

# set enablepass

Use the **set enablepass** command to change the privileged (enable) mode password on the switch.

**set enablepass**

---

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

---

**Defaults** The default configuration has no enable password configured.

---

**Command Types** Switch command.

---

**Command Modes** Privileged.

---

**Usage Guidelines** Passwords are case sensitive and may be 0—30 characters in length, including spaces. The command prompts you for the old password. If the password you enter is valid, you are prompted to enter a new password and to verify the new password.

---

**Examples** This example shows how to establish a new password:

```
Console> (enable) set enablepass
Enter old password: <old_password>
Enter new password: <new_password>
Retype new password: <new_password>
Password changed.
Console> (enable)
```

---

**Related Commands** **enable**  
**set password**

# set errordetection

Use the **set errordetection** command set to enable or disable various error detections.

```
set errordetection inband {enable | disable}
```

```
set errordetection memory {enable | disable}
```

Syntax Description	enable	Keyword to enable the specified error detection.
	disable	Keyword to disable the specified error detection.
	inband	Keyword to specify inband error detection.
	memory	Keyword to specify memory error detection.

**Defaults** The default is portcounters error detection is enabled and memory and inband error detection is disabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** The **inband** keyword is not supported.

**Examples** This example shows how to enable memory error detection.

```
Console> (enable) set errordetection memory enable
Memory error detection enabled.
Console> (enable)
```

# set feature fw-disable

Use the **set feature fw-disable** command to enable a feature that disables ports showing enough FCS and alignment errors to indicate a duplex mismatch.

```
set feature fw-disable {enable | disable}
```

---

**Syntax Description**

<b>enable</b>	Keyword to disable the feature.
<b>disable</b>	Keyword to disable the feature.

---

---

**Defaults**

The default is disabled.

---

**Command Types**

Switch command.

---

**Command Modes**

Privileged.

---

**Usage Guidelines**

If there is a duplex mismatch on an ISL trunk into a cat5000 switch, swBusCRCErrorDrop errors will be seen on all ports of the switch. The port with the mismatch will also see RxInnerCRCErrorDrop errors. If this mismatch is allowed to continue, then traffic between buses might be dropped.

Enter the **set feature fw-disable enable** command to disable the ports with the duplex mismatch.

For additional information, refer to the “Open and Resolved Caveats for Software Release 5.5(13)” section in the *Release Notes for Catalyst 5000 Family Software Release 5.x* publication and the DDTs release note entry for CSCdw11398.

---

**Examples**

This example shows how to turn on the feature to disable the port with the duplex mismatch:

```
Console> (enable) set feature fw-disable enable
no ISL entry feature enabled.
Console> (enable)
```

## set feature mdg

Use the **set feature** command to enable the Multiple Default Gateway (MDG) feature.

```
set feature mdg { enable | disable }
```

### Syntax Description

<b>enable</b>	Keyword that enables multiple default gateway feature on the switch.
<b>disable</b>	Keyword that disables multiple default gateway feature on the switch.

### Defaults

The default is MDG is enabled.

### Command Types

Switch command.

### Command Modes

Privileged.

### Usage Guidelines

If the MDG feature is enabled, the switch will ping its default gateways every ten seconds to verify that they are available.

### Examples

This example shows how to enable the MDG feature:

```
Console> (enable) set feature mdg enable
Multiple Default Gateway feature enabled.
Console> (enable)
```

This example shows how to disable the MDG feature:

```
Console> (enable) set feature mdg disable
Multiple Default Gateway feature disabled.
Console> (enable)
```

# set feature no-isl-entries

Use the **set feature no-isl-entries** command to enable installation of ISL system entries into the CAM table.

**set feature no-isl-entries {enable | disable}**

Syntax Description	enable	disable
	Keyword that prevents installation of ISL system entries in the CAM table.	Keyword that allows installation of ISL system entries in the CAM table.

**Defaults** The default is disabled; ISL system entries are installed.

**Command Types** Switch command.

**Command Modes** Privileged.

## Usage Guidelines



### Caution

Use caution when implementing the **set feature no-isl-entries** command. This command should only be used on stub switches that do not have any switches connected to it. This would ensure that the packets will not get flooded further down.

This feature is recommended only for DSL-type application service providers, where MAC addresses learned through ATM are not programmed in the CAM table.

For additional information, refer to the “Open and Resolved Caveats for Software Release 5.5(13)” section in the *Release Notes for Catalyst 5000 Family Software Release 5.x* publication and the DDTS release note entry for CSCdw86312.

**Examples** This example shows how to allow ISL system entries to be installed in the CAM table:

```
Console> (enable) set feature no-isl-entries enable
no ISL entry feature enabled.
Console> (enable)
```

## set fddi alarm

Use the **set fddi alarm** command to specify the LER-alarm value for an FDDI port. The value defines the rate at which the LER threshold is exceeded on a link. The LER-alarm value affects the results of the LER threshold test.

**set fddi alarm** *mod\_num/port\_num value*

Syntax Description	
<i>mod_num</i>	Number of the module.
<i>port_num</i>	Number of the port.
<i>value</i>	Value for the LER-alarm parameter. This exponential value represents the number of link errors per second (that is, $10^{-\text{value}}$ link errors per second). Valid values are between 7 and 15.

**Defaults** The default LER-alarm value is 8 milliseconds ( $10^{-8}$  seconds).

**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 change the LER-alarm value to  $10^{-11}$  seconds for port 1 on module 4:

```
Console> (enable) set fddi alarm 4/1 11
Port 4/1 alarm value set to 11.
Console> (enable)
```

**Related Commands**

- set fddi cutoff**
- set fddi tlmn**
- set fddi tnotify**
- set fddi treq**
- set fddi userdata**
- show fddi**

# set fddi cutoff

Use the **set fddi cutoff** command to specify the LER-cutoff value for an FDDI port. The LER-cutoff value determines the LER at which a connection is flagged as faulty. The LER-cutoff value affects the results of the LER threshold test.

**set fddi cutoff** *mod\_num/port\_num value*

Syntax Description	
<i>mod_num</i>	Number of the module.
<i>port_num</i>	Number of the port.
<i>value</i>	Exponential value for the LER-cutoff parameter (that is, $10^{-\text{value}}$ link errors per second). Valid values are between 7 and 15.

**Defaults** The default LER-cutoff value is 7 milliseconds ( $10^{-7}$  seconds).

**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 change the LER-cutoff value to  $10^{-10}$  seconds for port 1 on module 4:

```
Console> (enable) set fddi cutoff 4/1 10
Port 4/1 cutoff value set to 10.
Console> (enable)
```

**Related Commands**

- set fddi alarm
- set fddi tmin
- set fddi tnotify
- set fddi treq
- set fddi userdata
- show fddi

# set fddi tlmin

Use the **set fddi tlmin** command to change the TL\_MIN value for an FDDI port.

```
set fddi tlmin mod_num/port_num microseconds
```

## Syntax Description

<i>mod_num</i>	Number of the module.
<i>port_num</i>	Number of the port.
<i>microseconds</i>	Number of microseconds for the TL_MIN parameter.

## Defaults

The default value for TL\_MIN is 40 microseconds.

## Command Types

Switch command.

## Command Modes

Privileged.

## Usage Guidelines

This command is supported by the Catalyst 5000 family switches.

The TL\_MIN value specifies the minimum time to transmit a PHY line state before advancing to the next PCM state. This setting affects the station and switch interoperability and might affect the implementation of FDDI repeaters.

## Examples

This example shows how to change the TL\_MIN value to 80 microseconds for port 1 on module 4:

```
Console> (enable) set fddi tlmin 4/1 80
Port 4/1 tlmin set to 80 usec.
Console> (enable)
```

## Related Commands

```
set fddi alarm
set fddi cutoff
set fddi tnotify
set fddi treq
set fddi userdata
show fddi
```

# set fddi tnotify

Use the **set fddi tnotify** command to change the TNotify timer value for an FDDI module.

```
set fddi tnotify mod_num time
```

Syntax Description	
<i>mod_num</i>	Number of the module.
<i>time</i>	Number of seconds for the TNotify timer. Valid times are from 2 to 30 seconds.

