

# 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

<b>enable</b>	Enables the UDLD information display.
<b>disable</b>	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.

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 uddl 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 uddl 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 uddl disable  
UDLD disabled globally  
Console> (enable)
```

---

**Related Commands**    [show uddl](#)

# set udd aggressive-mode

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

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

Syntax Description	<b>enable</b>	Enables UDLD aggressive mode.
	<b>disable</b>	Disables UDLD 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, UDLD 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 UDLD 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 UDLD message interval timer, use the **set udd interval** command.

**set udd interval** *interval*

---

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

---

---

<b>Defaults</b>	The default is 15 seconds.
-----------------	----------------------------

---

---

<b>Command Types</b>	Switch command.
----------------------	-----------------

---

---

<b>Command Modes</b>	Privileged.
----------------------	-------------

---

---

<b>Examples</b>	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)
```

---

<b>Related Commands</b>	<a href="#">set udd</a> <a href="#">show udd</a>
-------------------------	---

---

# 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]
[backupcrf {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.
<b>name</b> <i>name</i>	(Optional) Defines a text string used as the name of the VLAN; valid values are from 1 to 32 characters.
<b>type</b> <i>type</i>	(Optional) Identifies the VLAN type.
<b>state</b> <i>state</i>	(Optional) Specifies whether the state of the VLAN is active or suspended.
<b>said</b> <i>said</i>	(Optional) Specifies the security association identifier; valid values are from 1 to 4294967294.
<b>mtu</b> <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.
<b>bridge</b> <i>bridge_num</i>	(Optional) Specifies the identification number of the bridge; valid values are hexadecimal numbers from 0x1 to 0xF.
<b>mode</b> <i>bridge_mode</i>	(Optional) Specifies the bridge mode; valid values are <b>srt</b> and <b>srb</b> .
<b>stp</b> <i>stp_type</i>	(Optional) Specifies the STP type; valid values are <b>ieee</b> , <b>ibm</b> , and <b>auto</b> .
<b>translation</b> <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.
<b>aremaxhop</b> <i>hopcount</i>	(Optional) Specifies the maximum number of hops for All-Routes Explorer frames; valid values are from 1 to 13.
<b>pvlan-type</b> <i>pvlan-type</i>	(Optional) Keyword and options to specify the private VLAN type. See the “Usage Guidelines” section for valid values.
<b>mistp-instance</b> <i>mistp_instance</i>	(Optional) Specifies the MISTP instance; valid values are <b>none</b> and from 1 to 16.
<b>ring</b> <i>hex_ring_number</i>	(Optional) Keyword to specify the VLAN as the primary VLAN in a private VLAN.
<b>decring</b> <i>decimal_ring_number</i>	(Optional) Specifies the decimal ring number; valid values are from 1 to 4095.
<b>parent</b> <i>vlan_num</i>	(Optional) Specifies the VLAN number of the parent VLAN; valid values are from 1 to 4094.
<b>backupcrf</b> <b>off</b> / <b>on</b>	(Optional) Specifies whether the TrCRF is a backup path for traffic.

<b>stemaxhop</b> <i>hopcount</i>	(Optional) Specifies the maximum number of hops for Spanning Tree Explorer frames; valid values are from 1 to 14.
<b>rspan</b>	(Optional) Creates a VLAN for remote SPAN.
<b>firewall-vlan</b>	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.
<b>msfc-fwsm-interface</b>	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.
- **two-way-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](#)
- [show pvlan](#)
- [show pvlan mapping](#)
- [show vlan](#)

# set vlan mapping

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

**set vlan mapping reserved** *vlan non-reserved* *vlan*

**set vlan mapping dot1q** *1q\_vlan\_num isl* *isl\_vlan\_num*

Syntax Description	reserved <i>vlan</i>	Specifies the reserved VLAN; valid values are from 1006 to 1024.
	<b>non-reserved</b> <i>vlan</i>	Specifies the nonreserved VLAN; valid values are from 1 to 1000 and from 1025 to 4094.
	<b>dot1q</b> <i>1q_vlan_num</i>	Specifies the 802.1Q VLAN; valid values are from 1001 to 4094.
	<b>isl</b> <i>isl_vlan_num</i>	Specifies the ISL VLAN; valid values are from 1 to 1024.

**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.

IEEE 802.1Q VLAN trunks support VLANs 1 through 4094. ISL VLAN trunks support VLANs 1 through 1024 (1005 to 1024 are reserved). The switch automatically maps 802.1Q VLANs 1000 and lower to ISL VLANs with the same number.

