

set default portstatus

Use the **set default portstatus** command to set the default port status.

```
set default portstatus {enable | disable}
```

Syntax Description	<table><tbody><tr><td>enable</td><td>Keyword to activate default port status.</td></tr><tr><td>disable</td><td>Keyword to deactivate default port status.</td></tr></tbody></table>	enable	Keyword to activate default port status.	disable	Keyword to deactivate default port status.
enable	Keyword to activate default port status.				
disable	Keyword to deactivate default port status.				
Defaults	This command has no default setting.				
Command Types	Switch command.				
Command Modes	Privileged.				
Usage Guidelines	<p>When you enter the clear config all command or in the event of a configuration loss, all ports collapse into VLAN 1. This might cause a security and network instability problem. Entering the set default portstatus command puts all ports into a disable state and blocks the traffic flowing through the ports during a configuration loss. You can then manually configure the ports back to the enable state.</p> <p>After you enter the set default portstatus command, you must reset the system so the new configuration setup can take effect.</p> <p>This command is not saved in the configuration file.</p> <p>Once you set the default port status, the default port status does not clear when you enter the clear config all command.</p>				
Examples	<p>This example shows how to disable the default port status:</p> <pre>Console> (enable) set default portstatus disable port status set to disable. WARNING: Please reset the system to have new setup in effect. Console> (enable)</pre>				
Related Commands	show default				

set enablepass

Use the **set enablepass** command to change the password for the privileged level of the CLI.

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 to 19 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 errdisable-timeout

Use the **set errdisable-timeout** command to configure a timeout for ports in errdisable state, after which the ports are reenabled automatically.

```
set errdisable-timeout {enable | disable} {reason}
```

```
set errdisable-timeout interval {interval}
```

Syntax Description	enable	Keyword to enable errdisable timeout.
	disable	Keyword to disable errdisable timeout.
	<i>reason</i>	Reason for the port being in the errdisable state; valid values are bpdu-guard , channel-misconfig , duplex-mismatch , udld , other , and all .
	interval <i>interval</i>	Timeout interval; valid values are from 30 to 86400 seconds (30 seconds to 24 hours).

Defaults The default is **disable** and the *interval* is 300 seconds.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The errdisable timeout feature allows you to configure a timeout period for ports in errdisable state. When this feature is enabled, ports are reenabled automatically after the timeout interval has elapsed. A port enters errdisable state for the following reasons (these reasons appear as configuration options with the set errdisable-timeout enable command):

- Channel misconfiguration
- Duplex mismatch
- BPDU port-guard
- UDLD
- Other (reasons other than the above)
- All (apply errdisable timeout to all reasons)

You can enable or disable errdisable timeout for each of the above listed reasons. The ports in errdisable state for reasons other than the first four reasons are considered "other." If you specify other, all ports errdisabled by causes other than the first four reasons are enabled for errdisable timeout. If you specify "all," all ports errdisabled for any reason are enabled for errdisable timeout.

Examples

This example shows how to enable an errdisable timeout for BPDU guard causes:

```
Console> (enable) set errdisable-timeout enable bpdu-guard  
Successfully enabled errdisable-timeout for bpdu-guard.  
Console> (enable)
```

This example shows how to set an errdisable timeout interval to 450 seconds:

```
Console> (enable) set errdisable-timeout interval 450  
Successfully set errdisable timeout to 450 seconds.  
Console> (enable)
```

Related Commands

show errdisable-timeout

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)
```

Related Commands **show errordetection**

set feature mdg

Use the **set feature mdg** command to enable or disable the multiple default gateway feature.

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

Syntax Description

enable Keyword to enable the multiple default gateway.

disable Keyword to disable the multiple default gateway.

Defaults

This command has no default setting.

Command Types

Switch command.

Command Modes

Privilege.

Usage Guidelines

If you enable the multiple default gateway feature, the Catalyst 6000 family switch pings the default gateways every 10 seconds to verify the gateways are still available.

Examples

This example shows how to enable the multiple default gateway feature:

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



This example shows how to disable the multiple default gateway feature:

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

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	<table border="1"> <tr> <td><i>timer_type</i></td> <td>Type of timer; valid values are join, leave, and leaveall.</td> </tr> <tr> <td><i>timer_value</i></td> <td>Timer values in milliseconds; valid values are from 1 to 2147483647 milliseconds.</td> </tr> </table>	<i>timer_type</i>	Type of timer; valid values are join , leave , and leaveall .	<i>timer_value</i>	Timer values in milliseconds; valid values are from 1 to 2147483647 milliseconds.
<i>timer_type</i>	Type of timer; valid values are join , leave , and leaveall .				
<i>timer_value</i>	Timer values in milliseconds; valid values are from 1 to 2147483647 milliseconds.				
Defaults	The default is the join timer default is 200 ms, the leave timer default is 600 ms, and the leaveall timer default is 10000 ms.				
Command Types	Switch command.				
Command Modes	Privileged.				
Usage Guidelines	<p>You must maintain the following <i>relationship</i> for the various timer values:</p> <ul style="list-style-type: none"> • Leave time must be greater than or equal to three times the join time. • Leaveall time must be greater than the leave time. 				
 Caution	Set the same GARP application (for example, GMRP and GVRP) timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP applications will not operate successfully.				
 Note	The modified timer values are applied to all GARP application (for example, GMRP and GVRP) timer values.				
Examples	<p>This example shows how to set the join timer value to 100 ms for all the ports on all the VLANs:</p> <pre>Console> (enable) set garp timer join 100 GMRP/GARP Join timer value is set to 100 milliseconds. Console> (enable)</pre> <p>This example shows how to set the leave timer value to 300 ms for all the ports on all the VLANs:</p> <pre>Console> (enable) set garp timer leave 300 GMRP/GARP Leave timer value is set to 300 milliseconds. Console> (enable)</pre>				

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)  
set gmrp timer  
set gvrp timer  
show gmrp timer
```