**Defaults** The default value for the TNotify timer is 30 seconds.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** This command is supported by the Catalyst 5000 family switches. The TNotify parameter sets the interval (in seconds) between neighbor notification frames. These frames advertise FDDI module MAC addresses to neighboring devices. Usually, the default setting is sufficient.

**Examples** This example shows how to change the TNotify timer value to 16 seconds for module 4:

```
Console> (enable) set fddi tnotify 4 16
Module 4 SMT T-Notify set to 16 sec.
Console> (enable)
```

**Related Commands**

- set fddi alarm
- set fddi cutoff
- set fddi tmin
- set fddi treq
- set fddi userdata
- show fddi

# set fddi treq

Use the **set fddi treq** command to change the TRequest value for an FDDI module.

```
set fddi treq mod_num time
```

Syntax Description	<i>mod_num</i>	Number of the module.
	<i>time</i>	Number of microseconds for the TRequest value. Valid times are from 2502 to 165,000 microseconds.

**Defaults** The default value for the TRequest is 165,000 microseconds.

**Command Types** Switch command.

**Command Modes** Privileged.

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

The TRequest parameter specifies the default TRT value for the FDDI module. This value is used when negotiating the TRT with other stations. The TRT is used to control ring scheduling during normal operation and to detect and recover from serious ring error situations. Whenever the TRT expires, the station uses the TRequest value to negotiate with other stations for the lowest value. The default setting of 165,000 microseconds is sufficient for most networks.

**Examples** This example shows how to change the TRequest value to 3500 microseconds for module 4:

```
Console> (enable) set fddi treq 4 3500
Mac 4/1 T-request set to 3500 usec.
Console> (enable)
```

**Related Commands**

- set fddi alarm
- set fddi cutoff
- set fddi tmin
- set fddi tnotify
- set fddi userdata
- show fddi

## set fddi userdata

Use the **set fddi userdata** command to configure the user-data string in the SMT MIB of an FDDI module.

```
set fddi userdata mod_num [userdata_string]
```

### Syntax Description

<i>mod_num</i>	Number of the module.
<i>userdata_string</i>	(Optional) Unique character string that identifies the node.

### Defaults

The default value for the FDDI user-data string is “Catalyst 5000.”

### Command Types

Switch command.

### Command Modes

Privileged.

### Usage Guidelines

This command is supported by the Catalyst 5000 family switches.

The user-data string identifies the FDDI module or the Catalyst 5000 family or 2926G series switch when you use a management tool to configure and maintain an internetwork or when you access the FDDI module remotely. The *userdata\_string* might be a term identifying the network node or the users connected to the network node.

### Examples

This example shows how to change the user-data string to Engineering for module 4:

```
Console> (enable) set fddi userdata 4 Engineering
Module 4 SMT User Data set to Engineering.
Console> (enable)
```

### Related Commands

```
set fddi alarm
set fddi cutoff
set fddi tmin
set fddi tnotify
set fddi treq
show fddi
```

## set garp timer

Use the **set garp timer** command to adjust the values of the join, leave, and leaveall timers.

**set garp timer** *timer\_type timer\_value*

Syntax Description	
<i>timer_type</i>	Type of timer; valid values are <b>join</b> , <b>leave</b> , and <b>leaveall</b> .
<i>timer_value</i>	Timer values in milliseconds; valid values are 1 to 2147483647 milliseconds.

**Defaults** The join timer default is 200 ms; the leave timer default is 600 ms; the leaveall timer default is 10000 ms.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** You must maintain the following unital relationship for the various timer values:

- leave time > 2 \* join time
- leaveall time > leave time



**Note**

The modified values of timers are applied to all GARP applications, ports, and VLANs on the switch.

### Examples

This example shows how to set the join timer value to 100 ms for all the ports on all the VLANs:

```
Console> (enable) set garp timer join 100
GMRP/GARP Join timer value is set to 100 milliseconds.
Console> (enable)
```

This example shows how to set the leave timer value to 300 ms for all the ports on all the VLANs:

```
Console> (enable) set garp timer leave 300
GMRP/GARP Leave timer value is set to 300 milliseconds.
Console> (enable)
```

This example shows how to set the leaveall timer value to 20000 ms for all the ports on all the VLANs:

```
Console> (enable) set garp timer leaveall 20000
GMRP/GARP LeaveAll timer value is set to 20000 milliseconds.
Console> (enable)
Related Coins
```

**set gmrp timer**  
**set gvrp timer**  
**show gmrp configuration**  
**show gvrp configuration**

# set gmrp

Use the **set gmrp** command to enable or disable GMRP on the switch in all VLANs on all ports.

**set gmrp { enable | disable }**

Syntax Description	enable	disable
	Keyword that specifies to enable GMRP on the switch.	Keyword that specifies to disable GMRP on the switch.

**Defaults** The default is GMRP is disabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** You cannot enable GMRP if IGMP snooping or CGMP is already enabled.

**Examples** This example shows how to enable GMRP on the switch:

```
Console> (enable) set gmrp enable
GMRP is enabled.
Console> (enable)
```

This example shows how to disable GMRP on the switch:

```
Console> (enable) set gmrp disable
GMRP is disabled.
Console> (enable)
```

This example shows the display if you try to enable GMRP on the switch with IGMP enabled:

```
Console> (enable) set gmrp enable
Disable IGMP to enable GMRP snooping feature.
Console> (enable)
```

**Related Commands** **show gmrp configuration**

# set gmrp fwdall

Use the **set gmrp fwdall** command to enable or disable the Forward All option on a specified port or module and port list.

```
set gmrp fwdall {enable | disable} mod/port...
```

Syntax Description	enable	disable	mod/port...
	enable	Keyword that enables GMRP Forward All on a specified port.	
	disable	Keyword that disables GMRP Forward All on a specified port.	
	mod/port...	Module number and port number list.	

**Defaults** The default is the Forward All option is disabled for all ports.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** When you enable the Forward All option on a port, that port receives all traffic for all multicast groups on the switch.

If you enable the Forward All option on a trunk port, the option is applied to all VLANs carried on that trunk port.

**Examples** This example shows how to enable GMRP Forward All on module 5, port 5:

```
Console> (enable) set gmrp fwdall enable 5/5
GMRP Forward All groups option enabled on port(s) 5/5.
Console> (enable)
```

This example shows how to disable the GMRP Forward All on module 3, port 2:

```
Console> (enable) set gmrp service fwdall disable 3/2
GMRP Forward All groups option disabled on port(s) 3/2.
Console> (enable)
```

**Related Commands** **show gmrp configuration**

# set gmrp registration

Use the **set gmrp registration** command to specify the GMRP registration type.

**set gmrp registration** *registration-type mod/port...*

<b>Syntax Description</b>	<i>registration-type</i>	Type of registration; valid values are <b>normal</b> , <b>fixed</b> , or <b>forbidden</b> .
	<i>mod/port...</i>	Module number and port number list.

**Defaults** The default is **normal** registration.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** If you enter a *registration-type* of **normal**, dynamic creation, registration, and deregistration of VLANs is supported.

If you enter a *registration-type* of **fixed**, manual VLAN creation and registration, prevention of VLAN deregistration, and registration of all VLANs known to other ports when the **set gvrp registration fixed** command is issued is supported.

If you enter a *registration-type* of **forbidden**, deregistration of all VLANs (except VLAN 1) and prevention of any further VLAN creation or registration is supported.

GMRP supports 100 multicast addresses per VLAN and a total of 3072 for the whole switch.

