

set enablepass

To change the privileged (enable) mode password on the switch, use the **set enablepass** command.

set enablepass

Syntax Description This command has no arguments or keywords.

Defaults No enable password is configured.

Command Types Switch command

Command Modes Privileged

Usage Guidelines Passwords are case sensitive; they may be 0 to 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 errdisable-timeout

To configure a timeout for ports in errdisable state so as to automatically reenable them, use the **set errdisable-timeout** command.

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

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

Syntax Description

enable	Enables errdisable timeout.
disable	Disables errdisable timeout.
<i>reason</i>	Reason for the port being in the errdisable state; valid values are bcast-suppression , bpdu-guard , channel-misconfig , cross-fallback , duplex-mismatch , gl2pt-ingress-loop , gl2pt-threshold-exc , udld , other , and all .
interval <i>interval</i>	Timeout interval; valid values are from 30 to 86,400 seconds (from 1/2 of a minute to 24 hours).

Defaults

The default settings are as follows:

- All errdisable reasons are globally disabled (timer stops whenever there are no reasons enabled).
- Timeout is set to **disable**.
- *Interval* is set at 300 seconds.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

These events can set a port to errdisable state:

- Channel misconfiguration
- Duplex mismatch
- BPDU port-guard
- UDLD
- Other

Ports that are in an errdisable state due to a cause other than a channel misconfiguration, duplex mismatch, BPDU port-guard, or UDLD will have an errdisable cause of **other**. If you specify **other for the reason variable**, the ports are in an errdisable timeout state.

Examples

This example shows how to enable an errdisable timeout due to a BPDU port-guard event:

```
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

To enable or disable detection of various errors, use the **set errordetection** command.

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

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

Syntax Description	inband	In-band error detection.
	enable	Enables the specified error detection.
	disable	Disables the specified error detection.
	memory	Memory error detection.

Defaults

The default settings are as follows:

- Error detection is disabled for **memory**.
- Error detection is disabled for **inband**.

Command Types

Switch command

Command Modes

Privileged

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

To enable or disable the Multiple Default Gateway (MDG) feature, use the **set feature mdg** command.

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

Syntax Description	enable Enables the multiple default gateway feature on the switch. disable Disables the multiple default gateway feature on the switch.
Defaults	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	<p>This example shows how to enable the MDG feature:</p> <pre>Console> (enable) set feature mdg enable Multiple Default Gateway feature enabled. Console> (enable)</pre> <p>This example shows how to disable the MDG feature:</p> <pre>Console> (enable) set feature mdg disable Multiple Default Gateway feature disabled. Console> (enable)</pre>

set garp timer

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

set garp 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 value, in milliseconds; valid values are from 1 to 2147483647 milliseconds.

Defaults The default settings are as follows:

- **join** is 200 ms
- **leave** is 600 ms
- **leaveall** is 10000 ms

Command Types Switch command

Command Modes Privileged

Usage Guidelines You must maintain the following initial relationships for the various timer values:

- Leave time must be greater than twice the join time
- Leaveall time must be greater than the 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)
```

```
set gmrp timer
set gvrp timer
show gmrp configuration
show gvrp configuration
```

set gmrp

To enable or disable GARP Multicast Registration Protocol (GMRP) on the switch in all VLANs on all ports, use the **set gmrp** command.

set gmrp { enable | disable }

Syntax Description	enable	Disables GMRP on the switch.
	disable	Enables GMRP on the switch.

Defaults 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

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

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

Syntax Description	enable	enable
	enable	Enables GARP Multicast Registration Protocol (GMRP) Forward All on a specified port.
	disable	Disables GMRP Forward All on a specified port.
	mod/port...	Module number and port number list.

Defaults The Forward All option is disabled on 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

To specify the GARP Multicast Registration Protocol (GMRP) registration type, use the **set gmrp registration** command.

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

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

Defaults Normal registration is enabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines If you enter a *registration-type* of **Normal**, dynamic creation, registration, and deregistration of VLANs are 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 are 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 are 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

To set values for the join, leave, and leaveall timers, use the **set gmrp timer** command.

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 value, in milliseconds; valid values are from 1 to 2147483647 milliseconds.