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 to enable GMRP on the switch.	Keyword 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 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 feature on a specified port or module and port list.

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

Syntax Description	enable	Keyword to enable GMRP Forward All on a specified port.
	disable	Keyword to disable GMRP Forward All on a specified port.
	mod/port...	Number of the module and the ports on the module.

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

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines Forward All indicates that a port is interested in receiving all the traffic for all the multicast groups. If the port is trunking, then this feature is applied to all the VLANs on that 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 {normal | fixed | forbidden} mod/port...
```

Syntax Description	normal	Keyword to specify dynamic GMRP multicast registration and deregistration on the port.
	fixed	Keyword to specify the multicast groups currently registered on the switch are applied to the port, but any subsequent registrations or deregistrations do not affect the port. Any registered multicast groups on the port are not deregistered based on the GARP timers.
	forbidden	Keyword to specify that all GMRP multicasts are deregistered and prevent any further GMRP multicast registration on the port.
	<i>mod/port...</i>	Number of the module and the ports on the module.

Defaults The default is administrative control is normal.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines You must return the port to **normal** registration mode to deregister multicast groups on the port. GMRP supports a total of 3072 multicast addresses 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}
```

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

Defaults The default is the join timer is 200 ms, the leave timer is 600 ms, and the leaveall timer is 10000 ms.

Command Types Switch command.

Command Modes Privileged.

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

- Leave time must be greater than or equal to three times the join time.
- Leaveall time must be greater than the leave time.



Caution

Set the same GARP application (for example, GMRP and GVRP) timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP applications will not operate successfully.



Note

The modified timer values are applied to all GARP application (for example, GMRP and GVRP) timer values.

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 20000 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 in the switch or on a per-port basis.

```
set gvrp {enable | disable} [mod/port]
```

Syntax Description	enable	disable	mod/port
	Keyword to enable GVRP on the switch.	Keyword to disable GVRP on the switch.	(Optional) Number of the module and port on the module.

Defaults The default is GVRP is globally set to disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines When you enable VTP pruning, VTP pruning runs on all the GVRP-disabled trunks. To run GVRP on a trunk, you need to enable GVRP both globally on the switch and individually on the trunk.

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 gvrp configuration**
- 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 to disallow the declaration of any VLAN out of blocking ports.	Keyword to enforce the declaration of all active VLANs out of blocking ports.	Number of the module and the ports on the module.

Defaults The default is GVRP applicant set to normal.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines To run GVRP on a trunk, you need to enable GVRP both globally on the switch and individually on the trunk.

On a port connected to a device that does not support the per-VLAN mode of STP, the port state may continuously cycle from blocking to listening to learning to learning, and back to blocking. To prevent this, you must enter the **set gvrp applicant active mod/port...** command on the port to send GVRP VLAN declarations when the port is in the STP blocking state.

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 dynamic VLAN creation.

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

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

This feature is not allowed when there are 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 and apply to all VLANs on the trunk. GVRP registration commands are entered on a per-port basis.

