

## set spantree portvlancost

To assign a lower path cost to a set of VLANs on a port, use the **set spantree portvlancost** command.

```
set spantree portvlancost mod/port [cost cost_value] [preferred_vlans]
```

Syntax Description	
<i>mod/port</i>	Number of the module and the port on the module.
<b>cost</b> <i>cost_value</i>	(Optional) Indicates the path cost. The port VLAN cost applies only to trunk ports; valid values are from 1 to 65535.
<i>preferred_vlans</i>	(Optional) Preferred VLANs. If you do not list a specific VLAN, the VLANs that were listed in prior use of this command are affected. If you do not list a specific cost, and previous cost values are specified in prior use of the command, then the port VLAN cost is set to one less than the current port cost for a port. However, this might not ensure load balancing in all cases; valid values are from 1 to 1005.

### Defaults

The default settings are as follows:

- The value specified is used as the path cost of the port for the specified set of VLANs.
- The rest of the VLANs have a path cost equal to the port path cost, set with the **set spantree portcost** command.
- If the path cost is not set, the value is the default path cost of the port.

### Command Types

Switch command

### Command Modes

Privileged

### Examples

These examples show various ways to use the **set spantree portvlancost** command:

```
Console> (enable) set spantree portvlancost 2/10 cost 25 1-20
Cannot set portvlancost to a higher value than the port cost, 10, for port 2/10.
Console> (enable)
```

```
Console> (enable) set spantree portvlancost 2/10 1-20
Port 2/10 VLANs 1-20 have a path cost of 9.
Console> (enable)
```

```
Console> (enable) set spantree portvlancost 2/10 cost 4 1-20
Port 2/10 VLANs 1-20 have path cost 4.
Port 2/10 VLANs 21-1000 have path cost 10.
Console> (enable)
Console> (enable) set spantree portvlancost 2/10 cost 6 21
Port 2/10 VLANs 1-21 have path cost 6.
Port 2/10 VLANs 22-1000 have path cost 10.
Console> (enable)
```

These examples show how to use the **set spantree portvlancost** command without explicitly specifying cost:

```
Console> (enable) set spantree portvlancost 1/2  
Port 1/2 VLANs 1-1005 have path cost 3100.  
Console> (enable)
```

```
Console> (enable) set spantree portvlancost 1/2 21  
Port 1/2 VLANs 1-20,22-1005 have path cost 3100.  
Port 1/2 VLANs 21 have path cost 3099.  
Console> (enable)
```

---

**Related Commands**

[clear spantree portvlancost](#)  
[show spantree](#)

# set spantree portvlanpri

To set the port priority for a subset of VLANs in the trunk port, use the **set spantree portvlanpri** command.

```
set spantree portvlanpri mod/port priority [vlans]
```

Syntax Description	
<i>mod/port</i>	Number of the module and the port on the module.
<i>priority</i>	Number that represents the cost of a link in a spanning tree bridge; valid values are <b>0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240</b> , with <b>0</b> indicating high priority and <b>240</b> , low priority. See “Usage Guidelines” for more information.
<i>vlan</i> s	(Optional) VLANs that use the specified priority level; valid values are from 1 to 1005.

## Defaults

The default settings are as follows:

- Port VLAN priority is set to 0.
- No VLANs are specified.

## Command Types

Switch command

## Command Modes

Privileged

## Usage Guidelines

Priority values that are not a multiple of 16 (between the values of 0 to 63) are converted to the nearest multiple of 16. This command is not supported by extended-range VLANs.

Use this command to add VLANs to a specified port priority level. Subsequent calls to this command do not replace VLANs that are already set at a specified port priority level.

This feature is not supported for the MSM.

The **set spantree portvlanpri** command applies only to trunk ports. If you enter this command, this message is displayed:

```
Port xx is not a trunk-capable port
```

If portvlanpri is modified for a set of vlans, then that value will also apply to the already configured set of portvlanpri VLANs and old portvlanpri is lost.

## Examples

This example shows how to set the port priority for module 1, port 2, on VLANs 21 to 40:

```
Console> (enable) set spantree portvlanpri 1/2 16 21-40
Port 1/2 vlans 3,6-20,41-1000 using portpri 32
Port 1/2 vlans 1-2,4-5,21-40 using portpri 16
Console> (enable)
```

■ `set spantree portvlanpri`

**Related Commands** `clear spantree portvlanpri`  
`show spantree`

# set spantree priority

To set the bridge priority for a VLAN or an instance when PVST+ or MISTP is running, use the **set spantree priority** command set.

```
set spantree priority bridge_priority [vlan]
```

```
set spantree priority bridge_priority mistp-instance instances
```

```
set spantree priority bridge_priority mst instances
```

Syntax Description		
	<i>bridge_priority</i>	Number representing the priority of the bridge; see “Usage Guidelines” for valid values.
	<i>vlan</i>	(Optional) Number of the VLAN. If you do not specify a VLAN number, VLAN 1 is used; valid values are from 1 to 1005.
	<b>mistp-instance</b> <i>instances</i>	Instance numbers; valid values are from 1 to 16.
	<b>mst</b> <i>instances</i>	MST instance numbers; valid values are from 0 to 15.

**Defaults** Bridge priority is set to 32768.

**Command Types** Switch command

**Command Modes** Privileged

**Usage Guidelines** If the MAC reduction feature is enabled, valid *bridge\_priority* values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440, with 0 indicating high priority and 61440 indicating low priority. Any other value will be rejected.

If the MAC reduction feature is disabled, valid *bridge\_priority* values are from 0 to 65535.

**Examples** This example shows how to set the bridge priority of instance 3:

```
Console> (enable) set spantree priority 14 mistp-instance 3
Instance 3 bridge priority set to 14.
Instance 3 does not exist.
Your configuration has been saved to NVRAM only.
Console> (enable)
```

This example shows how to set the bridge priority for MST instance 0:

```
Console> (enable) set spantree priority 28672 mst 0
MST Spantree 0 bridge priority set to 28672.
Console> (enable)
```

**set spantree priority**

This example shows how to set the bridge priority for multiple MST instances:

```
Console> (enable) set spantree priority 28672 mst 0-4  
MST Spantrees 0-4 bridge priority set to 28672.  
Console> (enable)
```

---

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

## set spantree root

To set the primary or secondary root for specific VLANs of the switch or for all VLANs of the switch, use the **set spantree root** command set.

```
set spantree root [secondary] [vlans] [dia network_diameter] [hello hello_time]
```

```
set spantree root [secondary] mistp-instance instances [dia network_diameter]
```

```
set spantree root [secondary] mst {instance | {[dia network_diameter] [hello hello_time]}}
```

Syntax Description		
<b>secondary</b>	(Optional) Designates this switch as a secondary root, if the primary root fails.	
<i>vlans</i>	(Optional) Number of the VLAN; valid values are from 1 to 1005.	
<b>dia network_diameter</b>	(Optional) Maximum number of bridges between any two points of attachment of end stations; valid values are from 2 to 7.	
<b>hello hello_time</b>	(Optional) Duration, in seconds, between generation of configuration messages by the root switch; valid values are from 1 to 10.	
<b>mistp-instance instances</b>	Instance number; valid values are from 1 to 16.	
<b>mst instance</b>	Sets the forward delay time for the IST instance and all MST instances.	

