

## set tokenring priority

Use the **set tokenring priority** command to specify the highest Token Ring frame priority that will go to the low-priority transmit queue and the minimum Token Ring frame priority that is used when requesting a token.

```
set tokenring priority mod/port {threshold thresh_num | minxmit min_num}
```

Syntax Description	
<i>mod/port</i>	Number of the module and the port on the module.
<b>threshold</b> <i>thresh_num</i>	Keyword and variable to specify the priority queue threshold; valid values are from <b>0</b> to <b>7</b> .
<b>minxmit</b> <i>min_num</i>	Keyword and variable to specify the minimum frame priority to be used; valid values are from <b>0</b> to <b>6</b> .

**Defaults** The default *thresh\_num* is 3 and the default *min\_num* is 4.

**Command Types** Switch command.

**Command Modes** Privileged.

**Examples** This example shows how to set the priority threshold levels on port 2 on module 4:

```
Console> (enable) set tokenring priority 4/2 threshold 6
Port 2 priority threshold set to 6.
Console> (enable)
```

This example shows how to set the minimum priority levels on port 2 on module 4:

```
Console> (enable) set tokenring priority 4/2 minxmit 5
Port 2 priority minxmit set to 5.
Console> (enable)
```

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

# set tokenring reduction

Use the **set tokenring reduction** command to reduce broadcast storms in an externally looped network.

**set tokenring reduction {enable | disable}**

<b>Syntax Description</b>	<b>enable   disable</b> Keyword to turn broadcast reduction on ( <b>enable</b> ) or off ( <b>disable</b> ).
---------------------------	---

<b>Defaults</b>	The default configuration is enabled.
-----------------	---------------------------------------

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

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

<b>Examples</b>	The following example shows how to enable All-Routes Explorer reduction:
-----------------	--

```
Console> (enable) set tokenring reduction enable
Tokenring reduction enabled
Console> (enable)
```

The following example shows how to disable All-Routes Explorer reduction:

```
Console> (enable) set tokenring reduction disable
Tokenring reduction disabled
Console> (enable)
```

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

# set traffic monitor

Use the **set traffic monitor** command to configure the threshold at which a high traffic log will be generated.

**set traffic monitor** *threshold*

---

**Syntax Description**

*threshold*     0 to 100 percent.

---

---

**Defaults**

The default threshold is 100 percent. No high traffic log is created.

---

**Command Types**

Switch command.

---

**Command Modes**

Privileged.

---

**Usage Guidelines**

If backplane traffic exceeds the threshold configured by the **set traffic monitor** command, a high traffic log is created. If the threshold is set to 100 percent, no high-traffic system warning is generated.

---

**Examples**

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)
```

---

**Related Commands**

[show traffic](#)

# set trunk

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

```
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) Keyword to force the port to become a trunk port and persuade the neighboring port to become a trunk port. The port becomes a trunk port even if the neighbor port does not agree to become a trunk. This is the only possible mode for ATM ports.
<b>off</b>	(Optional) Keyword to force a port to become a nontrunk port and persuade the neighboring port to become a nontrunk port. The port 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.
<b>desirable</b>	(Optional) Keyword to specify a port 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) Keyword to cause the port to become a trunk port if the neighboring port tries to negotiate a trunk link. This mode is not allowed on FDDI and ATM ports. This is the default mode for Fast Ethernet and Gigabit Ethernet ports.
<b>nonegotiate</b>	(Optional) Keyword to force the port to become a trunk port but prevent it from sending DTP frames to its neighbor. This mode is only allowed on ISL and IEEE 802.1Q trunks.
<i>vlan_range</i>	(Optional) VLANs to add to the list of allowed VLANs on the trunk. The VLAN range is from <b>1</b> to <b>1005</b> .
<b>isl</b>	(Optional) Keyword to specify an ISL trunk on an Ethernet port.
<b>dot1q</b>	(Optional) Keyword to specify an IEEE 802.1Q trunk on an Ethernet port. IEEE 802.1Q trunks are supported in Catalyst 5000 family 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 <b>nonegotiate</b> mode with 802.1Q trunks.
<b>dot10</b>	(Optional) Keyword to specify an IEEE 802.10 trunk on a FDDI or CDDI port.
<b>lane</b>	(Optional) Keyword to specify an ATM LANE trunk on an ATM port.
<b>negotiate</b>	(Optional) Keyword to specify that the port become an ISL (preferred) or 802.1Q trunk, depending on the configuration and capabilities of the neighboring port.