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

Syntax Description	normal	Keyword to allow dynamic registering and deregistering each VLAN (except VLAN 1) on the port.
	fixed	Keyword to support manual VLAN creation and registration, prevent VLAN deregistration, and register all VLANs known to other ports.
	forbidden	Keyword to specify that all the VLANs (except VLAN 1) are statically deregistered from the port.
	<i>mod/port..</i>	Number of the module and the ports on the module.
Defaults	The default is administrative control is normal.	
Command Types	Switch command.	
Command Modes	Privileged.	
Usage Guidelines	<p>When you set VLAN registration, you are telling the switch that the VLAN is interested in the user(s) connecting to this port and the VLAN's broadcast and multicast traffic is allowed to send to the port.</p> <p>For static VLAN configuration, you should set the <i>mod/port..</i> control to fixed or forbidden if the <i>mod/port..</i> will not receive or process any GVRP message.</p> <p>For each dynamically configured VLAN on a port, you should set the <i>mod/port..</i> control to normal (default), except for VLAN 1; GVRP registration mode for VLAN 1 is always fixed and is not configurable. VLAN 1 is always carried by 802.1Q trunks on which GVRP is enabled.</p> <p>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.</p>	

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 port 3/7.
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	<table border="1"> <tr> <td><i>timer_type</i></td> <td>Type of timer; valid values are join, leave, and leaveall.</td> </tr> <tr> <td><i>timer_value</i></td> <td>Timer values in milliseconds; valid values are from 1 to 2147483647 milliseconds.</td> </tr> </table>	<i>timer_type</i>	Type of timer; valid values are join , leave , and leaveall .	<i>timer_value</i>	Timer values in milliseconds; valid values are from 1 to 2147483647 milliseconds.
<i>timer_type</i>	Type of timer; valid values are join , leave , and leaveall .				
<i>timer_value</i>	Timer values in milliseconds; valid values are from 1 to 2147483647 milliseconds.				
Defaults	The default is the join timer is 200 ms, the leave timer is 600 ms, and the leaveall timer is 10000 ms.				
Command Types	Switch command.				
Command Modes	Privileged.				
Usage Guidelines	<p>You must maintain the following <i>relationship</i> for the various timer values:</p> <ul style="list-style-type: none"> • Leave time must be greater than or equal to three times the join time. • Leaveall time must be greater than the leave time. 				
 Caution	Set the same GARP application (for example, GMRP and GVRP) timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP applications will not operate successfully.				
 Note	The modified timer values are applied to all GARP application (for example, GMRP and GVRP) timer values.				

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 20000 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)
```

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	enable	Keyword to enable IGMP snooping on the switch.
	disable	Keyword to disable IGMP snooping on the switch.

Defaults The default is IGMP snooping is enabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines IGMP must be disabled to run GMRP.

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

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

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

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

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

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

Related Commands

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

set igmp fastleave

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

set igmp fastleave { enable | disable }

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

Defaults The default is disabled.

Command Types Switch command.

Command Modes Privileged.

Examples This command shows how to enable IGMP fastleave processing:

```
Console> (enable) set igmp fastleave enable
IGMP fastleave set to enable.
Warning: Can cause disconnectivity if there are more than one host joining the same group
per access port.
Console> (enable)
```

This command shows how to disable IGMP fastleave processing:

```
Console> (enable) set igmp fastleave disable
IGMP fastleave set to disable.
Console> (enable)
```

Related Commands

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

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 inlinepower defaultallocation

Use the **set inlinepower defaultallocation** command to set the default power allocation for a port.

set inlinepower defaultallocation *value*

Syntax Description	<i>value</i> Default power allocation; valid values are from 2000 to 12500 mW.
---------------------------	--------------------------------------------------------------------------------

Defaults	The default is 7000 mW.
-----------------	-------------------------

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

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

Examples	<p>This example shows how to set the default power allocation to 2000 mW:</p> <pre>Console> (enable) set inlinepower defaultallocation 2000 Default inline power allocation set to 9500 mWatt per applicable port. Console> (enable)</pre>
-----------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Related Commands	show environment power show port inlinepower
-------------------------	---------------------------------------------------------------

set interface

Use the **set interface** command set to configure the in-band and SLIP interfaces on the switch.

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

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