### Defaults

The default settings are as follows:

- Switch is the primary root, if no **secondary** keyword is specified.
- Value of *network\_diameter* is 7.
- Current value of *hello\_time* in NVRAM is used, if not specified.

### Command Types

Switch command

### Command Modes

Privileged

### Usage Guidelines

If you do not specify a VLAN number, VLAN 1 is used.

This command is not supported by the NAM.

This command runs on backbone or distribution switches.

This command increases path costs to a value greater than 3000.

If you enable MISTP, you cannot set the VLAN root. If you enable PVST+, you cannot set the instance root.

You can run the secondary root many times to create backup switches for use in case of a root failure.

The **set spantree root secondary** bridge priority value is 16,384 except when MAC reduction or MISTP are enabled, then the value is 28,672.

The **set spantree root** bridge priority value is 16,384 except when MAC reduction or MISTP are enabled, then the value is 24,576.

### Examples

This example shows how to set the primary root for a range of VLANs:

```
Console> (enable) set spantree root 1-10 dia 4
VLANs 1-10 bridge priority set to 8192
VLANs 1-10 bridge max aging time set to 14 seconds.
VLANs 1-10 bridge hello time set to 2 seconds.
VLANs 1-10 bridge forward delay set to 9 seconds.
Switch is now the root switch for active VLANs 1-6.
Console> (enable)
```

This example shows how to set the primary root for an instance:

```
Console> (enable) set spantree root mistp-instance 2-4 dia 4
Instances 2-4 bridge priority set to 8192
VLIstances 2-4 bridge max aging time set to 14 seconds.
Instances 2-4 bridge hello time set to 2 seconds.
Instances 2-4 bridge forward delay set to 9 seconds.
Switch is now the root switch for active Instances 1-6.
Console> (enable)
```

This example shows how to set the primary root for MST instance 5:

```
Console> (enable) set spantree root mst 5
Instance 5 bridge priority set to 24576.
Instance 5 bridge max aging time set to 16.
Instance 5 bridge hello time set to 2.
Instance 5 bridge forward delay set to 15.
Switch is now the root switch for active Instance 5.
Console> (enable)
```

This example shows how to set the secondary root for MST instance 0:

```
Console> (enable) set spantree root secondary mst 0
Instance 0 bridge priority set to 28672.
Instance 0 bridge max aging time set to 20.
Instance 0 bridge hello time set to 2.
Instance 0 bridge forward delay set to 15.
Console> (enable)
```

This example shows how to set the maximum number of bridges and the hello time of the root for MST instance 0:

```
Console> (enable) set spantree root mst 0 dia 7 hello 2
Instance 0 bridge priority set to 24576.
Instance 0 bridge max aging time set to 20.
Instance 0 bridge hello time set to 2.
Instance 0 bridge forward delay set to 15.
Switch is now the root switch for active Instance 0.
Console> (enable)
```

These examples show that setting the bridge priority to 8192 was not sufficient to make this switch the root. So, the priority was further reduced to 7192 (100 less than the current root switch) to make this switch the root switch. However, reducing it to this value did not make it the root switch for active VLANs 16 and 17.

```
Console> (enable) set spantree root 11-20.
VLANs 11-20 bridge priority set to 7192
VLANs 11-10 bridge max aging time set to 20 seconds.
VLANs 1-10 bridge hello time set to 2 seconds.
```

```
VLANS 1-10 bridge forward delay set to 13 seconds.  
Switch is now the root switch for active VLANs 11-15,18-20.  
Switch could not become root switch for active VLAN 16-17.  
Console> (enable)
```

```
Console> (enable) set spantree root secondary 22,24 dia 5 hello 1  
VLANS 22,24 bridge priority set to 16384.  
VLANS 22,24 bridge max aging time set to 10 seconds.  
VLANS 22,24 bridge hello time set to 1 second.  
VLANS 22,24 bridge forward delay set to 7 seconds.  
Console> (enable)
```

---

**Related Commands**

[clear spantree root](#)  
[show spantree](#)

## set spantree uplinkfast

To enable and Uplink Fast Switchover to alternate ports when the root port fails, use the **set spantree uplinkfast** command.

```
set spantree uplinkfast enable [rate station_update_rate] [all-protocols {off | on}]
```

```
set spantree uplinkfast disable
```

Syntax Description		
<b>enable</b>		Enables a fast switchover.
<b>rate</b> <i>station_update_rate</i>		(Optional) Number of multicast packets transmitted per 100 ms when an alternate port is chosen after the root port goes down.
<b>all-protocols</b>		(Optional) Designates whether the switch generates dummy multicast packets for all protocol groups (IP, IPX, and Group) in a network with switches using protocol filtering.
<b>off</b>		(Optional) Prevents the switch from generating multicasts for all protocol groups.
<b>on</b>		(Optional) Causes the switch to generate multicasts for all protocol groups.
<b>disable</b>		Disables Uplink Fast Switchover.

**Defaults** The value for *station\_update\_rate* is 15 packets per 100 ms.

**Command Types** Switch command

**Command Modes** Privileged

**Usage Guidelines** This command applies to a switch, not to a WAN.

The **set spantree uplinkfast enable** command has the following results:

- Changes the bridge priority to 49152 for all VLANs (allowed VLANs).
- Increases the path cost and port VLAN cost of all ports to a value greater than 3000.
- On detecting the failure of a root port, an instant cutover occurs to an alternate port selected by Spanning Tree Protocol.

If you run **set spantree uplinkfast enable** on a switch that has this feature already enabled, only the station update rate is updated. The rest of the parameters are not modified.

If you run **set spantree uplinkfast disable** on a switch, the UplinkFast feature is disabled, but the switch priority and port cost values are not reset to the factory defaults. To reset the values to the factory defaults, enter the **clear spantree uplinkfast** command.

The default *station\_update\_rate* value is 15 packets per 100 ms, which is equivalent to a 1 percent load on a 10-Mbps Ethernet port. If you specify this value as 0, the switch does not generate station-update-rate packets.

Use the **all-protocols on** keywords on switches that have UplinkFast enabled but do not have protocol filtering enabled, and that are connected to upstream switches in the network that have protocol filtering enabled. The **all-protocols on** keywords cause the switch to generate multicasts for each protocol-filtering group.

On switches with both UplinkFast and protocol filtering enabled, or if no other switches have protocol filtering enabled, you do not need to use the **all-protocols on** keywords.