**Examples** This example shows how to set the registration type to **fixed** on module 3, port 3:

```
Console> (enable) set gmrp registration fixed 3/3
GMRP Registration is set to Fixed for port(s) 3/3.
Console> (enable)
```

This example shows how to set the registration type to **forbidden** on module 1, port 1:

```
Console> (enable) set gmrp registration forbidden 1/1
GMRP Registration is set to Forbidden for port(s) 1/1.
Console> (enable)
```

**Related Commands** **show gmrp configuration**

# set gmrp timer

Use the **set gmrp timer** command to adjust the values of the join, leave, and leaveall timers.

**set gmrp timer** *timer-type timer-value*

<b>Syntax Description</b>	<i>timer-type</i>	Type of timer; valid values are <b>join</b> , <b>leave</b> , and <b>leaveall</b> .
	<i>timer-value</i>	Timer values in milliseconds; valid values are 1 to 2,147,483,647 milliseconds.

**Defaults** The join timer is 200 ms; the leave timer is 600 ms; the leaveall timer is 10,000 ms.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** You must maintain the following unital relationship for the various timer values:

- leave time > 2 \* join time, leaveall time > leave time



**Note**

The modified values of timers are applied to all the GARP applications, ports, and VLANs on the switch.

**Examples** This example shows how to set the join timer value to 100 ms for all the ports on all the VLANs:

```
Console> (enable) set gmrp timer join 100
GARP Join timer value is set to 100 milliseconds.
Console> (enable)
```

This example shows how to set the leave timer value to 300 ms for all the ports on all the VLANs:

```
Console> (enable) set gmrp timer leave 300
GARP Leave timer value is set to 300 milliseconds.
Console> (enable)
```

This example shows how to set the leaveall timer value to 20,000 ms for all the ports on all the VLANs:

```
Console> (enable) set gmrp timer leaveall 20000
GARP LeaveAll timer value is set to 20000 milliseconds.
Console> (enable)
```

**Related Commands**

- show gmrp timer
- set gvrp timer
- set garp timer

# set gvrp

Use the **set gvrp** command to enable or disable GVRP globally on the switch.

```
set gvrp {enable | disable}
```

Syntax Description	enable	disable
	Keyword that specifies to enable GVRP on the switch.	Keyword that specifies to disable GVRP on the switch.

**Defaults** The default is GVRP is disabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** To run GVRP on a trunk, enable GVRP globally on the switch and individually on the trunk. When VTP pruning is enabled, VTP pruning runs on all the GVRP-disabled trunks.

**Examples** This example shows how to enable GVRP globally on the switch:

```
Console> (enable) set gvrp enable
GVRP enabled.
Console> (enable)
```

This example shows how to disable GVRP:

```
Console> (enable) set gvrp disable
GVRP disabled.
Console> (enable)
```

This example shows how to enable GVRP on module 2, port 1:

```
Console> (enable) set gvrp enable 2/1
GVRP enabled on port 2/1.
Console> (enable)
```

**Related Commands**

- show gmrp timer
- show gmrp statistics
- set gvrp timer
- set garp timer

# set gvrp applicant

Use the **set gvrp applicant** command to specify whether or not a VLAN is declared out of blocking ports.

**set gvrp applicant normal | active mod/port...**

Syntax Description	normal	active	mod/port...
	Keyword that specifies to disallow the declaration of any VLAN out of blocking ports.	Keyword that specifies to allow the declaration of active VLANs out of blocking ports.	Module number and port number list.

**Defaults** The default is GVRP applicant set to normal.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** To run GVRP on a trunk, GVRP needs to be enabled both globally on the switch and enabled individually on the trunk.

To prevent undesirable STP topology reconfiguration on a port connected to a device that does not support the per-VLAN mode of STP, configure the GVRP applicant state to **active** on the port. Ports in the GVRP **active** applicant state send GVRP VLAN declarations when they are in the STP blocking state, which prevents the STP BPDUs from being pruned from the other port.



**Note**

Configuring fixed registration on the other device's port also prevents undesirable STP topology reconfiguration.

**Examples** This example shows how to enforce the declaration of all active VLANs out of specified blocking ports:

```
Console> (enable) set gvrp applicant active 4/2-3,4/9-10,4/12-24
Applicant was set to active on port(s) 4/2-3,4/9-10,4/12-24.
Console> (enable)
```

This example shows how to disallow the declaration of any VLAN out of specified blocking ports:

```
Console> (enable) set gvrp applicant normal 4/2-3,4/9-10,4/12-24
Applicant was set to normal on port(s) 4/2-3,4/9-10,4/12-24.
Console> (enable)
```

**Related Commands** show gvrp configuration

# set gvrp dynamic-vlan-creation

Use the **set gvrp dynamic-vlan-creation** command to enable or disable GVRP dynamic VLAN creation.

**set gvrp dynamic-vlan-creation {enable | disable}**

Syntax Description	enable	disable
	Keyword that specifies to enable dynamic VLAN creation.	Keyword that specifies to disable dynamic VLAN creation.

**Defaults** The default is dynamic VLAN creation is disabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** You can enable dynamic VLAN creation only when VTP is in transparent mode and no ISL trunks exist in the switch.

You cannot use this command when there are any 802.1q trunks that are not configured with GVRP.

**Examples** This example shows how to enable dynamic VLAN creation:

```
Console> (enable) set gvrp dynamic-vlan-creation enable
Dynamic VLAN creation enabled.
Console> (enable)
```

This example shows what happens if you try to enable dynamic VLAN creation and VTP is not in transparent mode:

```
Console> (enable) set gvrp dynamic-vlan-creation enable
VTP has to be in TRANSPARENT mode to enable this feature.
Console> (enable)
```

This example shows how to disable dynamic VLAN creation:

```
Console> (enable) set gvrp dynamic-vlan-creation disable
Dynamic VLAN creation disabled.
Console> (enable)
```

**Related Commands** **set vtp**  
**show gvrp configuration**

# set gvrp registration

Use the **set gvrp registration** command to set the administrative control of an outbound port. GVRP registration commands are entered on a per-port basis and applies to all VLANs on the trunk.

```
set gvrp registration { normal | fixed | forbidden } mod/port...
```

Syntax Description		
	<b>normal</b>	Keyword that specifies to allow dynamic registering and deregistering each VLAN (except VLAN 1) on the port.
	<b>fixed</b>	Keyword that specifies to support manual VLAN creation and registration, prevent VLAN deregistration, and register all VLANs known to other ports.
	<b>forbidden</b>	Keyword that specifies that all the VLANs (except VLAN 1) are statically deregistered from the port.
	<i>mod/port...</i>	Module number and port number list.

**Defaults** The default is administrative control is normal.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** When you set VLAN registration, you are indicating to the switch that the VLAN is interested in the users connecting to this port and the VLAN's broadcast and multicast traffic is allowed to send to the port.

For static VLAN configuration, you should set the *mod/port...* control to **fixed** or **forbidden** if the *mod/port...* will not receive or process any GVRP message.

For each dynamically configured VLAN on a port, you should set the *mod/port...* control to normal (default), except for VLAN 1; VLAN 1 should be set to **fixed**.

When GVRP is running, you can create a VLAN through a GVRP trunk port only if you enter the **set gvrp dynamic-vlan-creation enable** and the **set gvrp registration normal** commands.