```
set interface sl0 slip_addr dest_addr
```

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

Syntax Description		
sc0	Keyword to specify the in-band interface.	
sl0	Keyword to specify the SLIP interface.	
up	Keyword to bring the interface into operation.	
down	Keyword 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.	
<i>/netmask</i>	(Optional) Subnet mask.	
<i>broadcast</i>	(Optional) Broadcast address.	
<i>slip_addr</i>	IP address of the console port.	
<i>dest_addr</i>	IP address of the host to which the console port will be connected.	
dhcp	Keyword to perform DHCP operations on the sc0 interface.	
renew	Keyword to renew the lease on a DHCP-learned IP address.	
release	Keyword to release a DHCP-learned IP address back to the DHCP IP address pool.	
requestnew	Keyword used to request a new lease on a DHCP-learned IP address.	

Defaults

The default configuration is the in-band interface (sc0) in VLAN 1 with the IP address, subnet mask, and broadcast address set to 0.0.0.0. The default configuration for the SLIP interface (sl0) is that the IP address and broadcast address are set to 0.0.0.0.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

Two configurable network interfaces are on a Catalyst 6000 family switch: in-band (sc0) and SLIP (sl0). Configuring the sc0 interface with an IP address and subnet mask allows you to access the switch CLI via Telnet from a remote host. You should assign the sc0 interface to an active VLAN configured on the switch (the default is VLAN 1). Make sure the IP address you assign is in the same subnet as other stations in that VLAN.

Configuring the `sl0` interface with an IP address and destination address allows you to make a point-to-point connection to a host through the console port. Use the **slip attach** command to activate SLIP on the console port (you will not be able to access the CLI via a terminal connected to the console port until you use the **slip detach** command to deactivate SLIP on the console port).

When you specify the *netmask*, this indicates the number of bits allocated to subnetting in the hostid section of the given Class A, B, or C address. For example, if you enter an IP address for the `sc0` interface as 172.22.20.7, the hostid bits for this Class B address is 16. Any number of bits in the hostid bits can be allocated to the subnet field. If you do not enter the netmask, the number of bits is assumed to be the natural netmask.

The **set interface sc0 dhcp** command is valid only when the address is learned from the DHCP server and available in privileged mode only.

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 192.20.11.44/255.255.255.0
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` through a Telnet session. Note that the default netmask for that IP address class is used (for example, a Class C address uses 255.255.255.0, and a Class B uses 255.255.0.0):

```
Console> (enable) set interface sc0 192.200.11.40
This command may disconnect active telnet sessions.
Do you want to continue (y/n) [n]? y
Interface sc0 IP address set.
```

This example shows how to take the interface out of operation through a Telnet session:

```
Console> (enable) set interface sc0 down
This command will inactivate telnet sessions.
Do you want to continue (y/n) [n]? y
Interface sc0 administratively down.
```

This example shows how to assign the `sc0` interface to a particular VLAN:

```
Console> (enable) set interface sc0 5
Interface sc0 vlan set.
Console> (enable)
```

This example shows what happens when you assign the `sc0` interface to a nonactive VLAN:

```
Console> (enable) set interface sc0 200
Vlan is not active, user needs to set vlan 200 active
Interface sc0 vlan set.
Console> (enable)
```

This example shows how to release a DHCP-learned IP address back to the DHCP IP address pool:

```
Console> (enable) set interface sc0 dhcp release
Releasing IP address...Done
Console> (enable)
```

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

```
Console> (enable) set interface sc0 dhcp renew  
Renewing IP address...Done  
Console> (enable)
```

This example shows how to request a new lease on a DHCP-learned IP address:

```
Console> (enable) set interface sc0 dhcp requestnew  
Requesting new IP address...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 is one IP alias (0.0.0.0) configured as the default.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to define an IP alias of mercury for IP address 192.122.174.234:

```
Console> (enable) set ip alias mercury 192.122.174.234
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}
```

Syntax Description	enable	Keyword to enable DNS.
	disable	Keyword to disable DNS.

Defaults The default is DNS is disabled.

Command Types Switch command.

Command Modes Privileged.

Examples This example shows how to enable DNS:

```
Console> (enable) set ip dns enable  
DNS is enabled.  
Console> (enable)
```

This example shows how to disable DNS:

```
Console> (enable) set ip dns disable  
DNS is disabled.  
Console> (enable)
```

Related Commands **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*

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

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

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

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

Usage Guidelines	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 set ip dns domain command. If you specify a domain name with a trailing dot, the program considers this an <i>absolute</i> domain name.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Examples	This example shows how to set the default DNS domain name:
-----------------	------------------------------------------------------------

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

Related Commands	clear ip dns domain show ip dns
-------------------------	--------------------------------------------------

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]
```

Syntax Description	<table border="1"> <tbody> <tr> <td><i>ip_addr</i></td> <td>IP address of the DNS server.</td> </tr> <tr> <td>primary</td> <td>(Optional) Keyword to configure a DNS server as the primary server.</td> </tr> </tbody> </table>	<i>ip_addr</i>	IP address of the DNS server.	primary	(Optional) Keyword to configure a DNS server as the primary server.
<i>ip_addr</i>	IP address of the DNS server.				
primary	(Optional) Keyword to configure a DNS server as the primary server.				
Defaults	This command has no default setting.				
Command Types	Switch command.				
Command Modes	Privileged.				
Usage Guidelines	<p>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.</p> <p>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.</p>				
Examples	<p>These examples show how to set the IP address of a DNS server:</p> <pre>Console> (enable) set ip dns server 198.92.30.32 198.92.30.32 added to DNS server table as primary server.</pre> <pre>Console> (enable) set ip dns server 171.69.2.132 primary 171.69.2.132 added to DNS server table as primary server.</pre> <pre>Console> (enable) set ip dns server 171.69.2.143 primary 171.69.2.143 added to DNS server table as primary server.</pre> <p>This example shows what happens if you enter more than three DNS name servers as backup:</p> <pre>Console> (enable) set ip dns server 161.44.128.70 DNS server table is full. 161.44.128.70 not added to DNS server table.</pre>				
Related Commands	<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	enable	disable
	Keyword to permit fragmentation for IP packets bridged between FDDI and Ethernet networks.	Keyword 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, packets are dropped.

Examples This example shows how to disable IP fragmentation:

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

Related Commands **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 { default | port-num }
```