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.

The **reserved** *vlan* range is 1002 to 1024. You can map the entire reserved range with the exception of the default media VLANs 1002 to 1005.

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.

---

**Examples**

This example shows how to map reserved VLAN 1010 to nonreserved VLAN 4000:

```
Console> (enable) set vlan mapping reserved 1010 non-reserved 4000
Vlan 1010 successfully mapped to 4000.
Console> (enable)
```

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

```
Console> (enable) set vlan mapping reserved 1011 non-reserved 4001
Vlan mapping from vlan 1011 to vlan 4001 already exists.
Console> (enable)
```

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

```
Console> (enable) set vlan mapping reserved 1010 non-reserved 4000
Vlan mapping table full. Maximum of 8 mappings allowed.
Console> (enable)
```

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 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]
```

<b>Syntax Description</b>	<b>rcp</b>	Specifies rcp as the method for downloading the VLAN Membership Policy Server (VMPS) database.
	<b>tftp</b>	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]
```

<b>Syntax Description</b>	<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 vmps server

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

**set vmps server** *ip\_addr* [**primary**]

**set vmps server** **retry** *count*

**set vmps server** **reconfirminterval** *interval*

Syntax Description		
	<i>ip_addr</i>	IP address of the VMPS.
	<b>primary</b>	(Optional) Specifies the device as the primary VMPS.
	<b>retry</b> <i>count</i>	Specifies the retry interval; valid values are from 1 to 10 minutes.
	<b>reconfirminterval</b> <i>interval</i>	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 vmps 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 vmps server 192.168.69.171  
192.168.69.171 added to VMPS table as backup domain server.  
Console> (enable)
```

---

**Related Commands**

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

# set vmps state

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

```
set vmps 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 vmps state** command, you must use the **set vmps ftpserver** 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 vmps state enable
Vlan membership Policy Server enabled.
Console> (enable)
```

This example shows how to disable VMPS:

```
Console> (enable) set vmps 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 vmps](#)

# set vtp

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

```
set vtp [domain domain_name] [mode {client | server | transparent | off}] [passwd passwd]
[pruning {enable | disable}] [v2 {enable | disable}]
```

## Syntax Description

<b>domain</b> <i>domain_name</i>	(Optional) Defines the name that identifies the VLAN management domain. The <i>domain_name</i> can be from 1 to 32 characters in length.
<b>mode</b> { <b>client</b>   <b>server</b>   <b>transparent</b>   <b>off</b> }	(Optional) Specifies the VTP mode.
<b>passwd</b> <i>passwd</i>	(Optional) Defines the VTP password; the VTP password can be from 8 to 64 characters in length.
<b>pruning</b> { <b>enable</b>   <b>disable</b> }	(Optional) Enables or disables VTP pruning for the entire management domain.
<b>v2</b> { <b>enable</b>   <b>disable</b> }	(Optional) Enables or disables version 2 mode.

## Defaults

The defaults are as follows: server mode, no password, pruning disabled, and v2 disabled.

## Command Types

Switch command.

## Command Modes

Privileged.

## Usage Guidelines

This command is not supported on extended-range VLANs.

VTP pruning and MISTP cannot be enabled at the same time.

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 only need to enable VTP version 2 on one switch (using the **set vtp v2 enable** command); the version number is then propagated to the other version 2-capable switches in the VTP domain.

If the VTP password has already been defined, entering **passwd 0** (zero) clears the VTP password.

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 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.

The **pruning** keyword is used to enable or disable VTP pruning for the 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.

Use the **clear config all** command to remove the domain from the switch.

For more information about VTP, refer to Chapter 10, “Configuring VTP,” in the *Catalyst 6500 Series Switch Configuration Guide*.



#### Caution

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

#### Examples

This example shows how to use the **set vtp** command:

```
Console> (enable) set vtp domain Engineering mode client
VTP domain Engineering 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 command shows how to set VTP to off mode:

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

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

<b>Defaults</b>	The default is VLANs 2 through 1000 are eligible for pruning.
-----------------	---

<b>Command Types</b>	Switch command.
----------------------	-----------------

<b>Command Modes</b>	Privileged.
----------------------	-------------

<b>Usage Guidelines</b>	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 <b>set vtp</b> 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.

<b>Examples</b>	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>
```

<b>Related Commands</b>	<b>clear vtp pruneeligible</b> <b>set vlan</b> <b>show vtp domain</b>
-------------------------	---