**Examples** This example shows how to set the administrative control to **normal** on module 3, port 7:

```
Console> (enable) set gvrp registration normal 3/7
Registrar Administrative Control set to normal on port3/7.
Console> (enable)
```

This example shows how to set the administrative control to **fixed** on module 5, port 10:

```
Console> (enable) set gvrp registration fixed 5/10
Registrar Administrative Control set to fixed on Port 5/10.
Console> (enable)
```

■ **set gvrp registration**

This example shows how to set the administrative control to **forbidden** on module 5, port 2:

```
Console> (enable) set gvrp registration forbidden 5/2  
Registrar Administrative Control set to forbidden on port 5/2.  
Console> (enable)
```

---

**Related Commands**    **show gvrp configuration**

# set gvrp timer

Use the **set gvrp timer** command to adjust the values of the join, leave, and leaveall timers.

```
set gvrp timer {timer-type} {timer-value}
```

Syntax Description	
<i>timer-type</i>	Type of timer; valid values are <b>join</b> , <b>leave</b> , and <b>leaveall</b> .
<i>timer-value</i>	Timer values in milliseconds; valid values are 1 to 2,147,483,647 milliseconds.

**Defaults** The default is the join timer is 200 ms; the leave timer is 600 ms; and the leaveall timer is 10,000 ms.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** This command is equivalent to the **set garp timer** command.

You must maintain the following relationship for the various timer values:

- leave time > 2 \* join time
- leaveall time > leave time



**Note**

The modified values of timers are applied to all the GARP applications, ports, and VLANs.

**Examples**

This example shows how to set the join timer value to 100 ms for all the ports on all the VLANs:

```
Console> (enable) set gvrp timer join 100
GVRP/GARP Join timer value is set to 100 milliseconds.
Console> (enable)
```

This example shows how to set the leave timer value to 300 ms for all the ports on all the VLANs:

```
Console> (enable) set gvrp timer leave 300
GVRP/GARP Leave timer value is set to 300 milliseconds.
Console> (enable)
```

This example shows how to set the leaveall timer value to 20,000 ms for all the ports on all the VLANs:

```
Console> (enable) set gvrp timer leaveall 20000
GVRP/GARP LeaveAll timer value is set to 20000 milliseconds.
Console> (enable)
```

■ set gvrp timer

---

**Related Commands**

set garp timer  
show gvrp configuration

# set igmp

Use the **set igmp** command to enable or disable IGMP snooping on the switch.

```
set igmp {enable | disable}
```

## Syntax Description

<b>enable</b>	Keyword that specifies to enable IGMP snooping on the switch.
<b>disable</b>	Keyword that specifies to disable IGMP snooping on the switch.

## Defaults

IGMP snooping 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.

IGMP snooping requires supervisor engine software release 4.1 or later, a Catalyst 5000 family Supervisor Engine III or III F with a NFFC or NFFC II, or Supervisor Engine II G or III G, and a network connection from the switch to a router running IGMP. IGMP snooping is also supported on the Catalyst 2926G series switches.

Before enabling IGMP snooping, you must disable CGMP and CGMP leave processing (by using the **set cgmp** and **set cgmp leave** commands).

## Examples

This example shows how to enable IGMP snooping on the switch:

```
Console> (enable) set igmp enable
IGMP Snooping is enabled.
CGMP is disabled.
Console> (enable)
```

This example shows what happens if you try to enable IGMP if CGMP is already enabled:

```
Console> (enable) set igmp enable
Disable CGMP to enable IGMP Snooping feature.
Console> (enable)
```

## Related Commands

```
clear igmp statistics
show igmp statistics
```

# set igmp fastleave

Use the **set igmp fastleave** command to enable or disable IGMP fastleave processing.

**set igmp fastleave {enable | disable}**

Syntax Description	enable	disable
	Keyword that specifies to enable IGMP fastleave processing.	Keyword that specifies to disable IGMP fastleave processing.

**Defaults** By default, IGMP fastleave processing 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.

**Examples** This example shows how to enable IGMP fastleave processing:

```
Console> (enable) set igmp fastleave enable
IGMP support for fastleave processing enabled.
Console> (enable)
```

This example shows how to disable IGMP fastleave processing:

```
Console> (enable) set igmp fastleave disable
IGMP support for fastleave processing disabled.
Console> (enable)
```

**Related Commands**

- clear igmp statistics**
- set igmp**
- show igmp statistics**

# set igmp mode

Use the **set igmp mode** command to set the IGMP snooping mode.

```
set igmp mode {igmp-only | igmp-cgmp | auto}
```

Syntax Description	igmp-only	Keyword to specify IGMP snooping only.
	igmp-cgmp	Keyword to specify IGMP and CGMP modes.
	auto	Keyword to override the dynamic switching of IGMP snooping modes.

**Defaults** The default is **auto**.

**Command Types** Switch.

**Command Modes** Privileged.

**Usage Guidelines** The switch dynamically chooses either IGMP-only or IGMP-CGMP mode, depending on the traffic present on the network. IGMP-only mode is used in networks with no CGMP devices. IGMP-CGMP mode is used in networks with both IGMP and CGMP devices. Auto mode overrides the dynamic switching of the modes.

**Examples** This example shows how to set the IGMP mode to IGMP only:

```
Console> (enable) set igmp mode igmp-only
IGMP mode set to igmp-only
Console> (enable)
```

This example shows how to set the IGMP mode to auto:

```
Console> (enable) set igmp mode auto
IGMP mode set to auto
Console> (enable)
```

**Related Commands** **show igmp mode**

# set interface

Use the **set interface** command to set the network interface configuration and to enable or disable standard SNMP trap operation.

```
set interface {sc0 | me1 | sl0} {up | down}

set interface sc0 [vlan] [ip_addr [netmask [broadcast]]]

set interface sc0 [vlan] [ip_addr[/netmask] [broadcast]]

set interface me1 ip_addr [netmask [broadcast]]

set interface me1 ip_addr [/netmask [broadcast]]

set interface sl0 slip_addr dest_addr

set interface sc0 dhcp {renew | release}
```

Syntax Description		
<b>sc0</b>	Keyword that specifies the in-band management interface.	
<b>me1</b>	Keyword that specifies the out-of-band management Ethernet interface.	
<b>sl0</b>	Keyword that specifies the SLIP interface.	
<b>up</b>	Keyword that specifies to bring the interface into operation.	
<b>down</b>	Keyword that specifies to bring the interface out of operation.	
<i>vlan</i>	(Optional) Number of the VLAN to be assigned to the interface.	
<i>ip_addr</i>	(Optional) IP address to assign to the interface.	
<i>netmask</i>	(Optional) Subnet mask or mask bits to assign to the interface.	
<i>broadcast</i>	(Optional) Broadcast address to assign to the interface.	
<i>slip_addr</i>	SLIP source address of the console port.	
<i>dest_addr</i>	SLIP destination address of the host to which the console port will be connected.	
<b>dhcp</b>	Keyword that specifies to perform DHCP operations on the sc0 interface.	
<b>renew</b>	Keyword that specifies to renew the lease on a DHCP-learned IP address.	
<b>release</b>	Keyword that specifies to release a DHCP-learned IP address back to the DHCP IP address pool.	

## Defaults

The default configuration has the IP address, subnet mask, and broadcast address of the in-band management interface (sc0) and out-of-band management Ethernet interface (me1) set to 0.0.0.0, with the sc0 interface in VLAN 1. The default configuration for the SLIP interface (sl0) is that the SLIP source and destination addresses are set to 0.0.0.0.

## Command Types

Switch command.

## Command Modes

Privileged.

## Usage Guidelines



### Caution

On the Catalyst 4000 family, 2948G, and 2980G switches, when entering the **set interface me1** or **set interface trap {sc0 | sl0 | me1}** command, sc0 and me1 cannot be configured as **up** when both are in the same subnet or overlapping subnets. If you specify an IP address and subnet for the sc0 or me1 interface that causes an overlap, the me1 interface is kept up or brought up, and the sc0 interface is brought down. The only exception is when both the me1 and sc0 interfaces have IP address 0.0.0.0. In this case, the me1 interface is brought down and the sc0 interface is brought up to allow the DHCP and RARP to run on the sc0 interface.