---

**Defaults**

All ports except ATM LANE ports are nontrunk ports by default. ATM LANE and RSM ports are always configured as trunk ports.

---

**Command Types**

Switch command.

---

**Command Modes**

Privileged.

---

**Usage Guidelines**

Trunking capabilities are hardware dependent. Refer to the *Catalyst 5000 Family Module Installation Guide* to determine the trunking capabilities of your hardware, or enter the **show port capabilities** command.

The Catalyst 5000 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* for your switch 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 5000 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 5000 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** mode to force a port to become a trunk, even if it is in a different domain.

To remove VLANs from the allowed list for a trunk, enter the **clear trunk mod/port 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 remove VLANs from the allowed list, enter the **clear trunk mod/port vlan\_range** command. To later add VLANs that were removed, enter the **set trunk mod/port vlan\_range** command.

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

You cannot change the allowed VLAN range on the RSM port.

The RSM port can be configured only as an IEEE 802.1Q-type trunk.

To return a trunk to its default trunk type and mode, enter the **clear trunk mod/port** 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 a port is in trunking mode, the jumbo frame feature is automatically enabled on that port. When the port is not in trunking mode, the jumbo frame setting on that port returns to the original setting you have set. If you try to the disable jumbo frame feature on a trunk port, the port continues to pass jumbo frames until trunking is turned off.

---

**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 non-trunk 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 removed 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

Use the **set uddl** command to enable or disable the UDLD feature on specified ports or globally on all ports.

**set uddl enable** | **disable** *mod/ports*

Syntax Description	
<b>enable</b>	Keyword to enable the UDLD feature.
<b>disable</b>	Keyword to disable the UDLD feature.
<i>mod/ports</i>	Number of the module and the ports on the module.

**Defaults** The default is UDLD is globally disabled.

**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. UDLD can only be enabled on Ethernet fiber or copper interfaces.

**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 udd enable  
UDLD enabled globally  
Console> (enable)
```

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

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

---

**Related Commands**    [show udd](#)

## set uddl aggressive-mode

Use the **set uddl aggressive-mode** command to enable UDLD aggressive mode on specified ports or globally on all ports.

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

Syntax Description		
<b>enable</b>	Keyword to enable UDLD aggressive mode.	
<b>disable</b>	Keyword to disable UDLD aggressive mode.	
<i>mod/port</i>	Number of the module and the ports on the module.	

**Defaults** The default is 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 autonegotiation or FEFI 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 uddl 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 UDD 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

Use the **set udd interval** command to set the UDDL message interval timer.

```
set udd interval interval
```

---

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

---

---

<b>Defaults</b>	The default is 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  
UDLD message interval set to 90 seconds  
Console> (enable)
```

---

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

---

# set vlan

Use the **set vlan** command to group ports into a VLAN.

```
set vlan {vlan} {mod/port}
```

```
set vlan {vlan_num} [name name] [type {ethernet | fddi | fddinet | trcrf | trbrf}] [state {active
| suspend}] [said said] [mtu mtu][ring hex_ring_number ]
[decring decimal_ring_number ] [bridge bridge_num ] [parent vlan_num] [mode {srt |
srb}] [stp {ieec | ibm | auto}] [translation vlan_num] [backupcrf {off | on}]
[aremaxhop hopcount] [stemaxhop hopcount] [rspan]
```