Defaults The default settings are as follows:

- **join** is 200 ms
- **leave** is 600 ms
- **leaveall** is 10000 ms

Command Types Switch command

Command Modes Privileged

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

- Leave time must be greater than twice the join time
- Leaveall time must be greater than the 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 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)
```

■ set gmrp timer

Related Commands

[set garp timer](#)
[set gvrp timer](#)
[show gmrp timer](#)

set gvrp

To enable or disable GARP VLAN Registration Protocol (GVRP) globally on the switch, use the **set gvrp** command.

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

Syntax Description	enable	Disables GVRP on the switch.
	disable	Enables GVRP on the switch.

Defaults 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

- [set garp timer](#)
- [set gvrp timer](#)
- [show gvrp configuration](#)
- [show gvrp statistics](#)

set gvrp applicant

To specify if a VLAN is declared out of blocking ports, use the **set gvrp applicant** command.

set gvrp applicant {**Normal** | **active**} *mod/port...*

Syntax Description	Normal	Disallows the declaration of any VLAN out of blocking ports.
	active	Allows the declaration of active VLANs out of blocking ports.
	<i>mod/port...</i>	Module number and port number list.

Defaults The GVRP applicant is 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 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

To enable or disable GARP VLAN Registration Protocol (GVRP) dynamic VLAN creation, use the **set gvrp dynamic-vlan-creation** command.

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

Syntax Description

enable	Enables dynamic VLAN creation.
disable	Disables dynamic VLAN creation.

Defaults

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

To set the administrative control of an outbound port, use the **set gvrp registration** command.

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

Syntax Description	Normal	Allows dynamic registering and deregistering each VLAN (except VLAN 1) on the port.
	fixed	Supports manual VLAN creation and registration, prevents VLAN deregistration, and registers all VLANs known to other ports.
	forbidden	All the VLANs (except VLAN 1) are statically deregistered from the port.
	<i>mod/port...</i>	Module number and port number list.

Defaults Administrative control is set to Normal.

Command Types Switch command

Command Modes Privileged

Usage Guidelines GVRP registration commands are entered on a per-port basis and apply to all VLANs on the trunk. When you set VLAN registration, you are indicating to the switch that the VLAN is available for users to connect to this port and that 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 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)
```

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

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

```
set gvrp 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 value, in milliseconds; valid values are from 1 to 2,147,483,647 milliseconds.

Defaults The default settings are as follows:

- **join** is 200 ms
- **leave** is 600 ms
- **leaveall** is 10000 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 relationships for the various timer values:

- Leave time must be greater than twice the join time
- Leaveall time must be greater than the 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)
```

Related Commands

[set garp timer](#)
[show gvrp configuration](#)

set igmp filter

To enable IGMP multicast filtering on the switch, use the **set igmp filter** command.

```
set igmp filter enable
```

```
set igmp filter disable
```

To create an IGMP multicast filter profile by adding a multicast IP address or a range of IP addresses, use the **set igmp filter profile** command.

```
set igmp filter profile profile_id ip_addr [- ip_addr]
```

To allow an address or a range of addresses to be accepted or denied by the an IGMP filter profile on the switch, use the **set igmp filter profile *profile_id* match-action** command.

```
set igmp filter profile profile_id match-action permit
```

```
set igmp filter profile profile_id match-action deny
```

To associate a port or list of ports to an IGMP multicast filter profile, use the **set igmp filter map** command.

```
set igmp filter map profile_id port_list
```

Syntax Description

enable	Enables IGMP multicast filtering.
disable	Disables IGMP multicast filtering.
<i>profile_id</i>	Arbitrary number assigned to a profile.
<i>ip_addr</i>	Address of the IP; can be 1 or a range.
permit	Allows an address or range of addresses to be accepted by an IGMP filter profile.
deny	Prevents an address or range of addresses from being accepted by an IGMP filter profile.
<i>port_list</i>	Module/port value or range of values.

Defaults

The default settings are as follows:

- IGMP multicast filter feature is disabled.
- IGMP multicast filter feature does not filter.
- IGMP multicast filter feature denies IGMP filter match-action.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

The switch administrator configures IGMP traffic filtering using CLI and SNMP interfaces.