The Catalyst 5000 family and 2926G series switches support two IP management interfaces, the in-band management interface (sc0) and the SLIP interface (sl0). The sc0 interface is attached to the switching fabric of the switch. The slip interface is an out-of-band management port because it is not attached to the switching fabric and no traffic is switched over it.

The Catalyst 4000 family, 2948G, and 2980G switches support three IP management interfaces: sc0, sl0, and an out-of-band management Ethernet interface (me1). The me1 interface is not attached to the switching fabric. If both the sc0 and me1 interfaces are configured, the supervisor engine software determines which interface to use when performing standard transmission and reception of IP packets based on the local routing table. Operations that use this functionality include TFTP, ping, Telnet, and SNMP.

You can enter the *netmask* value in dotted decimal format or you can specify the number of bits in the netmask (for example, 204.20.22.7/24).

## Examples

This example shows how to use **set interface sc0** and **set interface sl0** from the console port. It also shows how to bring down **interface sc0** using a terminal connected to the console port:

```
Console> (enable) set interface sc0 192.200.11.44 255.255.255.0
Interface sc0 IP address and netmask set.
Console> (enable) set interface sl0 192.200.10.45 192.200.10.103
Interface sl0 SLIP and destination address set.
Console> (enable) set interface sc0 down
Interface sc0 administratively down.
Console> (enable)
```

This example shows how to set the IP address for sc0. If you do not specify a subnet mask, the default mask for that IP address class is used (for example, 255.255.0.0 for a class B address):

```
Console> (enable) set interface sc0 172.20.52.123
Interface sc0 IP address and netmask set.
Console> (enable)
```

This example shows how to set the VLAN, IP address, and subnet mask bits for the sc0 interface:

```
Console> (enable) set interface sc0 5 172.20.52.123/28
Interface sc0 vlan set, IP address and netmask set.
Console> (enable)
```

This example shows how to change the VLAN membership of the sc0 interface:

```
Console> (enable) set interface sc0 2
Interface sc0 vlan set.
Console> (enable)
```

This example shows how to take the sc0 interface down:

```
Console> (enable) set interface sc0 down
Interface sc0 administratively down.
Console> (enable)
```

This example shows how to bring the sc0 interface up:

```
Console> (enable) set interface sc0 up
Interface sc0 administratively up.
Console> (enable)
```

This example shows how to set the IP address and netmask for me1:

```
Console> (enable) set interface me1 10.10.10.20/24
Interface me1 IP address and netmask set.
Console> (enable)
```

This example shows how to set the SLIP source and destination addresses for the console port on the s10 interface:

```
Console> (enable) set interface s10 10.1.1.1 10.1.1.2
Interface s10 slip and destination address set.
Console> (enable)
```

This example shows how to release a DHCP IP address assigned to the sc0 interface:

```
Console> (enable) set interface sc0 dhcp release

Console> (enable)
```

This example shows how to renew the lease on a DHCP IP address assigned to the sc0 interface:

```
Console> (enable) set interface sc0 dhcp release

Console> (enable)
```

This example shows how to release a DHCP IP address assigned to the sc0 interface and obtain a new IP address from the DHCP server:

```
Console> (enable) set interface sc0 dhcp release

Console> (enable)
```

This example shows how to renew the lease on a DHCP-assigned IP address:

```
Console> (enable) set interface sc0 dhcp renew
Renewing IP address...
Console> (enable) Sending DHCP packet with address:00:90:0c:5a:8f:ff
dhcpcoffer
Sending DHCP packet with address:00:90:0c:5a:8f:ff
Timezone set to '', offset from UTC is 7 hours 58 minutes
Timezone set to '', offset from UTC is 7 hours 58 minutes
172.16.30.32 added to DNS server table as primary server.
172.16.31.32 added to DNS server table as backup server.
172.16.32.32 added to DNS server table as backup server.
NTP server 172.16.25.253 added
NTP server 172.16.25.252 added
%MGMT-5-DHCP_S:Assigned IP address 172.20.25.244 from DHCP Server 172.20.25.254
Console> (enable)
```

This example shows how to release the lease on a DHCP-assigned IP address:

```
Console> (enable) set interface sc0 dhcp release
Releasing IP address...
Console> (enable) Sending DHCP packet with address:00:90:0c:5a:8f:ff
Done
Console> (enable)
```

---

**Related Commands**

**show interface  
slip**

# set ip alias

Use the **set ip alias** command to add aliases of IP addresses.

```
set ip alias name ip_addr
```

Syntax Description	
<i>name</i>	Name of the alias being defined.
<i>ip_addr</i>	IP address of the alias being defined.

**Defaults** The default configuration has one IP alias, “default,” mapped to the IP address 0.0.0.0.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** IP aliases take precedence over DNS hostnames.

**Examples** This example shows how to define an IP alias of mercury for IP address 192.168.255.255:

```
Console> (enable) set ip alias mercury 192.168.255.255
IP alias added.
Console> (enable)
```

**Related Commands**

- clear ip alias
- show ip alias

# set ip dns

Use the **set ip dns** command to enable or disable DNS.

```
set ip dns {enable | disable}
```

<b>Syntax Description</b>	<table border="1"> <tbody> <tr> <td data-bbox="380 455 535 499"><b>enable</b></td> <td data-bbox="535 455 1541 499">Keyword that specifies to enable DNS.</td> </tr> <tr> <td data-bbox="380 499 535 541"><b>disable</b></td> <td data-bbox="535 499 1541 541">Keyword that specifies to disable DNS.</td> </tr> </tbody> </table>	<b>enable</b>	Keyword that specifies to enable DNS.	<b>disable</b>	Keyword that specifies to disable DNS.
<b>enable</b>	Keyword that specifies to enable DNS.				
<b>disable</b>	Keyword that specifies to disable DNS.				
<b>Defaults</b>	DNS is disabled.				
<b>Command Types</b>	Switch command.				
<b>Command Modes</b>	Privileged.				
<b>Usage Guidelines</b>	If DNS is disabled, you must use the IP address with all commands that require explicit IP addresses or manually define an alias for that address. The alias has priority over DNS.				
<b>Examples</b>	<p>This example shows how to enable DNS:</p> <pre>Console&gt; (enable) set ip dns enable DNS is enabled. Console&gt; (enable)</pre> <p>This example shows how to disable DNS:</p> <pre>Console&gt; (enable) set ip dns disable DNS is disabled. Console&gt; (enable)</pre>				
<b>Related Commands</b>	show ip dns				

# set ip dns domain

Use the **set ip dns domain** command to set the default DNS domain name.

**set ip dns domain** *name*

<b>Syntax Description</b>	<i>name</i> Default DNS domain name.
---------------------------	--------------------------------------

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

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

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

<b>Usage Guidelines</b>	If you specify a domain name on the command line, the system attempts to resolve the host name as entered. If the system cannot resolve the host name as entered, it appends the default DNS domain name as defined with the <b>set ip dns domain</b> command. If you specify a domain name with a trailing dot, the program considers this an <i>absolute</i> domain name.
-------------------------	---

<b>Examples</b>	This example shows how to set the default DNS domain name:
-----------------	--

```
Console> (enable) set ip dns domain yow.com
Default DNS domain name set to yow.com.
Console> (enable)
```

<b>Related Commands</b>	<b>clear ip dns domain</b> <b>show ip dns</b>
-------------------------	--

# set ip dns server

Use the **set ip dns server** command to set the IP address of a DNS server.

```
set ip dns server ip_addr [primary]
```