When you try to enable BackboneFast and the switch is in RAPID-PVST+ mode, this message is displayed:

```
Cannot enable backbonefast when the spantree mode is RAPID-PVST+.
```

## Examples

This example shows how to enable the spantree UplinkFast feature and specify the number of multicast packets transmitted to 40 packets per 100 ms:

```
Console>(enable) set spantree uplinkfast enable rate 40
VLANs 1-1005 bridge priority set to 49152.
The port cost and portvlancost of all ports increased to above 3000.
Station update rate set to 40 packets/100ms.
uplinkfast turned on for bridge.
Console> (enable)
```

This example shows how to disable the spantree UplinkFast feature:

```
console> (enable) set spantree uplinkfast disable
Uplinkfast disabled for switch.
Use clear spantree uplinkfast to return stp parameters to default.
console>(enable) clear spantree uplink
This command will cause all portcosts, portvlancosts, and the
bridge priority on all vlans to be set to default.
Do you want to continue (y/n) [n]? y
VLANs 1-1005 bridge priority set to 32768.
The port cost of all bridge ports set to default value.
The portvlancost of all bridge ports set to default value.
uplinkfast disabled for bridge.
Console> (enable)
```

This example shows how to enable the all-protocols feature:

```
Console> (enable) set spantree uplinkfast enable all-protocols on
uplinkfast update packets enabled for all protocols.
uplinkfast already enabled for bridge.
```

This example shows how to disable the all-protocols feature:

```
Console> (enable) set spantree uplinkfast disable all-protocols off
uplinkfast all-protocols field set to off.
uplinkfast already enabled for bridge.
Console> (enable)
```

■ set spantree uplinkfast

**Related Commands**    [clear spantree uplinkfast](#)  
[show spantree](#)

# set summertime

To specify whether the system should set the clock ahead one hour during daylight saving time, use the **set summertime** command.

```
set summertime {enable | disable} [zone]
```

```
set summertime recurring {week} {day} {month} {hh:mm} {week} {day} {month} {hh:mm}
[offset]
```

```
set summertime date {month} {date} {year} {hh:mm} {month} {date} {year} {hh:mm} [offset]
```

## Syntax Description

<b>enable</b>	Sets the clock ahead one hour during daylight saving time.
<b>disable</b>	Prevents the system from setting the clock ahead one hour during daylight saving time.
<i>zone</i>	(Optional) Time zone used by the <b>set summertime</b> command.
<i>week</i>	Week of the month (first, second, third, fourth, last, 1...5).
<i>day</i>	Day of the week; valid values are <b>sunday</b> , <b>monday</b> , <b>tuesday</b> , <b>wednesday</b> , <b>thursday</b> , <b>friday</b> , and <b>saturday</b> .
<i>month</i>	Month of the year; valid values are <b>january</b> , <b>february</b> , <b>march</b> , and so on.
<i>hh:mm</i>	Time in hours and minutes.
<i>offset</i>	(Optional) Amount of offset in minutes; valid values are from 1 to 1440 minutes.
<i>date</i>	Day of the month; valid values are from 1 to 31.
<i>year</i>	Number of the year; valid values are from 1993 to 2035.

## Defaults

The default settings are as follows:

- The command is disabled.
- When enabled, the *offset* is 60 minutes, following U.S. standards.

## Command Types

Switch command

## Command Modes

Privileged

## Usage Guidelines

When you enter the **clear config** command, the dates and times are set back to the default.

Unless otherwise configured, this command advances the clock one hour at 2:00 a.m. on the first Sunday in April and moves the clock back one hour at 2:00 a.m. on the last Sunday in October.

**Examples**

This example shows how to cause the system to set the clock ahead one hour during daylight saving time:

```
Console> (enable) set summertime enable PDT
Summertime is enabled and set to "PDT".
Console> (enable)
```

This example shows how to prevent the system from setting the clock ahead one hour during daylight saving time:

```
Console> (enable) set summertime disable
Summertime disabled.
Console> (enable)
```

This example shows how to set daylight saving time to zone name "AUS," repeat every year, starting from the third Monday of February at noon and ending at the second Saturday of August at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set summertime recurring 3 Mon Feb 03:00 4 Thursday oct 08:00 500
Command authorization none.
Summertime is enabled and set to ''
  start: Mon Feb 21 2000, 03:00:00
  end:   Fri Oct 20 2000. 08:00:00
  offset: 1..1440 minutes (default 60)
  Recurring: yes, starting at 03:00:00am of third Monday of February and ending on
08:00am of fourth Thursday of October.
Console> (enable)
```

This example shows how to set the daylight saving time to start on January 29, 1999 at 2:00 a.m. and end on August 19, 2004 at 3:00 p.m. with an offset of 30 minutes:

```
Console> (enable) set summertime date jan 29 1999 02:00 aug 19 2004 15:00 30
Summertime is disabled and set to ''
Start  : Fri Jan 29 1999, 02:00:00
End    : Thu Aug 19 2004, 15:00:00
Offset : 30 minutes
Recurring: no
Console> (enable)
```

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

# set switchacceleration

To increase the switching bandwidth of the switch, use the **set switchacceleration** command.

```
set switchacceleration {enable | disable} mod
```

Syntax Description	enable	Activates switch acceleration.
	disable	Deactivates switch acceleration.
	mod	Number of the module.

**Defaults** Switch acceleration is disabled.

**Command Types** Switch command

**Command Modes** Privileged

**Usage Guidelines** The **set switchacceleration** command is valid only on Catalyst 4000 family switches with Supervisor Engine II. To enable switch acceleration on the switch, you must disable both the ports on it. Switch acceleration on the switch can be disabled without any conditions.

**Examples** This example shows how to enable switch acceleration on port 1 of module 1 on the switch:

```
Console> (enable) set switchacceleration enable 1
Enabling or Disabling switch acceleration may impact performance for 1-2 seconds.
Do you want to continue (y/n) [n]? y
Switch Acceleration on module 1 enabled.
Console> (enable)
```

This example shows how to disable switch acceleration on port 1 of module 1 on the switch:

```
Console> (enable) set switchacceleration disable 1
Enabling or Disabling switch acceleration may impact performance for 1-2 seconds.
Do you want to continue (y/n) [n]? y
Switch Acceleration on module 1 disabled.
Console> (enable)
```

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

# set system baud

To set the console port baud rate, use the **set system baud** command.

**set system baud** *rate*

<b>Syntax Description</b>	<i>rate</i> Baud rate; valid baud rates are <b>600, 1200, 2400, 4800, 9600, 19200,</b> and <b>38400</b> .
---------------------------	---

<b>Defaults</b>	9600 baud
-----------------	-----------

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

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

<b>Examples</b>	This example shows how to set the system baud rate to 19,200:
-----------------	---

```
Console> (enable) set system baud 19200
System console port baud rate set to 19200.
Console> (enable)
```

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

# set system contact

To identify a contact person for the system, use the **set system contact** command.