Examples

This example shows how to enable IGMP multicast filtering on a switch.

```
Console> (enable) set igmp filter enable  
igmp filter set to enable  
Console> (enable)
```

This example shows how to disable IGMP multicast filtering on a switch.

```
Console> (enable) set igmp filter disable  
igmp filter set to disable  
Console> (enable)
```

This example shows how to create IGMP multicast filter profile 1 by adding a multicast IP address 226.1.1.1.

```
Console> (enable) set igmp filter profile 1 226.1.1.1  
Successfully add ip(s) to profile  
Console> (enable)
```

This example shows how to accept an address, or range of addresses, by an IGMP multicast filter profile on the switch.

```
Console> (enable) set igmp filter profile 1 match-action permit  
igmp filter match-action set to permit  
Console> (enable)
```

This example shows how to deny an address, or range of addresses, by an IGMP multicast filter profile on the switch.

```
Console> (enable) set igmp filter profile 1 match-action deny  
igmp filter match-action set to deny  
Console> (enable)
```

This example shows how to associate module 2/port 1 to IGMP multicast filter profile 1.

```
Console> (enable) set igmp filter map 1 2/1  
Console> (enable)
```

Related Commands

[show igmp filter](#)
[clear igmp filter](#)

set inlinepower defaultallocation

To set the default power allocation for a port, use the **set inlinepower defaultallocation** command.

set inlinepower defaultallocation *value*

Syntax Description	<i>value</i> Default power allocation; valid values are from 2000 to 15300 mW.
---------------------------	--

Defaults	10000 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	<p>show environment show port inlinepower</p>
-------------------------	--

set interface

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

```

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		
sc0		In-band management interface.
me1		Out-of-band management Ethernet interface.
sl0		SLIP interface.
up		Brings the interface into operation.
down		Takes 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.
dhcp		Performs DHCP operations on the sc0 interface.
renew		Renews the lease on a DHCP-learned IP address.
release		Releases a DHCP-learned IP address back to the DHCP IP address pool.

Defaults

The default settings for the in-band management interface (sc0) and the out-of-band management Ethernet interface (me1) are as follows:

- IP address, subnet mask, and broadcast address set to 0.0.0.0.
- The sc0 interface is in VLAN 1.

The default settings for the SLIP interface (sl0) are as follows:

- 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 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 4000 family 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 transmitting and receiving 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 sl0 interface:

```
Console> (enable) set interface sl0 10.1.1.1 10.1.1.2
Interface sl0 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

[set interface trap](#)
[show interface—switch](#)
[slip](#)

set interface trap

To enable or disable SNMP link-up or link-down traps on the switch interfaces, use the **set interface trap** command.

```
set interface trap {sc0 | me1 | sl0} {enable | disable}
```

Syntax Description	Parameter	Description
	sc0	In-band management interface.
	me1	Out-of-band management Ethernet interface.
	sl0	SLIP interface.
	enable	Enables the SNMP link up/down traps on the specified interface.
	disable	Disables the SNMP link up/down traps on the specified interface.

Defaults SNMP link-up or link-down traps are disabled on all interfaces.

Command Types Switch command

Command Modes Privileged

Examples This example shows how to enable SNMP link-up or link-down traps on the sc0 interface:

```
Console> (enable) set interface trap sc0 enable
Interface sc0 up/down trap enabled.
Console> (enable)
```

This example shows how to disable SNMP link-up or link-down traps on the sc0 interface:

```
Console> (enable) set interface trap sc0 disable
Interface sc0 up/down trap disabled.
Console> (enable)
```

Related Commands [set interface](#)
[show interface—switch](#)
[slip](#)

set ip alias

To add aliases of IP addresses, use the **set ip alias** command.

```
set ip alias name ip_addr
```

Syntax Description	<i>name</i>	Name for the alias you are defining.
	<i>ip_addr</i>	IP address of the alias you are defining.

Defaults The IP alias named default is 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

To enable or disable DNS, use the **set ip dns** command.

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

Syntax Description

enable	Enables DNS.
disable	Disables DNS.