<b>Syntax Description</b>	<table border="1"> <tbody> <tr> <td><i>ip_addr</i></td> <td>IP address of the DNS server.</td> </tr> <tr> <td><b>primary</b></td> <td>(Optional) Keyword that specifies to configure a DNS server as the primary server.</td> </tr> </tbody> </table>	<i>ip_addr</i>	IP address of the DNS server.	<b>primary</b>	(Optional) Keyword that specifies to configure a DNS server as the primary server.
<i>ip_addr</i>	IP address of the DNS server.				
<b>primary</b>	(Optional) Keyword that specifies to configure a DNS server as the primary server.				
<b>Defaults</b>	This command has no default setting.				
<b>Command Types</b>	Switch command.				
<b>Command Modes</b>	Privileged.				
<b>Usage Guidelines</b>	You can configure up to three DNS name servers as backup. You can also configure any DNS server as the primary server. The primary server is queried first. If the primary server fails, the backup servers are queried.				
<b>Examples</b>	<p>These examples show how to set the IP address of a DNS server:</p> <pre>Console&gt; (enable) <b>set ip dns server 198.92.30.32</b> 198.92.30.32 added to DNS server table as primary server. Console&gt; (enable)</pre> <pre>Console&gt; (enable) <b>set ip dns server 171.69.2.132 primary</b> 171.69.2.132 added to DNS server table as primary server. Console&gt; (enable)</pre> <pre>Console&gt; (enable) <b>set ip dns server 171.69.2.143 primary</b> 171.69.2.143 added to DNS server table as primary server. Console&gt; (enable)</pre> <p>This example shows what happens if you enter more than three DNS name servers as backup:</p> <pre>Console&gt; (enable) <b>set ip dns server 161.44.128.70</b> DNS server table is full. 161.44.128.70 not added to DNS server table. Console&gt; (enable)</pre>				
<b>Related Commands</b>	<pre>clear ip dns server show ip dns</pre>				

## set ip fragmentation

Use the **set ip fragmentation** command to enable or disable the fragmentation of IP packets bridged between FDDI and Ethernet networks. Note that FDDI and Ethernet networks have different MTUs.

**set ip fragmentation {enable | disable}**

### Syntax Description

<b>enable</b>	Keyword that specifies to permit fragmentation for IP packets bridged between FDDI and Ethernet networks.
<b>disable</b>	Keyword that specifies to disable fragmentation for IP packets bridged between FDDI and Ethernet networks.

### Defaults

The default value is IP fragmentation enabled.

### Command Types

Switch command.

### Command Modes

Privileged.

### Usage Guidelines

If IP fragmentation is disabled, FDDI packets that exceed the Ethernet MTU are dropped if they are being bridged to Ethernet on the switch.

### Examples

This example shows how to enable IP fragmentation:

```
Console> (enable) set ip fragmentation enable
Bridge IP fragmentation enabled.
Console> (enable)
```

This example shows how to disable IP fragmentation:

```
Console> (enable) set ip fragmentation disable
Bridge IP fragmentation disabled.
Console> (enable)
```

### Related Commands

**show bridge**  
**show ip route**

# set ip http port

Use the **set ip http port** command to configure the TCP port number for the HTTP server.

```
set ip http port {port_num} [default port_num]
```

Syntax Description	
<i>port_num</i>	TCP port number; valid values are from 1 to 65535.
<b>default</b> <i>port_num</i>	(Optional) Keyword and variable that specify the TCP default port number; valid values are from 80 to 65535.

**Defaults** The default TCP port number is 80.

**Command Types** Switch command.

**Command Modes** Privileged.

**Examples** This example shows how to set the IP HTTP port default:

```
Console> (enable) set ip http port default
HTTP TCP port number is set to 80.
Console> (enable)
```

This example shows how to set the IP HTTP port number:

```
Console> (enable) set ip http port 2398
HTTP TCP port number is set to 2398.
Console> (enable)
```

**Related Commands**

- set ip http server**
- show ip http**

## set ip http server

Use the **set ip http server** command to enable or disable the HTTP server.

```
set ip http server {enable | disable}
```

Syntax Description	
<b>enable</b>	Keyword that enables the HTTP server.
<b>disable</b>	Keyword that disables the HTTP server.

Defaults	
	The default is the HTTP server is disabled.

Command Types	
	Switch command.

Command Modes	
	Privileged.

Examples	
	This example shows how to enable the HTTP server:

```
Console> (enable) set ip http server enable
HTTP server is enabled.
Console> (enable)
```

This example shows the system response when the HTTP server **enable** command is not supported:

```
Console> (enable) set ip http server enable
Feature not supported.
Console> (enable)
```

This example shows how to disable the HTTP server:

```
Console> (enable) set ip http server disable
HTTP server disabled.
Console> (enable)
```

Related Commands	
	<b>set ip http port</b> <b>show ip http</b>

# set ip permit

Use the **set ip permit** command to enable or disable the IP permit list and to specify IP addresses to be added to the IP permit list.

```
set ip permit {enable | disable}
```

```
set ip permit {enable | disable} [telnet | snmp]
```

```
set ip permit ip_addr [mask] [telnet | snmp | all]
```

<b>Syntax Description</b>	<b>enable</b>	Keyword that specifies to enable the IP permit list.
	<b>disable</b>	Keyword that specifies to disable the IP permit list.
	<b>telnet</b>	(Optional) Telnet IP permit list.
	<b>snmp</b>	(Optional) SNMP IP permit list.
	<i>ip_addr</i>	IP address to be added to the IP permit list. An IP alias or host name that can be resolved through DNS can also be used.
	<i>mask</i>	(Optional) Subnet mask of the specified IP address.
	<b>all</b>	(Optional) Keyword that specifies all entries in the IP permit list.

**Defaults** The IP permit list is disabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** You can configure up to 100 entries in the permit list. If the IP permit list is enabled, but the permit list has no entries configured, a caution displays on the screen.

Make sure you enter the entire **disable** keyword when entering the **set ip permit disable** command. If you abbreviate the keyword, the abbreviation is interpreted as a host name to add to the IP permit list.

If the **snmp**, **telnet**, or **all** variable is not specified, the IP address is added to both the SNMP and Telnet permit lists.

You enter the mask in dotted decimal format, for example, 255.255.0.0.

**Examples** This example shows how to add an IP address to the IP permit list:

```
Console> (enable) set ip permit 192.168.255.255
192.168.255.255 added to IP permit list.
Console> (enable)
```

This example shows how to add an IP address using an IP alias or host name to both the SNMP and Telnet permit lists:

```
Console> (enable) set ip permit batboy
batboy added to IP permit list.
Console> (enable)
```

This example shows how to add a subnet mask of the IP address to both the SNMP and Telnet permit lists:

```
Console> (enable) set ip permit 192.168.255.255 255.255.192.0
192.168.255.255 with mask 255.255.192.0 added to IP permit list.
Console> (enable)
```

This example shows how to add an IP address to the Telnet IP permit list:

```
Console> (enable) set ip permit 172.16.0.0 255.255.0.0 telnet
172.16.0.0 with mask 255.255.0.0 added to telnet permit list.
Console> (enable)
```

This example shows how to add an IP address to the SNMP IP permit list:

```
Console> (enable) set ip permit 172.20.52.32 255.255.255.224 snmp
172.20.52.32 with mask 255.255.255.224 added to snmp permit list.
Console> (enable)
```

This example shows how to add an IP address to the all IP permit lists:

```
Console> (enable) set ip permit 172.20.52.3 all
172.20.52.3 added to IP permit list.
Console> (enable)
```

This example shows how to enable the IP permit list:

```
Console> (enable) set ip permit enable
IP permit list enabled.
Console> (enable)
```

This example shows how to disable the IP permit list:

```
Console> (enable) set ip permit disable
IP permit list disabled.
Console> (enable)
```

**Related Commands**    clear ip permit show ip permit

# set ip redirect

Use the **set ip redirect** command to enable or disable ICMP redirect messages.

```
set ip redirect {enable | disable}
```

Syntax Description	enable	disable
	Keyword that specifies to permit ICMP redirect messages to be returned to the source host.	Keyword that specifies to prevent ICMP redirect messages from being returned to the source host.