Syntax Description	default	Keyword to specify the default HTTP server port number (80).
	<i>port-num</i>	Number of the TCP port for the HTTP server; valid values are from 1 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	enable Keyword to enable the HTTP server.
	disable Keyword to disable 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 enabled 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	set ip http port show ip http
-------------------------	------------------------------------------------

set ip permit

Use the **set ip permit** command set 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]
```

Syntax Description		
enable	Keyword to enable the IP permit list.	
disable	Keyword to disable the IP permit list.	
telnet	(Optional) Keyword to specify removal from the Telnet IP permit list.	
snmp	(Optional) Keyword to specify removal from the SNMP IP permit list.	
all	Keyword to specify all entries in the IP permit list be removed.	
<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.	

Defaults The default is IP permit list is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines The same functionality of the IP permit list can be achieved by using VACLs. VACLs are handled by hardware (PFC) and the processing is considerably faster. For VACL configuration information, refer to the *Catalyst 6000 Family Multilayer Switch Feature Card and Policy Feature Card Configuration Guide*.

You can configure up to 100 entries in the permit list. If you enable the IP permit list, 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 you do not specify the **snmp**, **telnet**, or **all** keyword, 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 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 on the Catalyst 6000 family switches.

set ip redirect {enable | disable}

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

Defaults The default configuration is ICMP redirect is 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 {destination}/[netmask] {gateway} [metric] [primary]
```

Syntax Description	
<i>destination</i>	IP address, IP alias of the network, or specific host to be added. Use default as the destination to set the new entry as the default route.
<i>/netmask</i>	(Optional) Number of bits in netmask or dot format (for example, 172.20.22.7/24 or 172.20.22.7/255.255.255.0).
<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.
primary	(Optional) Keyword used with the Multiple IP Gateways feature to specify the default IP gateway with the highest priority.

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. The **primary** is the highest priority. If you do not designate a primary gateway, priority is based on the order of input. If you enter two primary definitions, the second definition becomes the primary and the first definition is now the secondary default IP gateway.

You can only specify the **primary** keyword for a default route.

When you enter the *destination* or *gateway*, enter it in dot notation, for example, a.b.c.d.

When you specify the *netmask*, this indicates the number of bits allocated to subnetting in the hostid section of the given Class A, B, or C address. For example, if you enter an IP address for the sc0 interface as 172.22.20.7, the hostid bits for this Class B address is 16. Any number of bits in the hostid bits can be allocated to the netmask field. If you do not enter the *netmask*, the number of bits is assumed to be the natural netmask.

When you enter the netmask, enter it as the number of bits or dot format, for example, **destination/24** or **destination/255.255.255.0**. If you enter the netmask in dot format, you must have contiguous 1s.

Examples

These examples show how to add three default routes to the IP routing table, checking after each addition using the **show ip route** command:

```
Console> (enable) set ip route default 192.122.173.42 1 primary
Route added.
Console> (enable)
```

```
Console> (enable) show ip route
Fragmentation  Redirect  Unreachable
-----
enabled        enabled   enabled
Destination    Gateway      Flags    Use      Interface
-----
default        192.122.173.42  UG      59444   sc0
192.22.74.0    192.22.74.223  U        5       sc0
```

```
Console> (enable) set ip route default 192.122.173.43 1
Route added.
Console> (enable)
```

```
Console> (enable) show ip route
Fragmentation  Redirect  Unreachable
-----
enabled        enabled   enabled
Destination    Gateway      Flags    Use      Interface
-----
default        192.122.173.43  UG      59444   sc0
default        192.122.173.42  UG      59444   sc0
192.22.74.0    192.22.74.223  U        5       sc0
```

```
Console> (enable) set ip route default 192.122.173.44 1
Route added.
Console> (enable)
```

```
Console> (enable) show ip route
Fragmentation  Redirect  Unreachable
-----
enabled        enabled   enabled
Destination    Gateway      Flags    Use      Interface
-----
default        192.122.173.44  UG      59444   sc0
default        192.122.173.43  UG      59444   sc0
default        192.122.173.42  UG      59444   sc0
192.22.74.0    192.22.74.223  U        5       sc0
```

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 Catalyst 6000 family switch.

set ip unreachable { enable | disable }

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

Defaults The default is ICMP unreachable messages is 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 a 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)
```

Related Commands **show ip route**

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**
- show kerberos**

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 user TGTs as they authenticate from the switch to Kerberized remote hosts on the network by using Kerberized Telnet.

Examples This example shows how to enable Kerberos credentials forwarding:

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

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

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
```