## Syntax Description

<i>vlan_num</i>	Number identifying the VLAN.
<i>mod</i>	Number of the module. This parameter is not valid when defining or configuring TrBRFs.
<i>port</i>	Numbers of the port on the module belonging to the VLAN; this parameter does not apply to TrBRFs.
<b>name</b> <i>name</i>	(Optional) Keyword to define a text string used as the name of the VLAN (1 to 32 characters).
<b>type</b> { <b>ethernet</b>   <b>fddi</b>   <b>fddinet</b>   <b>trcrf</b>   <b>trbrf</b> }	(Optional) Keywords to identify the VLAN type.
<b>state</b> { <b>active</b>   <b>suspend</b> }	(Optional) Keyword to specify whether the state of the VLAN is active or suspended. VLANs in suspended state do not pass packets.
<b>said</b> <i>said</i>	(Optional) Keyword to specify the security association identifier. Valid values are from <b>1</b> to <b>4294967294</b> ; this parameter does not apply to TrCRFs or TrBRFs.
<b>mtu</b> <i>mtu</i>	(Optional) Keyword to specify the maximum transmission unit (packet size, in bytes) that the VLAN can use. Possible values are <b>576</b> to <b>18190</b> .
<b>ring</b> <i>hex_ring_number</i>	(Optional) Keyword to specify the logical ring number for Token Ring VLANs. Possible values are hexadecimal numbers 0x1 to 0xFFF; this parameter is valid and required only when defining a TrCRF.
<b>decring</b> <i>decimal_ring_number</i>	(Optional) Keyword to specify the logical ring number for Token Ring VLANs. Possible values are decimal numbers <b>1</b> to <b>4095</b> ; this parameter is valid and required only when defining a TrCRF.
<b>bridge</b> <i>bridge_num</i>	(Optional) Keyword to specify the identification number of the bridge. Possible values are hexadecimal numbers 0x1 to 0xF. For Token Ring VLANs, the default is 0F. This parameter is not valid for TrCRFs.
<b>parent</b> <i>vlan_num</i>	(Optional) Keyword to set a parent VLAN. The range for <i>vlan_num</i> is <b>2</b> to <b>1005</b> . This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF.

<b>mode</b> {srt   srb}	(Optional) TrCRF bridging mode.
<b>stp</b> {ieee   ibm   auto}	(Optional) Keyword to specify the Spanning Tree Protocol version for a TrBRF to use, source routing transparent ( <b>ieee</b> ), source route bridging ( <b>ibm</b> ), automatic source selection ( <b>auto</b> ).
<b>translation</b> <i>vlan_num</i>	(Optional) Keyword to specify a translational VLAN used to translate FDDI to Ethernet; valid values are from <b>1</b> to <b>1005</b> . This parameter is not valid for defining or configuring Token Ring VLANs.
<b>backupcrf</b> {off   on}	(Optional) Keyword to specify whether the TrCRF is a backup path for traffic.
<b>aremaxhop</b> <i>hop_count</i>	(Optional) Keyword to specify the maximum number of hops for All-Routes Explorer frames. Possible values are <b>1</b> to <b>14</b> . This parameter is only valid when defining or configuring TrCRFs.
<b>stemaxhop</b> <i>hop_count</i>	(Optional) Keyword to specify the maximum number of hops for Spanning-Tree Explorer frames. Possible values are <b>1</b> to <b>14</b> . This parameter is only valid when defining or configuring TrCRFs.

### Defaults

The default configuration has all switched Ethernet ports and Ethernet repeater ports in VLAN 1. The default SAID is 100001 for VLAN 1, 100002 for VLAN 2, 100003 for VLAN 3, and so on. The default type is Ethernet. The default MTU is 1500 bytes. The default state is active.

The default TrBRF is 1005, the default TrCRF is 1003, and the default MTU for TrBRFs and TrCRFs is 4472. The default state is active. The default **aremaxhop** value is 7; the default **stemaxhop** value is 7.

### Command Types

Switch command.

### Command Modes

Privileged.

### Usage Guidelines

VLAN 1 parameters are factory configured and cannot be changed.

You cannot use the **set vlan** command until the Catalyst 5000 family switch is either in VTP transparent mode (**set vtp mode**) or until a VTP domain name has been set (**set vtp**).

Valid MTU values for Token Ring VLAN are 1500 or 4472. While you can enter any value for the MTU value, the value you enter defaults to the next lowest valid value.

You cannot set multiple VLANs for ISL ports using this command. The VLAN name can be from 1 to 32 characters in length. If adding a new VLAN, the VLAN number must be within the range 2 to 1001. When modifying a VLAN, the valid range for the VLAN number is 2 to 1005.

On a new Token Ring VLAN, if you do not specify the parent parameter for a TrCRF, the default TrBRF (1005) is used.

---

**Examples**

This example shows how to set VLAN 850 to include ports 4 through 7 on module 3, because ports 4 through 7 were originally assigned to TrCRF 1003, the message reflects the modification of VLAN 1003:

```
Console> (enable) set vlan 850 3/4-7
VLAN 850 modified.
VLAN 1003 modified.
VLAN Mod/Ports
-----
850 3/4-7
Console> (enable)
```

---

**Related Commands**

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

# set vlan mapping

Use the **set vlan mapping** command to map 802.1Q VLANs to ISL VLANs.

```
set vlan mapping dot1q lq_vlan_num isl isl_vlan_num
```

Syntax Description	dot1q	Keyword to specify the 802.1Q VLAN.
	<i>lq_vlan_num</i>	Number identifying the 802.1Q VLAN; valid values are from <b>1001</b> to <b>4095</b> .
	isl	Keyword to specify the ISL VLAN.
	<i>isl_vlan_num</i>	Number identifying the ISL VLAN; valid values are from <b>1</b> to <b>1000</b> .