```
set system contact [contact_string]
```

---

<b>Syntax Description</b>	<i>contact_string</i> (Optional) Contains the name of the person to contact for system administration. If no contact string is specified, the system contact string is cleared.
---------------------------	---

---

---

<b>Defaults</b>	No system contact is configured.
-----------------	----------------------------------

---

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

---

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

---

<b>Examples</b>	This example shows how to set the system contact string to Xena at ext. 24:
-----------------	---

```
Console> (enable) set system contact Xena ext.24  
System contact set.  
Console> (enable)
```

---

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

# set system countrycode

To specify the country where the system is physically located, use the **set system countrycode** command.

**set system countrycode** *code*

<b>Syntax Description</b>	<i>code</i> Country code. See “Usage Guidelines” for more information.
<b>Defaults</b>	Country is set to US (United States).
<b>Command Types</b>	Switch command
<b>Command Modes</b>	Privileged
<b>Usage Guidelines</b>	The country code is a 2-letter country code taken from ISO-3166 (for example, VU=Vanuatu and TF=French Southern Territories).
<b>Examples</b>	<p>This example shows how to set the system country code to Great Britain:</p> <pre> Console&gt; (enable) <b>set system countrycode GB</b> Country code is set to GB Console&gt; (enable) </pre>

# set system location

To identify the location of the system, use the **set system location** command.

```
set system location [location_string]
```

---

<b>Syntax Description</b>	<i>location_string</i> (Optional) Indicates where the system is located.
---------------------------	--

---

---

<b>Defaults</b>	This command has no default settings.
-----------------	---------------------------------------

---

---

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

---

---

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

---

---

<b>Usage Guidelines</b>	If no <i>location_string</i> is specified, the system location is cleared.
-------------------------	--

---

---

<b>Examples</b>	This example shows how to set the system location string to Closet 230 on the 4th floor:
-----------------	--

```
Console> (enable) set system location Closet 230 4/F  
System location set.  
Console> (enable)
```

---

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

---

# set system modem

To enable or disable modem control lines on the console port, use the **set system modem** command.

```
set system modem {enable | disable}
```

Syntax Description	enable	Deactivates modem control lines on the console port.
	disable	Activates modem control lines on the console port.

**Defaults** Modem control lines are disabled.

**Command Types** Switch command

**Command Modes** Privileged

**Examples** This example shows how to enable modem control lines on the console port:

```
Console> (enable) set system modem enable
Modem control lines enabled on console port.
Console> (enable)
```

This example shows how to disable modem control lines on the console port:

```
Console> (enable) set system modem disable
Modem control lines disabled on console port.
Console> (enable)
```

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

# set system name

To configure a name for the system, use the **set system name** command.

```
set system name [name_string]
```

---

<b>Syntax Description</b>	<i>name_string</i> (Optional) Identifies the system.
---------------------------	--

---

---

<b>Defaults</b>	No system name is configured.
-----------------	-------------------------------

---

---

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

---

---

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

---

---

<b>Usage Guidelines</b>	<p>In Catalyst 4000 family software release 4.4 and later, if you use the <b>set system name</b> command to assign a name to the switch, the switch name is used as the prompt string. However, if you specify a different prompt string using the <b>set prompt</b> command, that string is used for the prompt. If no name is specified, the system name is cleared.</p>
-------------------------	--

The system name can be 255 characters long, and the prompt can be 20 characters long. The system name is truncated appropriately when used as a prompt; a greater-than symbol (>) is appended to the truncated system name. If the system name was found from a DNS lookup, it is truncated to delete the domain name. If the prompt is obtained using the system name, it is updated whenever the system name changes. You can overwrite this prompt any time by setting the prompt manually. Any change in the prompt is reflected in all current open sessions.

---

<b>Examples</b>	This example shows how to set the system name to Information Systems:
-----------------	---

```
Console> (enable) set system name Information Systems  
System name set.  
Console> (enable)
```

---

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

---

# set system syslog-dump

To configure the switch to write the syslog buffer to a file before a crash, use the **set system syslog-dump** command.

```
set system syslog-dump {enable | disable}
```

## Syntax Description

<b>enable</b>	Enables syslog dump.
<b>disable</b>	Disables syslog dump.

## Defaults

Syslog dump is enabled.

## Command Types

Switch command

## Command Modes

Privileged

## Usage Guidelines

Disabling the **set system syslog-dump** command does not prevent you from configuring the syslog-file through the **set system syslog file** command.

## Examples

This example shows how to enable the switch to dump the syslog buffer to a flash file before a crash:

```
Console> (enable) set system core-dump enable
      Syslog-dump enabled
Console> (enable)
```

This example shows how to disable the switch from dumping the syslog buffer to a flash file before a crash:

```
Console> (enable) set system core-dump disable
      Syslog-dump disabled
Console> (enable)
```

## Related Commands

[set system syslog file](#)

## set system syslog file

To set the Flash filename that the syslog buffer is written to if the switch crashes, use the **set system syslog file** command.

```
set system syslog file device:filename
```

### Syntax Description

<i>device:</i>	Flash device name; valid devices include <b>bootflash:</b> , <b>slot0:</b> , and <b>slot1:</b> .
<i>filename</i>	Filename for the syslog buffer on the Flash device.

### Defaults

The Flash filename is bootflash:sysloginfo.

### Command Types

Switch command

### Command Modes

Privileged

### Usage Guidelines

You can set a syslog filename even if the **set system syslog-dump** command is disabled.

The syslog buffer is written to the specified file only if the switch crashes.

The syslog buffer is written to the specified file only if the **set system syslog-dump** command is enabled and the switch crashes. If the Flash file cannot be opened by the switch no further action will be taken and the syslog will not be written to the Flash file.

If you disable the **set system syslog-dump** command the syslog filename can still be set through the **set system syslog file** command.

### Examples

This example shows how to set the syslog file to the bootflash:sysloginfo1:

```
Console> (enable) set system syslog-file bootflash:sysloginfo1
  System syslog-file set.
Console> (enable)
```

### Related Commands

[set system syslog-dump](#)

# set tacacs directedrequest

To enable or disable the TACACS+ directed-request option, use the **set tacacs directedrequest** command.

**set tacacs directedrequest {enable | disable}**

Syntax Description	enable	Sends the portion of the address before the at (@) symbol (the username) to the host specified after the @ sign.
	disable	Sends the entire address string to the default TACACS+ server.

**Defaults** The TACACS+ directed-request option is disabled.

**Command Types** Switch command

**Command Modes** Privileged

**Usage Guidelines** When enabled, you can direct a request to any of the configured TACACS+ servers and only the username is sent to the specified server.

When **tacacs directedrequest** is enabled, you must specify a configured TACACS+ server after the @ sign. If the specified host name does not match the IP address of a configured TACACS+ server, the request is rejected. When **tacacs directedrequest** is disabled, the 4000 family, 2948G, and 2980G switch queries the list of servers beginning with the first server in the list and then sends the entire string, accepting the first response from the server. This command is useful for sites that have developed their own TACACS+ server software to parse the entire address string and make decisions based on the contents of the string.

**Examples** This example shows how to enable the TACACS+ directed-request option:

```
Console> (enable) set tacacs directedrequest enable
Tacacs direct request has been enabled.
Console> (enable)
```

This example shows how to disable the TACACS+ directed-request option:

```
Console> (enable) set tacacs directedrequest disable
Tacacs direct request has been disabled.
Console> (enable)
```

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

# set tacacs key

To set the key for TACACS+ authentication and encryption, use the **set tacacs key** command.

