

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_num/port_num { threshold thresh_num | minxmit min_num }
```

Syntax Description	
<i>mod_num</i>	Number of the module.
<i>port_num</i>	Number of the port on the module.
threshold	Keyword that specifies the priority queue threshold.
<i>thresh_num</i>	Valid values are 0 to 7; the default is 3.
minxmit	Keyword that specifies the minimum frame priority to be used.
<i>min_num</i>	Valid values are 0 to 6; the default is 4.

Defaults The default configuration for **threshold** is 3. The default configuration for **minxmit** is 4.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is supported by the Catalyst 5000 family switches.

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 }
```

Syntax Description	enable disable Keyword that specifies to turn broadcast reduction on (enable) or off (disable).
---------------------------	---

Defaults	The default configuration is enabled.
-----------------	---------------------------------------

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

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

Usage Guidelines	This command is supported by the Catalyst 5000 family switches.
-------------------------	---

Examples	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)
```

Related Commands	show tokenring
-------------------------	-----------------------

set trace

Use the **set trace** command to obtain the debug information for the switch web interface.

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

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

Syntax Description	<i>category</i> Trace category.
	<i>level</i> (Optional) Trace level; see the “Usage Guidelines” for valid values.
monitor	Keyword that specifies monitoring for debug information for the switch web interface.
enable	Keyword that enables the trace monitor.
disable	Keyword that disables the trace monitor.

Defaults The default trace level is 1.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines Valid values for the trace level are from 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 debug information:

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

Related Commands **show trace**

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_num/port_num [on | off | desirable | auto | nonegotiate] [vlan_range] [isl | dot1q | dot10 | lane | negotiate]
```

Syntax Description

<i>mod_num</i>	Number of the module.
<i>port_num</i>	Number of the port on the module.
on	(Optional) Keyword that specifies 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.
off	(Optional) Keyword that specifies 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.
desirable	(Optional) Keyword that specifies a port negotiate actively with the neighbor port to become a trunk link. This mode is not allowed on FDDI and ATM ports.
auto	(Optional) Keyword that specifies 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.
nonegotiate	(Optional) Keyword that specifies 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 1 to 1005.
isl	(Optional) Keyword that specifies an ISL trunk on an Ethernet port.
dot1q	(Optional) Keyword that specifies an IEEE 802.1Q trunk on an Ethernet port. 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 mode with 802.1Q trunks.
dot10	(Optional) Keyword that specifies an IEEE 802.10 trunk on a FDDI or CDDI port.
lane	(Optional) Keyword that specifies an ATM LANE trunk on an ATM port.
negotiate	(Optional) Keyword that specifies 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	<p>The Catalyst 2948G and 2980G switches are fixed configuration switches. Ports are located on module 2 for the 2948G and on modules 2 and 3 for the 2980G; for this reason, if you enter 1/N for the module/port number, an error message is displayed.</p> <p>Trunking capabilities are hardware dependent. Refer to the <i>Module Installation Guide</i> for your switch to determine the trunking capabilities of your hardware, or enter the show port capabilities command.</p> <p>The Catalyst 5000 family, 4000 family, 2926G series, 2948G, and 2980G 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 <i>Software Configuration Guide</i> for your switch for detailed information on how trunk ports are negotiated.</p> <p>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, 4000 family, 2926G series, 2948G, and 2980G 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, 4000 family, 2926G series, 2948G, and 2980G software release 2.4(3) and later.</p> <p>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.</p> <p>To remove 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 <i>all</i> VLANs to the allowed VLAN list for the trunk, even if you specify a VLAN range (the specified VLAN range is ignored).</p> <p>To remove VLANs from the allowed list, enter the clear trunk mod_num/port_num vlan_range command. To later add VLANs that were removed, enter the set trunk mod_num/port_num vlan_range command.</p> <p>If you do not enter a trunk-type keyword, the value is unchanged from the previous configuration.</p> <p>You cannot change the allowed VLAN range on the RSM port.</p> <p>The RSM port can be configured only as an IEEE 802.1Q-type trunk.</p> <p>The dot1q trunk type is the only trunk type supported by the Catalyst 4000 family and 2948G switches.</p> <p>To return a trunk to its default trunk type and mode, enter the clear trunk mod_num/port_num command.</p> <p>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.”</p>

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 udld

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

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

Syntax Description

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

Defaults

The defaults are as follows:

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

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

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

If you enter the global **set udld 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 udld 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 udd 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 udd aggressive-mode

Use the **set udd aggressive-mode** command to enable UDLD aggressive mode on specified ports.

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

Syntax Description	enable	Keyword that enables UDLD aggressive mode.
	disable	Keyword that disables UDLD aggressive mode.
	mod/port	Number of the module and ports.

Defaults The default is aggressive mode is disabled.

Command Types Switch command.