Defaults

Disabled

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

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.

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

To set the default DNS domain name, use the **set ip dns domain** command.

```
set ip dns domain name
```

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

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

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 period, the program considers this an absolute domain name.
-------------------------	---

Examples	This example shows how to set the default DNS domain name as yow.com:
-----------------	---

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

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

set ip dns server

To set the IP address of a DNS server, use the **set ip dns server** command.

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

Syntax Description	
<i>ip_addr</i>	IP address of the DNS server.
primary	(Optional) Configures a DNS server as the primary server.

Defaults This command has no default settings.

Command Types Switch command

Command Modes Privileged

Usage Guidelines 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.

Examples These examples show how to set the IP address of a DNS server:

```
Console> (enable) set ip dns server 198.92.30.32
198.92.30.32 added to DNS server table as primary server.
Console> (enable)
```

```
Console> (enable) set ip dns server 171.69.2.132 primary
171.69.2.132 added to DNS server table as primary server.
Console> (enable)
```

```
Console> (enable) set ip dns server 171.69.2.143 primary
171.69.2.143 added to DNS server table as primary server.
Console> (enable)
```

This example shows what happens if you enter more than three DNS name servers as backup:

```
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.
Console> (enable)
```

Related Commands [clear ip dns server](#)
[show ip dns](#)

set ip fragmentation

To enable or disable the fragmentation of IP packets bridged between FDDI and Ethernet networks, use the **set ip fragmentation** command.

set ip fragmentation {enable | disable}

Syntax Description	enable	disable
	Enables fragmentation for IP packets bridged between FDDI and Ethernet networks.	Disables fragmentation for IP packets bridged between FDDI and Ethernet networks.

Defaults 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.



Note

FDDI and Ethernet networks have different maximum transmission units (MTUs).

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 ip route—switch](#)

set ip http port

To configure the TCP port number for the HTTP server, use the **set ip http port** command.

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

Syntax Description	<i>port</i>	TCP port number; valid values are from 1 to 65535.
	default <i>port</i>	(Optional) TCP default port number; valid values are from 80 to 65535.

Defaults The 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

To enable or disable the HTTP server, use the **set ip http server** command.

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

Syntax Description	enable Enables the HTTP server.
	disable Disables the HTTP server.

Defaults	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	set ip http port show ip http
-------------------------	--

set ip permit

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

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

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

Syntax Description

enable	Enables the IP permit list.
disable	Disables the IP permit list.
telnet	(Optional) Telnet IP permit list.
ssh	(Optional) SSH permit list.
snmp	(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.
all	(Optional) All entries in the IP permit list.

Defaults

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 is displayed on the screen.

Ensure 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 **telnet**, **ssh**, **snmp**, or **all** variables are 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

To enable or disable Internet Control Message Protocol (ICMP) redirect messages, use the **set ip redirect** command.

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

Syntax Description	enable	Permits ICMP redirect messages to be returned to the source host.
	disable	Prevents ICMP redirect messages from being returned to the source host.

Defaults 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—switch](#)
[show netstat](#)

set ip route—ROM monitor

To set the default IP address or alias to the IP routing table, use the **set ip route** command.

```
set ip route default {ip_addr}
```

Syntax Description	default	Entry as a default route.
	<i>ip_addr</i>	IP address of the router.

Defaults This command has no default settings.

Command Types ROM monitor command

Command Modes Normal

Examples This example shows how to add the default route to the routing table:

```
rommon 1 > set ip route default 172.20.52.35  
rommon 2 >
```

Related Commands [clear ip route—ROM monitor](#)
[show ip route—ROM monitor](#)

set ip route—switch

To add IP addresses or aliases to the IP routing table, use the **set ip route** command.

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

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

Syntax Description

default	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.
primary	(Optional) 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

After sc0 is configured, the local network is routed through the sc0 interface with metric 0.

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 gateway 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 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—switch](#)
[show ip route—switch](#)

set ip unreachable

To enable or disable ICMP unreachable messages on the switch, use the **set ip unreachable** command.

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

Syntax Description	enable	Allows IP unreachable messages to be returned to the source host.
	disable	Prevents IP unreachable messages from being returned to the source host.