```
set tacacs key key
```

<b>Syntax Description</b>	<i>key</i> Printable ASCII characters used for authentication and encryption.
<b>Defaults</b>	The key is set to NULL.
<b>Command Types</b>	Switch command
<b>Command Modes</b>	Privileged
<b>Usage Guidelines</b>	The key length that you set must be less than 100 characters. The key must be the same as the key used on the TACACS+ server. All leading spaces are ignored. Spaces within the key and at the end of the key are included. Double quotation marks are not required, even if there are spaces between words in the key, unless the quotation marks themselves are part of the key. The key can consist of any printable ASCII characters except the tab character.
<b>Examples</b>	This example shows how to set the authentication and encryption key:  Console> (enable) <b>set tacacs key Who Goes There</b> The tacacs key has been set to Who Goes There. Console> (enable)
<b>Related Commands</b>	<a href="#">clear tacacs key</a> <a href="#">show tacacs</a>

## set tacacs server

To define a TACACS+ server, use the **set tacacs server** command.

```
set tacacs server ip_addr [primary]
```

<b>Syntax Description</b>	<i>ip_addr</i>	IP address of the server on which the TACACS+ server resides.
	<b>primary</b>	(Optional) Designates the specified server as the primary TACACS+ server.

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

**Command Types** Switch command

**Command Modes** Privileged

**Usage Guidelines** You can configure a maximum of three servers. The primary server, if configured, is contacted first. If no primary server is configured, the first server configured becomes the primary server.

**Examples** This example shows how to configure the server on which the TACACS+ server resides and to designate it as the primary server:

```
Console> (enable) set tacacs server 170.1.2.20 primary
170.1.2.20 added to TACACS server table as primary server.
Console> (enable)
```

**Related Commands** [clear tacacs server](#)  
[show tacacs](#)

# set tacacs timeout

To set the response timeout interval for the TACACS+ server daemon, use the **set tacacs timeout** command.

**set tacacs timeout** *seconds*

<b>Syntax Description</b>	<i>seconds</i> Timeout response interval in seconds; valid values are from 1 to 255.
<b>Defaults</b>	5 seconds
<b>Command Types</b>	Switch command
<b>Command Modes</b>	Privileged
<b>Usage Guidelines</b>	The TACACS+ server must respond to a TACACS+ authentication request before this interval expires or the next configured server is queried.
<b>Examples</b>	This example shows how to set the response timeout interval for the TACACS+ server to 8 seconds: <pre>Console&gt; (enable) <b>set tacacs timeout 8</b> Tacacs timeout set to 8 seconds. Console&gt; (enable)</pre>
<b>Related Commands</b>	<a href="#">show tacacs</a>

# set test diaglevel

To set the diagnostic level, use the **set test diaglevel** command.

```
set test diaglevel { complete | minimal | bypass }
```

Syntax Description	complete	Minimal diagnostics.
	minimal	Minimal diagnostics.
	bypass	Bypasses diagnostics.

**Defaults** Complete diagnostics

**Command Types** Switch command

**Command Modes** Privileged

**Usage Guidelines** The **minimal** keyword is not supported at this time. Setting the diagnostic level to minimal will be ignored.

Setting the diagnostic level to bypass will skip POST and online diagnostic testing. If you skip diagnostic testing, the **show test mod\_num** command reports that the module has passed all tests.



**Caution**

Be careful when setting the diagnostic level to bypass. Bypassing diagnostic tests allows hardware failures to go undetected and could cause other problems.

**Examples** This example shows how to set the diagnostic level to complete:

```
Console> (enable) set test diaglevel complete
Diagnostic level set to complete.
Console> (enable)
```

This example shows how to set the diagnostic level to minimal:

```
Console> (enable) set test diaglevel minimal
Diagnostic level set to minimal.
Console> (enable)
```

This example shows how to set the diagnostic level to bypass:

```
Console> (enable) set test diaglevel bypass
Diagnostic level set to bypass.
Console> (enable)
```

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

# set time

To change the time of day on the system clock, use the **set time** command.

```
set time [day_of_week] [mm/dd/yyyy] [hh:mm:ss]
```

Syntax Description	
<i>day_of_week</i>	(Optional) Day of the week; valid values are <b>mon</b> , <b>tues</b> , <b>wed</b> , <b>thur</b> , <b>fri</b> , <b>sat</b> , and <b>sun</b> .
<i>mm/dd/yyyy</i>	(Optional) Month (in numeric form), day, and year.
<i>hh:mm:ss</i>	(Optional) Current time, in 24-hour format.

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

**Command Types** Switch command

**Command Modes** Privileged

**Examples** This example shows how to set the system clock to Sunday, March 21, 2000, 7:50 a.m:

```
Console> (enable) set time sun 03/21/2000 7:50
Sun Mar 21 2000, 07:50:00
Console> (enable)
```

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

# set timezone

To set the time zone for the system, use the **set timezone** command.

```
set timezone [zone_name] [hours [minutes]]
```

Syntax Description	
<i>zone_name</i>	(Optional) Name of the time zone to be displayed.
<i>hours</i>	(Optional) Number of hours offset from UTC; valid values are from -12 to 12.
<i>minutes</i>	(Optional) Number of minutes offset from UTC; valid values are from 0 to 59.

**Defaults** The time zone is set to UTC.

**Command Types** Switch command

**Command Modes** Privileged

**Usage Guidelines** If the specified hours value is a negative number, then the minutes value is assumed to be negative as well.

The **set timezone** command is effective only when NTP is running. If you set the time explicitly and NTP is disengaged, the **set timezone** command has no effect. If you have enabled NTP and have not entered the **set timezone** command, the Catalyst 4000 family switch displays UTC by default.

**Examples** This example shows how to set the time zone to Pacific Standard Time with an offset of -8 hours from UTC:

```
Console> (enable) set timezone PST -8
Timezone set to "PST", offset from UTC is -8 hours.
Console> (enable)
```

**Related Commands** [clear timezone](#)  
[show timezone](#)

# set trace

To obtain the debugging information for the switch web interface, use the **set trace** command.