Command Modes Privileged.

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

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

Examples This example shows how to enable aggressive mode:

```
Console> (enable) set udd aggressive-mode enable 2/1
Aggressive UDLD enabled on port 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

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

set udd interval *interval*

Syntax Description	<i>interval</i> Message interval in seconds; valid values are from 7 to 90 seconds.
Defaults	The default is 15 seconds.
Command Types	Switch command.
Command Modes	Privileged.
Examples	This example shows how to set the message interval timer: <pre>Console> (enable) set udd interval 90 UDLD message interval set to 90 seconds Console> (enable)</pre>
Related Commands	show udd

set vlan

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

```
set vlan vlan_num mod_num/port_list
```

```
set vlan vlan_num [name name] [type {ethernet | fdi | fdinet | 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 {ieee | ibm | auto}] [translation vlan_num] [backupcrf {off | on}]
  [aremaxhop hop_count] [stemaxhop hop_count]
```

Syntax Description

<i>vlan_num</i>	Number identifying the VLAN.
<i>mod_num</i>	Number of the module. This parameter is not valid when defining or configuring TrBRFs.
<i>port_list</i>	Numbers of the port on the module belonging to the VLAN. This parameter does not apply to TrBRFs.
name <i>name</i>	(Optional) Keyword that specifies to define a text string used as the name of the VLAN (1 to 32 characters).
type { ethernet fdi fdinet trcrf trbrf }	(Optional) Keywords that identify the VLAN type.
state { active suspend }	(Optional) Keyword that specifies whether the state of the VLAN is active or suspended. VLANs in suspended state do not pass packets; the default is active.
said <i>said</i>	(Optional) Keyword that specifies the security association identifier. Possible values are 1 to 4294967294. This parameter does not apply to TrCRFs or TrBRFs.
mtu <i>mtu</i>	(Optional) Keyword that specifies the maximum transmission unit (packet size, in bytes) that the VLAN can use. Possible values are 576 to 18190.
ring <i>hex_ring_number</i>	(Optional) Keyword that specifies the logical ring number for Token Ring VLANs. Possible values are hexadecimal numbers 0x1 to 0xFFF. For Token Ring VLANs, this parameter is valid and required only when defining a TrCRF.
decring <i>decimal_ring_number</i>	(Optional) Keyword that specifies the logical ring number for Token Ring VLANs. Possible values are decimal numbers 1 to 4095. For Token Ring VLANs, this parameter is valid and required only when defining a TrCRF.
bridge <i>bridge_num</i>	(Optional) Keyword that specifies 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.
parent <i>vlan_num</i>	(Optional) Keyword that specifies to set a parent VLAN. The range for <i>vlan_num</i> is 2 to 1005. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF.
mode { srt srb }	(Optional) TrCRF bridging mode. Valid values for this parameter are srt and srb .
stp { ieee ibm auto }	(Optional) Keyword that specifies the version of the Spanning-Tree Protocol for a TrBRF to use, source routing transparent (ieee), source route bridging (ibm), automatic source selection (auto).

translation <i>vlan_num</i>	(Optional) Keyword that specifies a translational VLAN used to translate FDDI to Ethernet. Possible values are 1 to 1005. This parameter is not valid for defining or configuring Token Ring VLANs.
backuprf { off on }	(Optional) Keyword that specifies whether the TrCRF is a backup path for traffic.
aremaxhop <i>hop_count</i>	(Optional) Keyword that specifies the maximum number of hops for All-Routes Explorer frames. Possible values are 1 to 14. This parameter is only valid when defining or configuring TrCRFs.
stemaxhop <i>hop_count</i>	(Optional) Keyword that specifies the maximum number of hops for Spanning-Tree Explorer frames. Possible values are 1 to 14. 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** is 7; the default **stemaxhop** is 7.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You cannot use the **set vlan** command until the Catalyst 5000 family, 4000 family, and 2926G series switches are 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.

The Catalyst 4000 family, 2948G, and 2980G switches are Ethernet-only devices.

The Catalyst 2948G and 2980G switches are fixed configuration switches. Ports are located on module 2 for the 2948G and on modules 2 and 3 for the 2980G; for this reason, if you enter **1/N** for the module/port number, an error message is displayed.

Examples

This example shows how to set VLAN 850 to include ports 4 through 7 on module 3. Ports 4 through 7 were originally assigned to TrCRF 1003, therefore, 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

show vlan
clear vlan

set vlan mapping

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

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

Syntax Description	dot1q	Keyword that specifies the 802.1Q VLAN.
	<i>1q_vlan_num</i>	Number identifying the 802.1Q VLAN; valid values are 1001 to 4095.
	isl	Keyword that specifies the ISL VLAN.
	<i>isl_vlan_num</i>	Number identifying the ISL VLAN; valid values are 1 to 1000.

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.

Catalyst 4000 family, 2948G, and 2980G switches only support 802.1Q trunks. You can map up to seven VLAN indexes greater than 1000 to ISL VLANs.

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

show vlan
clear vlan mapping

set vmps downloadmethod

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

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

Syntax Description		
	rcp	Keyword that specifies rcp as the method for downloading the VMPS database.
	tftp	Keyword that specifies TFTP as the method for downloading the VMPS database.
	<i>username</i>	(Optional) Specifies a username for downloading with rcp.

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

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is supported by the Catalyst 5000 family switches and the Catalyst 2926G series switches.

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

Related Commands