**Defaults** The default is no 802.1Q-to-ISL mappings are defined.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** IEEE 802.1Q VLAN trunks support VLANs 1 through 4095. ISL VLAN trunks support VLANs 1 through 1000. The switch automatically maps 802.1Q VLANs 1000 and lower to ISL VLANs with the same number.

The native VLAN of the 802.1Q trunk cannot be used in the mapping.

Use this feature to map 802.1Q VLANs above 1000 to ISL VLANs. Note that if you map a 802.1Q VLAN over 1000 to an ISL VLAN, the corresponding 802.1Q VLAN will be blocked. For example, if you map 802.1Q VLAN 2000 to ISL VLAN 200, then 802.1Q VLAN 200 will be blocked.

You can map up to seven VLANs. 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 is in the mapping table, the command is aborted. You must first clear that mapping.

If *vlan\_num* 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.

---

**Examples**

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

```
Console> (enable) set vlan mapping dot1q 1022 isl 850
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 1017 isl 999
Vlan mapping successful
Warning: vlan 999 non-existent
Vlan 999 configuration successful
Console> (enable)
```

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

```
Console> (enable) set vlan mapping dot1q 1033 isl 722
722 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 1099 isl 917
Vlan Mapping Table Full.
Console> (enable)
```

---

**Related Commands**

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

# set vmpls downloadmethod

Use the **set vmpls downloadmethod** command to specify whether to use TFTP or rcp to download the VMPS database.

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

Syntax Description	rcp	Keyword to specify rcp as the method for downloading the VMPS database.
	tftp	Keyword to specify TFTP as the method for downloading the VMPS database.
	username	(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 TFTP is specified as the download method.

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

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

**Related Commands**

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

# set vmps downloadserver

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

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

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

**Defaults** If a 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 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 vmps](#)
- [set vmps state](#)
- [show vmps](#)

## set vmpls server

Use the **set vmpls server** command set to configure the VMPS server.

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

```
set vmpls server retry count
```

```
set vmpls server reconfirminterval interval
```

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

**Defaults** If no IP address is specified, 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 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 vmpls server 192.168.10.140 primary
192.168.10.140 added to VMPS table as primary domain server.
Console> (enable)
```

**set vmps server**

This example shows how to define a VMPS server:

```
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**    [show vmps](#)

# set vmps state

Use the **set vmps state** command to enable or disable VMPS.

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

Syntax Description	enable	Keyword to enable VMPS.
	disable	Keyword to disable 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 tftpserver** command to specify the IP address of the server from which the VMPS database is downloaded.

**Examples** This example shows how to enable VMPS:

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

# set vtp

Use the **set vtp** command to set the options for VTP.

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

Syntax Description		
<b>domain</b> <i>domain_name</i>	(Optional) Keywords to define the name that identifies the VLAN management domain.	
<b>mode</b>	(Optional) Keyword to specify the VTP mode.	
<b>client</b>	(Optional) Keyword to specify VTP client mode.	
<b>server</b>	(Optional) Keyword to specify VTP server mode.	
<b>transparent</b>	(Optional) Keyword to specify VTP transparent mode.	
<b>passwd</b> <i>passwd</i>	(Optional) Keyword to define the VLAN trunk protocol password. The VTP password can be 8 to 64 characters in length.	
<b>pruning enable   disable</b>	(Optional) Keywords to specify to enable or disable VTP pruning for the entire management domain.	
<b>v2</b>	(Optional) Keyword to set version 2 mode.	
<b>enable</b>	(Optional) Keyword to enable v2.	
<b>disable</b>	(Optional) Keyword to disable v2.	

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

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** All switches in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on switches in the same VTP domain. VTP version 2 is supported in software release 3.1(1) and later and is disabled by default.

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.

The *domain\_name* can be 1 to 32 characters in length.

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

VTP supports three different modes: server, client, and transparent. 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.

If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, 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.

If you assign a VTP password, no VTP or VLAN configuration changes can be made without first entering the password.

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 pruning** commands to specify which VLANs should or should not be pruned when pruning is enabled for the domain.