Defaults 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

To use Kerberos client authentication to validate other services on the network, use the **set kerberos clients mandatory** command.

set kerberos clients mandatory

Syntax Description This command has no arguments or keywords.

Defaults Kerberos clients is not 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 [clear kerberos clients mandatory](#)
[set kerberos credentials forward](#)
[show kerberos](#)

set kerberos credentials forward

To configure clients to forward a user's credentials as the user connects to other hosts in the Kerberos realm, use the **set kerberos credentials forward** command.

set kerberos credentials forward

Syntax Description This command has no arguments or keywords.

Defaults Forwarding is disabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines A user authenticated to a switch configured for kerberos encryption 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 remote hosts configured for kerberos encrypting the network when using similarly configured Telnet sessions.

Examples This example shows how to enable Kerberos credentials forwarding:

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

Related Commands

- [clear kerberos credentials forward](#)
- [set kerberos clients mandatory](#)
- [show kerberos](#)
- [show kerberos creds](#)

set kerberos local-realm

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

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

Syntax Description

kerberos_realm IP address or name of the Kerberos realm.

Defaults

Kerberos database contains a NULL string.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

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 Name System (DNS) domain to the Kerberos realm.

You must use uppercase characters for the `kerberos_realm` variable.

Examples

This example shows how to set CISCO.COM as the default Kerberos local realm for the switch:

```
kerberos> (enable) set kerberos local-realm CISCO.COM
Kerberos local realm for this switch set to CISCO.COM.
aspen-kerberos> (enable)
```

Related Commands

[clear kerberos realm](#)
[set kerberos realm](#)
[show kerberos](#)

set kerberos realm

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

```
set kerberos realm {dns-domain | host} kerberos_realm
```

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

Defaults This command has no default settings.

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 using 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.

You must use uppercase characters for the `kerberos_realm` variable.

Examples This example shows how to map the Kerberos realm CISCO.COM to the CISCO domain name:

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

Related Commands

- [clear kerberos realm](#)
- [set kerberos local-realm](#)
- [show kerberos](#)

set kerberos server

To specify which Key Distribution Center (KDC) to use on the switch, use the **set kerberos server** command.

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

Syntax Description

<i>kerberos_realm</i>	Name of the Kerberos realm.
<i>hostname</i>	Name of host running the KDC.
<i>ip_address</i>	IP address of host running the KDC.
<i>port_number</i>	(Optional) Number of the port.

Defaults

This command has no default settings.

Command Types

Switch command

Command Modes

Privileged

Usage Guidelines

You can specify to the switch which KDC to use in a Kerberos realm. Optionally, you can also specify which port number the KDC monitors. 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.

You must use uppercase characters for the `kerberos_realm` variable.

Examples

This example shows how to specify the Kerberos server:

```
kerberos> (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
kerberos> (enable)
```

Related Commands

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

set kerberos srvtab entry

To enter the SRVTAB file from the command line, use the **set kerberos srvtab entry** command.

```
set kerberos srvtab entry {kerberos_principal} {principal_type} {timestamp} {key_version}
{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</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 Key Distribution Center (KDC). This key is encrypted with the private DES key when you copy the configuration to a file or enter the show config command.

Defaults

This command has no default settings.

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
kerberos> (enable)
```

Related Commands

[clear kerberos srvtab entry](#)
[set kerberos srvtab remote](#)
[show kerberos](#)

set kerberos srvtab remote

To provide the switch with a copy of the SRVTAB file from the Key Distribution Center (KDC) that contains the secret key, use the **set kerberos srvtab remote** command.

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 settings.