Syntax Description	<i>kerberos_realm</i> IP address or name (in uppercase characters) of the Kerberos realm.
Defaults	The default value is a NULL string.
Command Types	Switch command.
Command Modes	Privileged.
Usage Guidelines	<p>To authenticate a user defined in the Kerberos database, you must configure the switch to know the host name or IP address of the host running the KDC and the name of the Kerberos realm.</p> <p>You must enter Kerberos realms in uppercase characters.</p>
Examples	<p>This example shows how to set a default Kerberos local realm for the switch:</p> <pre>Console> (enable) set kerberos local-realm CISCO.COM Kerberos local realm for this switch set to CISCO.COM. Console> (enable)</pre>
Related Commands	<pre>set kerberos realm clear kerberos realm show kerberos</pre>

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 host 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 You can map the name of the Kerberos realm to a DNS domain name or a host name by entering the **set kerberos realm** 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.

You must enter Kerberos realms in uppercase characters.

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**
- show kerberos**

set kerberos server

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

```
set kerberos server kerberos_realm {hostname | ip_address} [port]
```

Syntax Description	<table border="1"> <tr> <td><i>kerberos_realm</i></td> <td>Keyword specifying Kerberos realm.</td> </tr> <tr> <td><i>hostname</i></td> <td>Name of host running the KDC.</td> </tr> <tr> <td><i>ip_address</i></td> <td>IP address of host running the KDC.</td> </tr> <tr> <td><i>port</i></td> <td>(Optional) Number of the port.</td> </tr> </table>	<i>kerberos_realm</i>	Keyword specifying Kerberos realm.	<i>hostname</i>	Name of host running the KDC.	<i>ip_address</i>	IP address of host running the KDC.	<i>port</i>	(Optional) Number of the port.
<i>kerberos_realm</i>	Keyword specifying Kerberos realm.								
<i>hostname</i>	Name of host running the KDC.								
<i>ip_address</i>	IP address of host running the KDC.								
<i>port</i>	(Optional) Number of the port.								
Defaults	This command has no default setting.								
Command Types	Switch command.								
Command Modes	Privileged.								
Usage Guidelines	<p>You can specify to the switch which 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.</p> <p>The KDC is a Kerberos server and database program running on a network host that allocates the Kerberos credentials to different users or network services.</p>								
Examples	<p>This example shows how to specify the Kerberos server:</p> <pre>Console> (enable) set kerberos server CISCO.COM 187.0.2.1 750 Kerberos Realm-Server-Port entry set to:CISCO.COM - 187.0.2.1 - 750 Console> (enable)</pre>								
Related Commands	<pre>set kerberos server clear kerberos server show kerberos</pre>								

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.

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.

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 table size is 20 entries.

The KDC is a Kerberos server and database program running on a network host that allocates the Kerberos credentials to different users or network services.

The key is encrypted with the private DES key when you copy the configuration to a file or enter the **show config** command.

Examples

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

```
Console> (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

clear kerberos clients mandatory
show kerberos

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 KDC is a Kerberos server and database program running on a network host that allocates the Kerberos credentials to different users or network services.

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 TFTP.

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

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

Related Commands

- set kerberos srvtab entry**
- clear kerberos creds**
- show kerberos**

set key config-key

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

set key config-key *string*

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

set lcperroraction

Use the **set lcperroraction** command to configure how your system handles LCP errors when a module reports an ASIC problem to the NMP.

set lcperroraction *action*

Syntax Description	<i>action</i>	Action for handling LCP errors. See “Usage Guidelines” for more information about valid values for action levels.
---------------------------	---------------	-------------------------------------------------------------------------------------------------------------------

Defaults	The default is that the action level is set to ignore .
-----------------	----------------------------------------------------------------

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

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

Usage Guidelines	<p>Valid values for action levels are as follows:</p> <ul style="list-style-type: none"> • operator—The system displays a recommended action for you to take. The system also logs the LCP error. • system—The system automatically takes an action to handle the LCP error. The system also logs the LCP error. • ignore—No action is taken. The system only logs the LCP error.
-------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Note	Be careful when using the system value because the switch automatically takes action, including possibly resetting or power cycling modules.
-------------	-----------------------------------------------------------------------------------------------------------------------------------------------------

Examples	This example shows how to set the action that handles an LCP error:
-----------------	---------------------------------------------------------------------

