible again.

Examples	This example shows how to configure pruning eligibility for VLANs 120 and 150:
-----------------	--

```
Console> set vtp pruneeligible 120,150
Vlans 120,150 eligible for pruning on this device.
VTP domain nada modified.
Console>
```

In this example, VLANs 200–500 were made pruning ineligible using the **clear vtp pruneeligible** command. This example shows how to make VLANs 220 through 320 pruning eligible again:

```
Console> set vtp pruneeligible 220-320
Vlans 2-199,220-320,501-1000 eligible for pruning on this device.
VTP domain Company modified.
Console>
```

Related Commands	clear vtp pruneeligible set vlan show vtp domain
-------------------------	---

set web-auth

To enable or disable web-based proxy authentication globally, use the **set web-auth** command.

```
set web-auth {disable | enable}
```

Syntax Description	disable	enable
	Disables web-based proxy authentication.	Enables web-based proxy authentication.

Defaults Disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines



Note

If you have disabled web-based proxy authentication globally, web-based proxy authentication on a port may not start but will be stored in the configuration.

Examples

This example shows how to enable web-based proxy authentication globally:

```
Console> (enable) set web-auth enable
web-authentication successfully enabled on globally.
Console> (enable)
```

This example shows how to disable web-based proxy authentication globally:

```
Console> (enable) set web-auth disable
web-authentication successfully disabled on globally.
Console> (enable)
```

Related Commands

```
clear web-auth
set port web-auth
set port web-auth initialize
set web-auth login-attempts
set web-auth login-fail-page
set web-auth login-page
set web-auth quiet-timeout
set web-auth session-timeout
show port web-auth
show web-auth summary
```

set web-auth login-attempts

To specify the maximum number of unsuccessful login attempts allowed before blocking the user, use the **set web-auth login-attempts** command.

set web-auth login-attempts *count*

Syntax Description	<i>count</i>	Maximum number of unsuccessful login attempts allowed; valid values are from 3 to 10 attempts.
---------------------------	--------------	--

Defaults	3 attempts.
-----------------	-------------

Command Types	Switch command.
----------------------	-----------------

Command Modes	Privileged.
----------------------	-------------

Examples	This example shows how to specify the maximum number of login attempts:
-----------------	---

```
Console> (enable) set web-auth login-attempts 2
web-authentication max retry count set to 2
Console> (enable)
```

Related Commands	<ul style="list-style-type: none"> clear web-auth set port web-auth set port web-auth initialize set web-auth set web-auth login-fail-page set web-auth login-page set web-auth quiet-timeout set web-auth session-timeout show port web-auth show web-auth summary
-------------------------	---

set web-auth login-fail-page

To configure the URL for the Login Fail page, use the **set web-auth login-fail-page** command.

```
set web-auth login-fail-page url
```

Syntax Description	<i>url</i> Login Fail page URL.
---------------------------	---------------------------------

Defaults	This command has no default settings.
-----------------	---------------------------------------

Command Types	Switch command.
----------------------	-----------------

Command Modes	Privileged.
----------------------	-------------

Usage Guidelines	The URL that you enter must be fewer than 256 characters and must begin with http://.
-------------------------	---

Examples	This example shows how to configure the URL for the Login Fail page: <pre>Console> (enable) set web-auth login-fail-page http://proxyauth.cisco.com/login.html web-auth login fail page configured. Console> (enable)</pre>
-----------------	---

Related Commands	clear web-auth set port web-auth set port web-auth initialize set web-auth set web-auth login-attempts set web-auth login-page set web-auth quiet-timeout set web-auth session-timeout show port web-auth show web-auth summary
-------------------------	--

set web-auth login-page

To configure the URL for the Login page, use the **set web-auth login-page** command.

```
set web-auth login-page url url
```

Syntax Description

<i>url</i>	Login page URL.
------------	-----------------

Defaults

This command has no default settings.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

The URL that you enter must be fewer than 256 characters and must begin with http://.

Examples

This example shows how to configure the URL for the Login page:

```
Console> (enable) set web-auth login-page http://proxyauth.cisco.com/login.html
web-auth login-page configured.
Console> (enable)
```

Related Commands

- [clear web-auth](#)
- [set port web-auth](#)
- [set port web-auth initialize](#)
- [set web-auth](#)
- [set web-auth login-attempts](#)
- [set web-auth login-fail-page](#)
- [set web-auth quiet-timeout](#)
- [set web-auth session-timeout](#)
- [show port web-auth](#)
- [show web-auth summary](#)

set web-auth quiet-timeout

To set the quiet timeout interval for which the web-based proxy authentication is in the Held state, use the **set web-auth quiet-timeout** command.

set web-auth quiet-timeout *seconds*

Syntax Description	<i>seconds</i>	Quiet timeout interval; valid values are from 1 to 43200 seconds.
---------------------------	----------------	---

Defaults	60 seconds.
-----------------	-------------

Command Types	Switch command.
----------------------	-----------------

Command Modes	Privileged.
----------------------	-------------

Usage Guidelines	The quiet-timeout interval is the time that the web-based proxy authentication is in the Held state after maximum authentication attempts have been exceeded.
-------------------------	---

Examples	This example shows how to set the quiet timeout interval for web-based proxy authentication:
-----------------	--

```
Console> (enable) set web-auth session-timeout 55  
web-authentication session-timeout set to 55 seconds.  
Console> (enable)
```

Related Commands	clear web-auth set port web-auth set port web-auth initialize set web-auth set web-auth login-attempts set web-auth login-fail-page set web-auth login-page set web-auth session-timeout show port web-auth show web-auth summary
-------------------------	--

set web-auth session-timeout

To set the global session timeout for the web-authenticated sessions, use the **set web-auth session-timeout** command.

set web-auth session-timeout *seconds*

Syntax Description	<i>seconds</i>	Global session timeout interval; valid values are from 300 to 86400 seconds.
---------------------------	----------------	--

Defaults	3600 seconds.
-----------------	---------------

Command Types	Switch command.
----------------------	-----------------

Command Modes	Privileged.
----------------------	-------------

Usage Guidelines	The session-timeout interval is the time that this session is valid. The web-authenticated sessions are terminated after this timeout. The RADIUS-supplied session timeout takes precedence over the locally configured value.
-------------------------	--

Examples	This example shows how to set the global session timeout for the web-authenticated sessions:
-----------------	--

```
Console> (enable) set web-auth session-timeout 1800
web-authentication session-timeout set to 1800 seconds.
Console> (enable)
```

Related Commands	<ul style="list-style-type: none"> clear web-auth set port web-auth set port web-auth initialize set web-auth set web-auth login-attempts set web-auth login-fail-page set web-auth login-page set web-auth quiet-timeout show port web-auth show web-auth summary
-------------------------	--