```
set trace {category} [level]
```

```
set trace monitor {enable | disable}
```

## Syntax Description

<i>category</i>	Trace category.
<i>level</i>	(Optional) Trace level; see “Usage Guidelines” for valid values.
<b>monitor</b>	Monitors the switch web interface for debugging information.
<b>enable</b>	Enables the trace monitor.
<b>disable</b>	Disables the trace monitor.

## Defaults

The trace level is set to 1.

## Command Types

Switch command

## Command Modes

Privileged

## Usage Guidelines

Valid values for the trace level are 0 to 15. Trace levels 0 to 255 are for inband only. To disable the trace level, set the value to 0.

## Examples

This example shows how to obtain switch web interface debugging information:

```
Console> (enable) set trace vmps
VMPS tracing set to 1.
Warning!! Turning on trace may affect the operation of the system.
Use with caution.
Console> (enable)
```

This example shows how to enable trace monitoring:

```
Console> (enable) set trace monitor enable
Trace monitor is enabled for this session.
Console> (enable)
```

This example shows how to disable trace monitoring:

```
Console> (enable) set trace monitor disable
Trace monitor is disabled for this session.
Console> (enable)
```

## Related Commands

[show trace](#)

# set traffic monitor

To configure the threshold at which a high traffic log will be generated, use the **set traffic monitor** command.

**set traffic monitor** *threshold*

<b>Syntax Description</b>	<i>threshold</i>	Threshold percentage at which a high traffic log will be generated; valid values are from 0 to 100 percent.
---------------------------	------------------	---

<b>Defaults</b>	The default settings are as follows: <ul style="list-style-type: none"> <li>• <i>threshold</i> is set to 100 percent</li> <li>• No high traffic log is created</li> </ul>
-----------------	---

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

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

<b>Usage Guidelines</b>	If backplane traffic exceeds the threshold configured by the <b>set traffic monitor</b> command, a high traffic log is created. If the threshold is set to 100 percent, no high-traffic system warning is generated.
-------------------------	--

<b>Examples</b>	This example shows how to set the high traffic threshold to 80 percent:
-----------------	---

```
Console> (enable) set traffic monitor 80
Traffic monitoring threshold set to 80%.
Console> (enable)
```

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

# set trunk

To configure trunk ports and to add VLANs to the allowed VLAN list for existing trunks, use the **set trunk** command.

```
set trunk mod/port [on | off | desirable | auto | nonegotiate] [vlan_range] [isl | dot1q | dot10 | lane | negotiate]
```

Syntax Description	
<i>mod/port</i>	Number of the module and the port on the module.
<b>on</b>	(Optional) Forces the port to become a trunk port and persuade the neighboring port to become a trunk port.
<b>off</b>	(Optional) Forces a port to become a nontrunk port and persuades the neighboring port to become a nontrunk port.
<b>desirable</b>	(Optional) Causes a port to negotiate actively with the neighbor port to become a trunk link. This mode is not allowed on FDDI and ATM ports.
<b>auto</b>	(Optional) Causes the port to become a trunk port if the neighboring port tries to negotiate a trunk link.
<b>nonegotiate</b>	(Optional) Forces the port to become a trunk port but prevents it from sending DTP frames to its neighbor.
<i>vlan_range</i>	(Optional) Adds VLANs to the list of allowed VLANs on the trunk; valid values are from 1 to 1005.
<b>isl</b>	(Optional) ISL trunk on an Ethernet port.
<b>dot1q</b>	(Optional) IEEE 802.1Q trunk on an Ethernet port.
<b>dot10</b>	(Optional) IEEE 802.10 trunk on a FDDI or CDDI port.
<b>lane</b>	(Optional) ATM LANE trunk on an ATM port.
<b>negotiate</b>	(Optional) Causes the port to become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring port.

## Defaults

The default settings are as follows:

- All non-ATM LANE ports are nontrunk ports.
- ATM LANE ports are trunk ports.
- RSM ports are trunk ports.

## Command Types

Switch command

## Command Modes

Privileged

**Usage Guidelines**

When you configure a port to trunk it becomes a trunk port even if the neighbor port does not agree to become a trunk. The only possible mode for ATM ports is **on**.

When you configure a port not to trunk it becomes a nontrunk port even if the neighbor port does not agree to become a nontrunk port. This is the default mode for FDDI trunks. This option is not allowed for ATM ports.

Setting the mode to **auto** is not allowed on FDDI and ATM ports. This is the default mode for Fast Ethernet and Gigabit Ethernet ports.

Setting the mode to **nonegotiate** is allowed only on ISL and IEEE 802.1Q trunks.

IEEE 802.1Q trunks are supported in Catalyst 5000 family and 2926G series software release 4.1(1) and later with 802.1Q-capable hardware. Automatic negotiation of 802.1Q trunks is supported in software release 4.2(1) and later. In software release 4.1, you must use the **nonegotiate** keyword with 802.1Q trunks.

Trunking capabilities are hardware dependent. Refer to the *Module Installation Guide* for your switch to determine the trunking capabilities of your hardware, or enter the **show port capabilities** command.

The Catalyst 4000 family switches use the DTP (formerly known as DISL) to negotiate trunk links automatically on Fast Ethernet and Gigabit Ethernet ports. Whether a port will negotiate to become a trunk port depends on both the mode and the trunk type specified for that port. Refer to the *Software Configuration Guide—Catalyst 4000 Family, 2948G, and 2980G Switches* for detailed information on how trunk ports are negotiated.

DTP is a point-to-point protocol. However, some internetworking devices might improperly forward DTP frames. You can avoid this problem by ensuring that trunking is turned **off** on ports connected to non-Catalyst 4000 family devices if you do not intend to trunk across those links. When enabling trunking on a link to a Cisco router, enter the **nonegotiate** keyword to cause the port to become a trunk but not generate DTP frames. The **nonegotiate** keyword is available in Catalyst 4000 family software release 2.4(3) and later.

For trunking to be negotiated on Fast Ethernet and Gigabit Ethernet ports, the ports must be in the same VTP domain. However, you can use the **on** or **nonegotiate** keywords to force a port to become a trunk, even if it is in a different domain.

To delete VLANs from the allowed list for a trunk, enter the **clear trunk mod\_num/port\_num vlan\_range** command. When you first configure a port as a trunk, the **set trunk** command always adds *all* VLANs to the allowed VLAN list for the trunk, even if you specify a VLAN range (the specified VLAN range is ignored).

To delete VLANs from the allowed list, enter the **clear trunk mod\_num/port\_num vlan\_range** command. To later add VLANs that were deleted, enter the **set trunk mod\_num/port\_num vlan\_range** command.

If you do not enter a trunk-type keyword, the value is unchanged from the previous configuration.

The **dot1q** trunk type is the only trunk type supported by the Catalyst 4000 family switches.

To return a trunk to its default trunk type and mode, enter the **clear trunk mod\_num/port\_num** command.

If you enter the **set trunk** command on a Token Ring port, you receive a message indicating that the port is “not a trunk-capable port.”

When you are running the **set trunk** command on an Access Gateway module, you have limited usage of the command.

---

**Examples**

This example shows how to set port 2 on module 1 as a trunk port:

```
Console> (enable) set trunk 1/2 on  
Port(s) 1/2 trunk mode set to on.  
Console> (enable)
```

This example shows how to set port 2 on module 1 as a nontrunk port:

```
Console> (enable) set trunk 1/2 off  
Port(s) 1/2 trunk mode set to off.  
Console> (enable)
```

This example shows how to set port 2 on module 1 as a preferred trunk port:

```
Console> (enable) set trunk 1/2 desirable  
Port(s) 1/2 trunk mode set to desirable.  
Console> (enable) 2000 Jan 11 09:16:29 %DTP-5-TRUNKPORTON:Port 1/2 has become ik
```

This example shows how to add VLANs 5 through 50 to the allowed VLAN list for a trunk port (VLANs were previously deleted from the allowed list with the **clear trunk** command):