```
Console> (enable) set lcperroraction ignore
Console> (enable)
```

Related Commands	show lcperroraction
-------------------------	----------------------------

set lda

Use the **set lda** command set to configure the ASLB information on the Catalyst 6000 family switch.

set lda enable | disable

set lda vip {*server_virtual_ip*} {*destination_tcp_port*} [{*server_virtual_ip*}
{*destination_tcp_port*}] ...

set lda mac ld {*ld_mac_address*}

set lda mac router {*mac_address*}...

set lda router {*router_vlan*} {*ld_mod/port*} [*backup_ld_mod/port*]

set lda server {*server_vlan*} {*ld_mod/port*} [*backup_ld_mod/port*]

set lda udpage {*udpagetime*}

Syntax Description		
enable disable		Keyword to enable or disable the ASLB feature.
vip <i>server_virtual_ip</i> <i>destination_tcp_port</i>		Keyword and variables to specify the virtual IP address of the server and the number of the destination TCP port that will be accelerated by the switch (up to 1024).
mac ld <i>ld_mac_address</i>		Keyword and variables to specify the LD MAC address.
mac router <i>mac_address...</i>		Keyword and variable to specify the router MAC address.
router <i>router_vlan</i> <i>ld_mod/port</i>		Keyword and variable to specify the router VLAN. Module and port number of the port connected to the LD on the VLAN.
<i>backup_ld_mod/port</i>		(Optional) Module and port number of the port connected to the backup LD.
server <i>server_vlan</i>		Keyword and variable to specify the server VLAN.
udpage <i>udpagetime</i>		Keyword and variable to specify the UDP aging time for LocalDirector acceleration.

Defaults The default is the ASLB is disabled.

Command Types Switch command.

Command Modes Privileged.

Usage Guidelines

You can enter a zero (0) as a wildcard (don't care) digit for the *destination_tcp_port*.

You can enter up to 1024 *server_virtual_ip destination_tcp_port* entries separated by a space.

To cancel a previously entered VIP, use the **clear lda vip** command.

To cancel a previously entered MAC LD or router, use the **clear lda mac** command.

You need to enter the **set lda** commands to provide all the necessary information before using the **commit lda** command to program the setup into hardware.

The information you enter through the **set lda** commands are immediately saved into NVRAM, but you must enter the **commit lda** command for the setting to take effect.

When you disable the ASLB feature, you can enter the **set lda** commands, but the **commit lda** command will fail.

When you enter the **set lda mac router** command, you can enter up to 32 MAC addresses.

You can enter the value zero (0) to disable the **udpage** option. The *udpagingtime* is specified in milliseconds; values are from 0 ms to 2024000 ms.

Examples

This example shows how to enable the ASLB feature:

```
Console> (enable) set lda enable
Successfully enabled Local Director Acceleration.
Console> (enable)
```

This example shows how to disable the ASLB feature:

```
Console> (enable) set lda disable
Disabling Local Director Acceleration....
Successfully disabled Local Director Acceleration.
Console> (enable)
```

This example shows how to specify the virtual IP address:

```
Console> (enable) set lda vip 10.0.0.8 8
Successfully set server virtual ip and port information.
Use commit lda command to save settings to hardware.
Console> (enable)
```

This example shows how to specify the MAC address for the LocalDirector:

```
Console> (enable) set lda mac ld 1-2-3-4-5-6
Successfully set mac address.
Use commit lda command to save settings to hardware.
Console> (enable)
```

This example shows how to specify multiple router MAC addresses:

```
Console> (enable) set lda mac router 1-2-3-4-5-6 3-4-56-67-4-5
Successfully set mac address.
Use commit lda command to save settings to hardware.
Console> (enable)
```

This example shows how to specify the router VLAN:

```
Console> (enable) set lda router 110 4/26
Successfully set router vlan and ld port.
Use commit lda command to save settings to hardware.
Console> (enable)
```

This example shows how to specify the udpage aging time:

```
Console> (enable) set lda udpage 20  
Successfully set LDA UDP aging time to 20ms.  
Console> (enable)
```

This example shows how to specify the server VLAN:

```
Console> (enable) set lda server 105 4/40  
Successfully set server vlan and LD port.  
Use commit lda command to save settings to hardware.  
Console> (enable)
```

Related Commands

commit lda
show lda
clear lda

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 from 0 to 512.
	default	(Optional) Keyword to set the number of lines in the terminal display screen for the current administration session and all other sessions.

Defaults The default value is 24 lines upon starting a session.

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 you use the **default** keyword, a change to the terminal length value applies only to the current session.

When you change the value in a session, it applies only to that session. When you use the **clear config** command, the number of lines in the terminal display screen is reset to the factory-set default of 100.

The **default** keyword is available in privileged mode only.

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 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	Keyword to enable system message logging to the console.
	disable	Keyword to disable system message logging to the console.

Defaults The default is 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**

set logging history

Use the **set logging history** command to set the size of the syslog history table.

set logging history *syslog_history_table_size*

Syntax Description	<i>syslog_history_table_size</i> Size of the syslog history table; valid values are from 0 to 500.
---------------------------	----------------------------------------------------------------------------------------------------

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

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

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

Examples	This example shows how to set the size of the syslog history table to 400:
-----------------	----------------------------------------------------------------------------

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

Related Commands	show logging clear logging buffer
-------------------------	----------------------------------------------------

set logging level

Use the **set logging level** command to set the facility and severity level used when logging system messages.

set logging level *facility severity* [**default**]

Syntax Description

<i>facility</i>	Value that specifies the type of system messages to capture; facility types are listed in Table 2-8.
<i>severity</i>	Value that specifies the severity level of system messages to capture; severity level definitions are listed in Table 2-9.
default	(Optional) Keyword to cause the specified logging level to apply to all sessions.

Table 2-8 Facility Types

Facility Name	Definition
all	All facilities
acl	ACL facility
cdp	Cisco Discovery Protocol
dtp	Dynamic Trunking Protocol
drip	DRIP facility
earl	Enhanced Address Recognition Logic
fddi	FDDI facility
gvrp	GARP VLAN Registration Protocol
ip	Internet Protocol
kernel	Kernel
ld	ASLB facility
mcast	Multicast
mgmt	Management
mls	Multilayer Switching
pagp	Port Aggregation Protocol
protfilt	Protocol Filter
pruning	VTP pruning
privatevlan	Private VLAN facility
radius	Remote Access Dial-In User Service
security	Security
snmp	Simple Network Management Protocol

Table 2-8 Facility Types (continued)

Facility Name	Definition
spantree	Spanning Tree Protocol
sys	System
tac	Terminal Access Controller
tcp	Transmission Control Protocol
telnet	Terminal Emulation Protocol
tftp	Trivial File Transfer Protocol
udld	User Datagram Protocol
vtp	Virtual Terminal Protocol

Table 2-9 Severity Level Definitions

Severity Level	Description
0—emergencies	System unusable
1—alerts	Immediate action required
2—critical	Critical condition
3—errors	Error conditions
4—warnings	Warning conditions
5—notifications	Normal bug significant condition
6—informational	Informational messages
7—debugging	Debugging messages

Defaults

The default is *facility* is set to **all**, and *level* is set to **0**.

Command Types

Switch command.

Command Modes

Privileged.

Usage Guidelines

You can also set the logging level by using the **set logging server** command.

If you do not use the **default** keyword, the specified logging level applies only to the current session.

Examples

This example shows how to set the default facility and severity level for system message logging:

```
Console> (enable) set logging level snmp 2 default  
System logging facility <snmp> set to severity 2(critical).  
Console> (enable)
```

Related Commands

show logging
show logging buffer

set logging server

Use the **set logging server** command set to enable and disable system message logging to configured syslog servers and to add a syslog server to the system logging server table.

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

set logging server *ip_addr*

set logging server *facility severity*

set logging server severity *severity*

set logging server *facility*

Syntax Description	enable	disable	<i>ip_addr</i>	severity <i>severity</i>	<i>facility</i>
	Keyword to enable system message logging to configured syslog servers.	Keyword to disable system message logging to configured syslog servers.	IP address of the syslog server to be added to the configuration.	Keyword and variable to globally set the syslog maximum severity control for all message types; severity level definitions are listed in Table 2-9.	Type of system messages to capture; server facility types are listed in Table 2-10.

Table 2-10 Server Facility Types

Severity Level	Description
local 0	Server facility local 0
local 1	Server facility local 1
local 2	Server facility local 2
local 3	Server facility local 3
local 4	Server facility local 4
local 5	Server facility local 5
local 6	Server facility local 6
local 7	Server facility local 7
syslog	syslog facility

Defaults

The default is no syslog servers are configured to receive system messages.

Command Types

Switch command.

Command Modes Privileged.

Usage Guidelines You can also set the logging level by using the **set logging level** command. If you do not enter the facility or server keywords, the parameter is applied to all levels.

Severity logging to a configured syslog server depends on the configuration set by **set logging level** command. The server severity level must be greater than or equal to the default severity level of those message facility that you expect to receive in syslog messages on the syslog server.

An IP alias or a host name that can be resolved through DNS can also be used.

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

```
Console> (enable) set logging server enable
System logging messages will be sent to the configured syslog servers.
Console> (enable)
```

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

```
Console> (enable) set logging server disable
System logging messages will not be sent to the configured syslog servers.
Console> (enable)
```

This example shows how to add a server to the system logging server table using its IP address:

```
Console> (enable) set logging server 171.69.192.205
171.69.192.205 added to the System logging server table.
Console> (enable)
```

This example shows how to globally set the syslog maximum severity control for all message types:

```
Console> (enable) set logging server severity 4
System logging server severity set to 4(warnings).
Console> (enable)
```

Related Commands **clear logging server**
show logging

■ set logging server