```
set rcp username
show vmps
download vmps
```

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

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is supported by the Catalyst 5000 family switches and the Catalyst 2926G series switches.

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

```
set vmps state
show vmps
download vmps
```

set vmips server

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

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.
	primary	(Optional) Keyword to specify the device as the primary VMPS server.
	retry <i>count</i>	Keyword and variable to specify the retry interval; valid values are from 1 to 10 minutes.
	reconfirminterval <i>interval</i>	Keyword and variable to specify the reconfirmation interval; valid values are from 0 to 120 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 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 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 vmmps state

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

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

Syntax Description	enable	disable
	Keyword that specifies to enable VMPS.	Keyword that specifies to disable VMPS.

Defaults By default, VMPS is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines This command is supported by the Catalyst 5000 family switches and the Catalyst 2926G series switches.

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

This example shows how to disable VMPS:

```
Console> (enable) set vmmps 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 **show vmmps**
download vmmps

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	
domain <i>domain_name</i>	(Optional) Keywords that specifies to define the name that identifies the VLAN management domain. The <i>domain_name</i> can be 1 to 32 characters in length.
mode	(Optional) Keyword that specifies the VTP mode.
client	(Optional) Keyword that specifies VTP client mode.
server	(Optional) Keyword that specifies VTP server mode.
transparent	(Optional) Keyword that specifies VTP transparent mode.
passwd <i>passwd</i>	(Optional) Keyword that specifies to define the VLAN trunk protocol password. The VTP password can be 8 to 64 characters in length.
pruning enable disable	(Optional) Keywords that specify to enable or disable VTP pruning for the entire management domain.
v2	(Optional) Keyword that specifies to set version 2 mode.
enable	(Optional) Keyword that specifies to enable v2.
disable	(Optional) Keyword that specifies 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.

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 pruneeligible** 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

```
show vtp domain
set vlan
clear vlan
show vlan
set vtp pruneeligible
clear vtp pruneeligible
```

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

Syntax Description

*vlan*s Range of VLAN numbers; valid values are 2 to 1000.

Defaults

By default, VLANs 2 through 1000 are eligible for pruning.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

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

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

If VLANs have been made pruning ineligible, use the **set vtp pruneeligible** command to make them pruning eligible again.

Examples

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

```
Console> (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 pruneeligible** 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)
```

■ `set vtp pruneeligible`

Related Commands

`show vtp domain`
`set vlan`
`clear vtp pruneeligible`

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 setting.

Command Types Switch command.

Command Modes Privileged.

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

```

Console> (enable) 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> (enable)

```

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

```

Console> (enable) 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> (enable)

```

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]
```

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

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

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

Command Modes	Normal.
----------------------	---------

Examples	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>
```

Related Commands	clear kerberos clients mandatory session set alias
-------------------------	---

show arp

Use the **show arp** command to display the ARP table.

```
show arp [ip_addr | hostname] [noalias]
```

Syntax Description	
<i>ip_addr</i>	(Optional) Number of the IP address.
<i>hostname</i>	(Optional) Name of the host.
noalias	(Optional) Keyword that specifies to force the display to show only IP addresses, not IP aliases.

Defaults This command has no default setting.

Command Types Switch command.

Command Modes Normal.

Usage Guidelines The ARP Aging time display in the output is the period of time that indicates when an ARP entry is removed from the ARP table. Set this value by entering the **set arp agingtime** command. The remaining lines of the display show the mappings of IP addresses (or IP aliases) to MAC addresses.

Use the *ip_addr* or the *hostname* options to specify a specific IP host when the ARP cache is large.

Examples This example shows how to display the ARP table:

```
Console> (enable) show arp
ARP Aging time = 300 sec
+ - Permanent Arp Entries
* - Static Arp Entries
* 2.2.2.2                at 00-08-cc-44-aa-18 on vlan 5
+ 1.1.1.1                at 00-08-94-cc-02-aa on vlan 5
142.10.52.195           at 00-10-07-3c-05-13 port 7/1-4 on vlan 5
121.23.79.121           at 00-00-1c-03-00-40 port 7/1-4 on vlan 5
Console> (enable)
```

Related Commands **clear arp**
set arp