```
Console> (enable) set trunk 1/1 5-50  
Adding vlans 5-50 to allowed list.  
Port(s) 1/1 allowed vlans modified to 1,5-50,101-1005.  
Console> (enable)
```

This example shows how to set port 5 on module 4 as an 802.1Q trunk port in desirable mode:

```
Console> (enable) set trunk 4/5 desirable dot1q  
Port(s) 4/5 trunk mode set to desirable.  
Port(s) 4/5 trunk type set to dot1q.  
Console> (enable)
```

This example shows how to set port 1 on module 1 as an ISL trunk port:

```
Console> (enable) set trunk 1/1 isl  
Port(s) 1/1 trunk type set to isl.  
Console> (enable)
```

---

**Related Commands**

[clear trunk](#)  
[set vtp](#)  
[show trunk](#)  
[show vtp statistics](#)

# set uddl

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

```
set uddl {enable | disable} mod/ports...
```

## Syntax Description

<b>enable</b>	Enables the UDLD feature.
<b>disable</b>	Disables the UDLD feature.
<i>mod/ports...</i>	Number of the module and ports.

## Defaults

UDLD is disabled globally.

## 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 (via 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 UDLD is running on an interface or not depends on its per-port configuration.

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

## Examples

This example shows how to enable the UDLD feature 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 on all the ends of the connection
in order to work properly.
Console> (enable)
```

This example shows how to disable the UDLD feature 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 on all the ends of the connection
in order to work properly.
Console> (enable)
```

This example shows how to enable the UDLD feature 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 UDLD aggressive mode on specified ports or globally on all ports, use the **set udd aggressive-mode** command.

```
set udd aggressive-mode {enable | disable} mod/port
```

Syntax Description	enable	enable
	enable	Enables UDLD aggressive mode.
	disable	Disables UDLD aggressive mode.
	mod/port	Number of the module and port(s).

**Defaults** Aggressive mode is disabled.

**Command Types** Switch command

**Command Modes** Privileged

**Usage Guidelines** After all the neighbors of a port have aged out either in the advertisement or in the detection phase, aggressive mode allows UDLD to restart the linkup sequence to resynchronize with any potentially out-of-sync neighbors, and shut down the port if the link is still undetermined after the fast train of messages.

You also can enable aggressive mode to shut down an active port that does not support FEF1 or autonegotiation and becomes connected to its neighbor by a single fiber strand or copper wire after being part of a bidirectional link. This prevents possible spanning tree loops if the port belongs to a channel.

**Examples** This example shows how to enable aggressive mode:

```
Console> (enable) set udd aggressive-mode enable 2/1
Aggressive UDLD enabled on port 2/1.
Warning: UniDirectional Link Detection should be enabled on all the ends of the connection
in order to work properly.
Console> (enable)
```

This example shows how to disable aggressive mode:

```
Console> (enable) set udd aggressive-mode disable 2/1
Aggressive UDLD disabled on port 2/1.
Warning: UniDirectional Link Detection should be enabled on all the ends of the connection
in order to work properly.
Console> (enable)
```

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

# set udd interval

To set the UDDL 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>	UDDL message interval timer is set to 60 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  
UDDL message interval set to 90 seconds  
Console> (enable)
```

---

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

---

# set vlan

To group ports into a VLAN, set the private VLAN type, or map or unmap VLANs to or from an instance, 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]
```

## Syntax Description

<i>vlans</i>	Number identifying the VLAN; valid values are from <b>1</b> to <b>1000</b> and from <b>1025</b> to <b>4094</b> .
<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) Designates whether the state of the VLAN is active or suspended.
<b>said</b> <i>said</i>	(Optional) Security association identifier; valid values are from <b>1</b> to <b>4294967294</b> .
<b>mtu</b> <i>mtu</i>	(Optional) Maximum transmission unit (packet size, in bytes) that the VLAN can use; valid values are from <b>576</b> to <b>18190</b> .
<b>bridge</b> <i>bridge_num</i>	(Optional) Identification number of the bridge; valid values are hexadecimal numbers from <b>0x1</b> to <b>0xF</b> .
<b>mode</b> <i>bridge_mode</i>	(Optional) Bridge mode; valid values are <b>srt</b> and <b>srb</b> .
<b>stp</b> <i>stp_type</i>	(Optional) STP type; valid values are <b>ieee</b> , <b>ibm</b> , and <b>auto</b> .
<b>translation</b> <i>vlan_num</i>	(Optional) Translational VLAN used to translate FDDI or Token Ring to Ethernet; valid values are from <b>1</b> to <b>1000</b> and from <b>1025</b> to <b>4094</b> .
<b>aremaxhop</b> <i>hopcount</i>	(Optional) Maximum number of hops for All-Routes Explorer frames; valid values are from <b>1</b> to <b>13</b> .
<b>pvlan-type</b> <i>pvlan-type</i>	(Optional) Private VLAN type. See the “Usage Guidelines” section for valid values.
<b>mistp-instance</b> <i>mistp_instance</i>	(Optional) MISTP instance; valid values are <b>none</b> and from <b>1</b> to <b>16</b> .
<b>ring</b> <i>hex_ring_number</i>	(Optional) VLAN as the primary VLAN in a private VLAN.
<b>decring</b> <i>decimal_ring_number</i>	(Optional) Decimal ring number; valid values are from <b>1</b> to <b>4095</b> .
<b>parent</b> <i>vlan_num</i>	(Optional) VLAN number of the parent VLAN; valid values are from <b>1</b> to <b>1000</b> and from <b>1025</b> to <b>4094</b> .
<b>backupcrf</b> <b>off</b>   <b>on</b>	(Optional) Designates whether the TrCRF is a backup path for traffic. TrCRFs are achieved when you subdivide a Token Ring switching module into multiple virtual rings.

<b>stemaxhop</b> <i>hopcount</i>	(Optional) Specifies the maximum number of hops for Spanning Tree Explorer frames; valid values are from <b>1</b> to <b>14</b> .
<b>rspan</b>	(Optional) Creates a VLAN for remote SPAN.

### Defaults

The default settings 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 non.e
- *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

If you are configuring Normal-range VLANs, you cannot use the **set vlan** command until the Catalyst 4000 family 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.

VLAN 1 parameters are factory configured and cannot be changed.

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 1000 or 1025 to 4094.

If you want to use the extended-range VLANs (1025 to 4094), you must enable the MAC address reduction feature using the **set spantree macreduction** command. When you enable MAC address reduction, the pool of MAC addresses used for the VLAN spanning tree is disabled, leaving a single MAC address that identifies the switch.

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 4000 family 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 1025 to 4094 are extended-range VLANs.

VLANs in a suspended state do not pass packets.

## Examples

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