**Defaults** The default configuration has ICMP redirect enabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Examples** This example shows how to deactivate ICMP redirect messages:

```
Console> (enable) set ip redirect disable
ICMP redirect messages disabled.
Console> (enable)
```

**Related Commands** **show ip route**  
**show netstat**

# set ip route

Use the **set ip route** command to add IP addresses or aliases to the IP routing table.

```
set ip route default gateway [metric] [primary]
```

```
set ip route destination[/netmask] gateway
```

## Syntax Description

<b>default</b>	Keyword that specifies the entry as a default route.
<i>gateway</i>	IP address or IP alias of the router.
<i>metric</i>	(Optional) Value used to indicate the number of hops between the switch and the gateway.
<b>primary</b>	(Optional) Keyword that specifies the primary default route.
<i>destination</i>	IP address or IP alias of the network, or IP address, DNS hostname, or IP alias of a specific host to be added.
<i>/netmask</i>	(Optional) Subnet mask or mask bits to assign to the interface.

## Defaults

The default configuration routes the local network through the sc0 interface with metric 0 as soon as sc0 is configured.

## Command Types

Switch command.

## Command Modes

Privileged.

## Usage Guidelines

You can configure up to three default gateways. You can specify a primary default gateway using the primary keyword. If a primary is not designated, the first default gateway you configure is the primary.

The switch forwards all off-network IP traffic generated by the switch itself to the primary default gateway unless the primary is unavailable. The entries in the IP routing table are only used for IP traffic generated by the switch itself (for example, Telnet, ping, or TFTP sessions from the switch CLI), not for IP data travelling through the switch.

On the Catalyst 4000 family, 2948G, and 2980G switches, the supervisor engine software automatically determines whether a default gateway is reached through the sc0 interface or the me1 interface.

You can enter the destination and gateway as either an IP alias or IP address in dotted format (for example, 172.20.52.7). You can enter the destination network mask in dotted decimal format or you can specify the number of bits in the netmask (for example, 204.20.22.7/24). CIDR IP address and subnet mask values are accepted for the destination network address.

---

**Examples**

This example shows how to add three default routes to the IP routing table:

```
Console> (enable) set ip route default 172.20.52.35
Route added.
Console> (enable) set ip route default 172.20.52.40
Route added.
Console> (enable) set ip route default 172.20.52.45
Route added.
Console> (enable)
```

This example shows how to add a route to network 10.10.0.0/16 through gateway 172.20.52.33:

```
Console> (enable) set ip route 10.10.0.0/16 172.20.52.33
Route added.
Console> (enable)
```

This example shows how to add a route to a specific host:

```
Console> (enable) set ip route 172.20.50.2/32 172.20.52.41
Route added.
Console> (enable)
```

---

**Related Commands**

**clear ip route**  
**show ip route**

# set ip unreachable

Use the **set ip unreachable** command to enable or disable ICMP unreachable messages on the switch.

**set ip unreachable { enable | disable }**

Syntax Description	enable	disable
	Keyword that specifies to allow IP unreachable messages to be returned to the source host.	Keyword that specifies to prevent IP unreachable messages from being returned to the source host.

**Defaults** The default has ICMP unreachable messages enabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** When you enable ICMP unreachable messages, the switch returns an ICMP unreachable message to the source host whenever it receives an IP datagram that it cannot deliver. When you disable ICMP unreachable messages, the switch does not notify the source host when it receives an IP datagram that it cannot deliver.

For example, a switch has the ICMP unreachable message function enabled and IP fragmentation disabled. If an FDDI frame is received and needs to transmit to an Ethernet port, the switch cannot fragment the packet. The switch drops the packet and returns an IP unreachable message to the Internet source host.

**Examples** This example shows how to disable ICMP unreachable messages:

```
Console> (enable) set ip unreachable disable
ICMP Unreachable message disabled.
Console> (enable)
```

# set kerberos clients mandatory

Use the **set kerberos clients mandatory** command to make Kerberos authentication mandatory for authenticating to services on the network.

## **set kerberos clients mandatory**

---

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

---

**Defaults** Kerberos clients are not set to mandatory.

---

**Command Types** Switch command.

---

**Command Modes** Privileged.

---

**Usage Guidelines** As an added layer of security, you can optionally configure the switch so that after users authenticate to it, they can authenticate to other services on the network only with Kerberos clients. If you do not make Kerberos authentication mandatory and Kerberos authentication fails, the application attempts to authenticate users using the default method of authentication for that network service. For example, Telnet prompts for a password.

---

**Examples** This example shows how to make Kerberos authentication mandatory:

```
Console> (enable) set kerberos clients mandatory
Kerberos clients set to mandatory
Console> (enable)
```

---

**Related Commands** **set kerberos credentials forward**  
**clear kerberos clients mandatory**

# set kerberos credentials forward

Use the **set kerberos credentials forward** command to configure clients to forward users' credentials as they connect to other hosts in the Kerberos realm.

## set kerberos credentials forward

---

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

---

**Defaults** Forwarding is disabled by default.

---

**Command Types** Switch command.

---

**Command Modes** Privileged.

---

**Usage Guidelines** A user authenticated to a Kerberized switch has a ticket granting ticket (TGT) and can use it to authenticate to a host on the network. However, if forwarding is not enabled and a user tries to list credentials after authenticating to a host, the output will show no Kerberos credentials present.

You can optionally configure the switch to forward users' TGTs with them as they authenticate from the switch to Kerberized remote hosts on the network when using Kerberized Telnet.

---

**Examples** This example shows how to enable Kerberos credentials forwarding:

```
kerberos> (enable) set kerberos credentials forward
Kerberos credentials forwarding enabled
kerberos> (enable)
```

---

**Related Commands** **set kerberos credentials forward**  
**set kerberos clients mandatory**

# set kerberos local-realm

Use the **set kerberos local-realm** command to configure a switch to authenticate users defined in the Kerberos database.

```
set kerberos local-realm kerberos-realm
```

<b>Syntax Description</b>	<i>kerberos-realm</i> IP address or name (in uppercase characters) of the Kerberos realm.
<b>Defaults</b>	Default value is a NULL string.
<b>Command Types</b>	Switch command.
<b>Command Modes</b>	Privileged.
<b>Usage Guidelines</b>	For a switch to authenticate a user defined in the Kerberos database, the switch must know the host name or IP address of the host running the Key Distribution Center (KDC) and the name of the Kerberos realm. Optionally, the switch should be able to map the host name or Domain Naming System (DNS) domain to the Kerberos realm.
<b>Examples</b>	This example shows how to set a default Kerberos local realm for the switch:  kerberos> (enable) <b>set kerberos local-realm CISCO.COM</b> Kerberos local realm for this switch set to CISCO.COM. aspen-kerberos> (enable)
<b>Related Commands</b>	<b>set kerberos realm</b> <b>clear kerberos realm</b>

# set kerberos realm

Use the **set kerberos realm** command to map the name of a Kerberos realm to a DNS domain name or a host name.

**set kerberos realm** *dns-domain* | *host* *kerberos-realm*

Syntax Description		
	<i>dns-domain</i>	DNS domain name to map to Kerberos realm.
	<i>host</i>	IP address or name to map to Kerberos realm.
	<i>kerberos-realm</i>	IP address or name of Kerberos realm.

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

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** The name of the Kerberos realm can be mapped to a DNS domain name or a host name. This can be done by the **set kerberos realm** command, which is an optional command. The information entered with this command is stored in a table with one entry for each Kerberos realm. The maximum number of entries in the table is 100.