To disable VTP, enter the **set vtp mode transparent** command. This disables VTP from the domain but does not remove the domain from the switch. Use the **clear config all** command to remove the domain from the switch.

**Caution**

---

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

---

**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)
```

**Related Commands**

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

# set vtp pruneeligible

Use the **set vtp pruneeligible** command to specify which VLANs in the VTP domain are eligible for pruning.

**set vtp pruneeligible** *vlan*s

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

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

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

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

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

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

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

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

```
Console> (enable) clear vtp pruneeligible 200-500
Vlans 1,200-500,1001-1005 will not be pruned on this device.
VTP domain Company modified.
Console> (enable)
Console> (enable) set vtp pruneeligible 220-320
Vlans 2-199,220-320,501-1000 eligible for pruning on this device.
VTP domain Company modified.
Console> (enable)
```

**Related Commands**

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

# show accounting

Use the **show accounting** command to display accounting setup and configuration information on the switch.

## show accounting

**Syntax Description** This command has no arguments or keywords.

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

**Command Types** Switch command.

**Command Modes** Privileged.

**Examples** This example shows the configuration details of a switch with RADIUS accounting enabled:

```

Console> show accounting
Event      Method1 Mode
-----
exec:      tacacs+ start-stop
connect:   radius  stop-only
system:    tacacs+ stop-only
commands:
config:    tacacs+ stop-only
all:       -      -

TACACS+ Suppress for no username: disabled
Update Frequency: newinfo

Accounting information:
-----

Active Accounted actions on tty21680592841, User NULL Priv 15
  Task ID 3, EXEC Accounting record, 0,00:00:22 Elapsed
  task_id=3 start_time=934463479 timezone=UTC service=shell
Active Accounted actions on tty01, User kannank Priv 15
  Task ID 2, EXEC Accounting record, 0,00:01:23 Elapsed
  task_id=2 start_time=934463418 timezone=UTC service=shell
Active Accounted actions on tty21680592841, User danny Priv 15
  Task ID 4, Connection Accounting record, 0,00:00:07 Elapsed
  task_id=4 start_time=934463495 timezone=UTC service=connection protocol=telnet
  addr=-1407968771 cmd=telnet 172.20.25.253

Overall Accounting Traffic:
      Starts  Stops  Active
Exec      1      0      2
Connect   0      0      1
Command   0      0      0
System    0      0      0
Console>

```

This example shows the configuration details of a switch with TACACS+ accounting enabled:

```

Console> show accounting
Tacacs key:
Tacacs login attempts: 3
Tacacs timeout: 5 seconds
Tacacs direct request: disabled

Tacacs-Server                Status
-----
171.69.1.2                    primary
171.69.1.3

TACACS+ Suppress for no username: disabled
Update Frequency: newinfo

Accounting information:
-----

Active Accounted actions on tty21680592841, User NULL Priv 15
Task ID 3, EXEC Accounting record, 0,00:00:22 Elapsed
task_id=3 start_time=934463479 timezone=UTC service=shell

Active Accounted actions on tty01, User kannank Priv 15
Task ID 2, EXEC Accounting record, 0,00:01:23 Elapsed
task_id=2 start_time=934463418 timezone=UTC service=shell

Active Accounted actions on tty21680592841, User danny Priv 15
Task ID 4, Connection Accounting record, 0,00:00:07 Elapsed
task_id=4 start_time=934463495 timezone=UTC service=connection protocol=telnet
addr=-1407968771 cmd=telnet 172.20.25.253

Overall Accounting Traffic:
      Starts  Stops  Active
Exec      1      0       2
Connect   0      0       1
Command   0      0       0
System    0      0       0

Console>

```

### Related Commands

- [set accounting commands](#)
- [set accounting connect](#)
- [set accounting exec](#)
- [set accounting suppress](#)
- [set accounting system](#)
- [set accounting update](#)

# show alias

Use the **show alias** command to display a list of defined command aliases.

```
show alias [name]
```

<b>Syntax Description</b>	<i>name</i> (Optional) Name of the alias to be displayed. If <i>name</i> is not specified, all defined aliases are displayed.
---------------------------	---

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

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

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

<b>Examples</b>	This example shows how to display all aliases:
-----------------	--

```
Console> show alias
shint          show interface
cc            clear config
shf           show flash
sip           show ip route
Console>
```

<b>Related Commands</b>	<a href="#">clear kerberos clients mandatory session</a> <a href="#">set alias</a>
-------------------------	---