```
Console> (enable) set vlan 850 3/4-7
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)
```

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

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

<b>Syntax Description</b>	<p><b>dot1q</b> <i>1q_vlan_num</i> 802.1Q VLAN; valid values are from <b>1001</b> to <b>4094</b>.</p> <p><b>isl</b> <i>isl_vlan_num</i> ISL VLAN; valid values are from <b>1</b> to <b>1024</b>.</p>
<b>Defaults</b>	This command has no default settings.
<b>Command Types</b>	Switch command
<b>Command Modes</b>	Privileged
<b>Usage Guidelines</b>	<p>VLAN and MISTP instance mapping can be set only on the switch that is in either VTP server mode or in transparent mode.</p> <p>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.</p> <p>Use this feature to map 802.1Q VLANs above 1000 to ISL VLANs.</p> <p>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.</p> <p>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.</p> <p>The <b>reserved</b> <i>vlan</i> range is 1002 to 1024. You can map the entire reserved range with the exception of the default media VLANs 1002 to 1005.</p> <p>You cannot overwrite existing VLAN mapping. If the VLAN number already exists, the command is aborted. You must first clear that mapping.</p> <p>If the VLAN number does not exist, then either of the following occurs:</p> <ul style="list-style-type: none"> <li>• If the switch is in server or transparent mode, the VLAN is created with all default values.</li> <li>• 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.</li> </ul> <p>If the table is full, the command is aborted with an error message indicating the table is full. dot1q VLANs are rejected if any extended-range VLANs are present.</p>

---

**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]
```

Syntax Description		
	<b>rcp</b>	Uses rcp as the method for downloading the VMPS database.
	<b>tftp</b>	Uses TFTP as the method for downloading the VMPS database.
	<i>username</i>	(Optional) Username for downloading with rcp.

**Defaults** TFTP will be used if no other method is specified.

**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** Filename vmps-config-database.1 is used if no filename is specified.

**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 vmips server

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

```
set vmips server ip_addr [primary]
```

```
set vmips server retry count
```

```
set vmips server reconfirminterval interval
```

### Syntax Description

<i>ip_addr</i>	IP address of the VMPS server.
<b>primary</b>	(Optional) Device as the primary VMPS server.
<b>retry count</b>	Retry interval; valid values are from <b>1</b> to <b>10</b> minutes.
<b>reconfirminterval interval</b>	Reconfirmation interval; valid values are from <b>0</b> to <b>120</b> minutes.

### Defaults

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

### Command Types

Switch command

### Command Modes

Privileged

### Usage Guidelines

You can specify the IP addresses of up to three VMPS servers. You can define any VMPS server as the primary VMPS server.

If the primary VMPS server is down, all subsequent queries go to a secondary VMPS server. VMPS checks on the primary server's availability once every five minutes. When the primary VMPS server comes back online, subsequent VMPS queries are directed back to the primary VMPS server.

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 server:

```
Console> (enable) set vmips 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 server:

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

### Related Commands

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

# set vmps state

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

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

<b>Syntax Description</b>	<table border="1"> <tr> <td><b>enable</b></td> <td>Enables VMPS.</td> </tr> <tr> <td><b>disable</b></td> <td>Disables VMPS.</td> </tr> </table>	<b>enable</b>	Enables VMPS.	<b>disable</b>	Disables VMPS.
<b>enable</b>	Enables VMPS.				
<b>disable</b>	Disables VMPS.				
<b>Defaults</b>	Disabled				
<b>Command Types</b>	Switch command				
<b>Command Modes</b>	Privileged				
<b>Usage Guidelines</b>	Before using the <b>set vmps state</b> command, you must use the <b>set vmps tftpserver</b> command to specify the IP address of the server from which the VMPS database is downloaded.				
<b>Examples</b>	<p>This example shows how to enable VMPS:</p> <pre>Console&gt; (enable) set vmps state enable Vlan membership Policy Server enabled. Console&gt; (enable)</pre> <p>This example shows how to disable VMPS:</p> <pre>Console&gt; (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&gt; (enable)</pre>				
<b>Related Commands</b>	<ul style="list-style-type: none"> <li><a href="#">download</a></li> <li><a href="#">show vmps</a></li> </ul>				

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

### Defaults

The default settings are as follows:

- Server mode
- No password
- Pruning disabled
- 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, enable VTP version 2 on one switch (using the **set vtp v2 enable** command). The version number is automatically 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. Be sure you 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 VTP “off” mode, the switch behaves the same as in VTP transparent mode with the exception 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 deleted from VTP updates if there are no stations belonging to that VLAN on a particular switch port. Use the **set vtp pruneeligible** and **clear vtp pruning** 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 delete the domain from the switch.

For more information about VTP, refer to Chapter 10, “Configuring VTP,” in the *Catalyst 6000 Family 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

**show vtp domain**  
**set vlan**  
**clear vlan**  
**show vlan**  
**set vtp pruneeligible**  
**clear vtp pruning**

# set vtp pruneeligible

To specify the VTP domain on which VLANs are prune 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>	VLANs 2 to 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 deleted from VTP updates if there are no stations belonging to that VLAN on a particular switch port. Use the <b>set vtp</b> command to enable VTP pruning.
-------------------------	---

By default, VLANs 2 to 1000 are pruning eligible. You do not need to use the **set vtp pruning** command unless you have previously used the **clear vtp pruning** command to make some VLANs pruning ineligible. If VLANs have been made pruning ineligible, use the **set vtp pruning** 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 to 500 were made pruning ineligible using the **clear vtp pruning** command. This example shows how to make VLANs 220 to 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 pruning</b> <b>set vlan</b> <b>show vtp domain</b>
-------------------------	---

# set vtp pruning

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

**set vtp pruning** *vlan*s

<b>Syntax Description</b>	<i>vlan</i> s                      Range of VLAN numbers; valid values are from 2 to 1000.
<b>Defaults</b>	VLANs 2 to 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 deleted 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. You do not need to use the <b>set vtp pruning</b> command unless you have previously used the <b>clear vtp pruning</b> command to make some VLANs pruning ineligible. If VLANs have been made pruning ineligible, use the <b>set vtp pruning</b> command to make them pruning eligible again.
<b>Examples</b>	<p>This example shows how to configure pruning eligibility for VLANs 120 and 150:</p> <pre>Console&gt; (enable) <b>set vtp pruning 120,150</b> Vlans 120,150 eligible for pruning on this device. VTP domain nada modified. Console&gt; (enable)</pre> <p>In this example, VLANs 200–500 were made pruning ineligible using the <b>clear vtp pruning</b> command. This example shows how to make VLANs 220 to 320 pruning eligible again:</p> <pre>Console&gt; (enable) <b>clear vtp pruning 200-500</b> Vlans 1,200-500,1001-1005 will not be pruned on this device. VTP domain Company modified. Console&gt; (enable)</pre> <pre>Console&gt; (enable) <b>set vtp pruning 220-320</b> Vlans 2-199,220-320,501-1000 eligible for pruning on this device. VTP domain Company modified. Console&gt; (enable)</pre>

■ set vtp pruning

---

**Related Commands**

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