**Examples** This example shows how to map the Kerberos realm to a domain name:

```
Console> (enable) set kerberos realm CISCO CISCO.COM
Kerberos DnsDomain-Realm entry set to CISCO - CISCO.COM
Console> (enable)
```

**Related Commands**

- set kerberos local-realm
- clear kerberos realm

# set kerberos server

Use the **set kerberos realm** command to specify which KDC to use on the switch.

```
set kerberos server kerberos-realm hostname | ip-address [port-number]
```

<b>Syntax Description</b>	<p><i>kerberos-realm</i> Name of the Kerberos realm.</p> <p><i>hostname</i> Name of host running the KDC.</p> <p><i>ip-address</i> IP address of host running the KDC.</p> <p><i>port-number</i> (Optional) Number of the port.</p>
<b>Defaults</b>	This command has no default setting.
<b>Command Types</b>	Switch command.
<b>Command Modes</b>	Privileged.
<b>Usage Guidelines</b>	You can specify to the switch which key distribution center (KDC) to use in a Kerberos realm. Optionally, you can also specify the port number which the KDC is monitoring. The Kerberos server information you enter is maintained in a table with one entry for each Kerberos realm. The maximum number of entries in the table is 100.
<b>Examples</b>	<p>This example shows how to specify the Kerberos server:</p> <pre>kerberos&gt; (enable) <b>set kerberos server CISCO.COM 187.0.2.1 750</b> Kerberos Realm-Server-Port entry set to:CISCO.COM - 187.0.2.1 - 750 kerberos&gt; (enable)</pre>
<b>Related Commands</b>	<b>clear kerberos server</b>

## set kerberos srvtab entry

Use the **set kerberos srvtab entry** command to enter the SRVTAB file directly into the switch from the command line.

**set kerberos srvtab entry** *kerberos-principal principal-type timestamp key-version number key-type key-length encrypted-keytab*

### Syntax Description

<i>kerberos-principal</i>	Service on the switch.
<i>principal-type</i>	Version of the Kerberos SRVTAB.
<i>timestamp</i>	Number representing the date and time the SRVTAB entry was created.
<i>key-version number</i>	Version of the encrypted key format.
<i>key-type</i>	Type of encryption used.
<i>key-length</i>	Length, in bytes, of the encryption key.
<i>encrypted-keytab</i>	Secret key the switch shares with the KDC. This key is encrypted with the private DES key when you copy the configuration to a file or enter the <b>show config</b> command.

### Defaults

This command has no default setting.

### Command Types

Switch command.

### Command Modes

Privileged.

### Usage Guidelines

When you enter the SRVTAB directly into the switch, create an entry for each Kerberos principal (service) on the switch. The entries are maintained in the SRVTAB table. The maximum size of the table is 20 entries.

### Examples

This example shows how to enter a SRVTAB file directly into the switch:

```
kerberos> (enable) set kerberos srvtab entry host/niners.cisco.com@CISCO.COM 0 932423923
1 1 8 03;;5>00>50;0=0=0
Kerberos SRVTAB entry set to
Principal:host/niners.cisco.com@CISCO.COM
Principal Type:0
Timestamp:932423923
Key version number:1
Key type:1
Key length:8
Encrypted key tab:03;;5>00>50;0=0=0
```

**Related Commands**    set kerberos srvtab remote  
                              clear kerberos srvtab entry

## set kerberos srvtab remote

Use the **set kerberos srvtab remote** command to provide the switch with a copy of the SRVTAB file from the KDC that contains the secret key.

```
set kerberos srvtab remote {hostname | ip-address} filename
```

Syntax Description	
<i>hostname</i>	Name of host running the KDC.
<i>ip-address</i>	IP address of host running the KDC
<i>filename</i>	Name of the SRVTAB file.

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

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** To make it possible for remote users to authenticate to the switch using Kerberos credentials, the switch must share a secret key with the KDC. To do this, you must give the switch a copy of the file that is stored in the KDC, which contains the secret key. These files are called SRVTAB files.

The most secure method to copy SRVTAB files to the hosts in your Kerberos realm is to copy them onto physical media and go to each host in turn and manually copy the files onto the system. To copy SRVTAB files to the switch, which does not have a physical media drive, you must transfer them through the network using the Trivial File Transfer Protocol (TFTP).

**Examples** This example shows how to remotely copy SRVTAB files to the switch from the KDC:

```
kerberos> (enable) set kerberos srvtab remote 187.20.32.10 /users/jdoe/krb5/ninerskeytab
kerberos> (enable)
```

**Related Commands** [set kerberos srvtab entry](#)

# set key config-key

Use the **set key config-key** command to define a private DES key for the switch.

**set key config-key** *string*

<b>Syntax Description</b>	<i>string</i> DES key for switch. Should be no longer than eight bytes.
<b>Defaults</b>	This command has no default setting.
<b>Command Types</b>	Switch command.
<b>Command Modes</b>	Privileged.
<b>Usage Guidelines</b>	You can define a private DES key for the switch. The private DES key can be used to encrypt the secret key that the switch shares with the KDC. If the DES key is set, the secret key is not displayed in clear text when the <b>show kerberos</b> command is executed. The key length should be eight characters or less.
<b>Examples</b>	This example shows how to define a DES key: <pre>kerberos&gt; (enable) <b>set key config-key abcd</b> Kerberos config key set to abcd kerberos&gt; (enable)</pre>
<b>Related Commands</b>	<b>clear key config-key</b>

# set length

Use the **set length** command to configure the number of lines in the terminal display screen.

**set length** *number* [**default**]

Syntax Description	
<i>number</i>	Number of lines to display on the screen; valid values are 0 and 5 to 512. 0 turns off the scrolling feature.
<b>default</b>	(Optional) Keyword that specifies to set the number of lines in the terminal display screen for the current administration session and all other sessions. This keyword is only available in normal mode.

**Defaults** The default screen length is 24 lines.

**Command Types** Switch command.

**Command Modes** Privileged.

**Usage Guidelines** Output from a single command that overflows a single display screen is followed by the --More-- prompt. At the --More-- prompt, you can press **Ctrl-C**, **q**, or **Q** to interrupt the output and return to the prompt, press the **Spacebar** to display an additional screen of output, or press **Return** to display one more line of output.

Setting the screen length to 0 turns off the scrolling feature and causes the entire output to display at once. Unless the **default** keyword is used, a change to the terminal length value applies only to the current session.

**Examples** This example shows how to set the screen length to 60 lines:

```
Console> (enable) set length 60
Screen length for this session set to 60.
Console> (enable)
```

This example shows how to set the default screen length to 40 lines:

```
Console> (enable) set length 40 default
Screen length set to 40.
Console> (enable)
```

# set logging buffer

Use the **set logging buffer** command to limit the number of system logging messages buffered.

**set logging buffer** *buffer\_size*

---

<b>Syntax Description</b>	<i>buffer_size</i> Number of system logging messages to store in the buffer; valid values are 1 to 500.
---------------------------	---

---

---

<b>Defaults</b>	The default value is 500.
-----------------	---------------------------

---

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

---

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

---

<b>Examples</b>	This example shows how to limit the syslog message buffer to 400 messages:
-----------------	--

```
Console> (enable) set logging buffer 400  
System logging buffer size set to <400>.  
Console> (enable)
```

---

<b>Related Commands</b>	<b>set logging timestamp</b> <b>show logging buffer</b> <b>clear logging buffer</b>
-------------------------	---

# set logging console

Use the **set logging console** command to enable and disable the sending of system logging messages to the console.

**set logging console {enable | disable}**

Syntax Description	enable	disable
	Keyword that specifies to enable system message logging to the console.	Keyword that specifies to disable system message logging to the console.

**Defaults** By default, system message logging to the console is enabled.

**Command Types** Switch command.

**Command Modes** Privileged.

**Examples** This example shows how to enable system message logging to the console:

```
Console> (enable) set logging console enable
System logging messages will be sent to the console.
Console> (enable)
```

This example shows how to disable system message logging to the console:

```
Console> (enable) set logging console disable
System logging messages will not be sent to the console.
```

**Related Commands**

- set logging level
- set logging session
- show logging
- show logging buffer