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 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](#)
[show kerberos](#)

set key config-key

To define a private DES key for the switch, use the **set key config-key** command.

```
set key config-key string
```

Syntax Description	<i>string</i> DES key for switch; cannot exceed eight bytes.
---------------------------	--

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

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

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

Usage Guidelines	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 show kerberos command is run. The key length can be up to eight characters in length.
-------------------------	--

Examples	This example shows how to define a DES key: <pre>kerberos> (enable) set key config-key abcd Kerberos config key set to abcd kerberos> (enable)</pre>
-----------------	---

Related Commands	clear key config-key
-------------------------	--------------------------------------

set lacp-channel system-priority

To set the priority of the system, use the **set lacp-channel system-priority** command.

set lacp-channel system-priority *value*

Syntax Description	<i>value</i> Number of the priority; valid values are from 1 to 65535.
---------------------------	--

Defaults	System priority is 32768.
-----------------	---------------------------

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

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

Usage Guidelines	Although set lacp-channel system-priority is a global command, the priority is used only for the modules that are running LACP, but the priority is ignored on the modules that are running PAgP. Higher values correspond to lower priority levels.
-------------------------	---

Related Commands	<ul style="list-style-type: none"> clear lacp-channel statistics set channelprotocol set port lacp-channel set spantree channelcost set spantree channelvlancost show lacp-channel show port lacp-channel
-------------------------	--

set length

To configure the number of lines in the terminal display, use the **set length** command.

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

Syntax Description	<i>number</i>	Number of lines to display on the screen; valid values are 0 and from 5 to 512. Specifying zero (0) disables the scrolling feature.
	default	(Optional) Sets the number of lines in the terminal display screen for the current administration session and all other sessions. This keyword is available only in Normal mode.

Defaults The terminal display 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 localuser

To configure the switch to use local user authentication, use the **set localuser** command.

```
set localuser authentication {enable | disable}
```

```
set localuser user username [password pwd] [privilege privilege_level]
```

```
set localuser user password [username]
```

```
set localuser password user [username]
```

Syntax Description		
enable		Enables local user authentication.
disable		Disables local user authentication.
user <i>username</i>		Local user account.
password <i>pwd</i>		(Optional) Local user password.
privilege <i>privilege_level</i>		(Optional) Privilege level; valid values are 0 and 15.

Defaults Local user authentication is disabled.

Command Types Switch command

Command Modes Privileged

Usage Guidelines The privilege level assigned to a username and password combination designates whether a user will be logged in to Normal or Privilege mode after successful authentication. A user with a privilege level of 0 is automatically logged in to Normal mode and a user with a privilege level of 15 is logged in to Privilege mode. A user with a privilege level of 0 can still access Privilege mode by entering the **enable** command and password combination.

You can configure a maximum of twenty-five local user accounts on each switch.

Before you can enable local user authentication you must define at least one local user account.

A username must be less than sixty-five characters in length and can consist of only alphanumeric characters, one of which must be alphabetic.



Note

If you are running a Cisco View image or are logging in using HTTP log in the initial authentication is done using the username and password combination. Privilege mode authentication can be done by either providing the privilege password or using the username and password combination, provided the local user has a privilege level of 15.

Examples

This example shows how to use the create a local user account, including password and privilege level:

```
Console> (enable) set localuser user picard password captain privilege 15  
Added local user picard.  
Console> (enable)
```

This example shows how to enable local user authentication:

```
Console> (enable) set localuser authentication enable  
LocalUser authentication enabled  
Console> (enable)
```

This example shows how to disable local user authentication:

```
Console> (enable) set localuser authentication disable  
LocalUser authentication disabled  
Console> (enable)
```

This example shows you how to reset your own password:

```
Console> (enable) set localuser password  
Enter old password:*****  
Enter new password:*****  
Retype new password:*****  
Password changed.  
Console> (enable)
```

This example shows you, as an administrator, how to reset the password for a user:

```
Console> (enable) set localuser password picard  
Enter new password:*****  
Retype new password:*****  
Password changed.  
Console> (enable)
```

Related Commands

[clear localusers](#)
[show localusers](#)

set logging buffer

To limit the number of system logging messages that are buffered, use the **set logging buffer** command.

set logging buffer *buffer_size*

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

Defaults	500 messages
-----------------	--------------

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

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

Examples	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)
```

Related Commands	clear logging buffer set logging timestamp show logging buffer
-------------------------	--

set logging console

To enable or disable the sending of system logging messages to the console, use the **set logging console** command.

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

Syntax Description	enable	Enables system message logging to the console.
	disable	Disables system message logging to the console.

Defaults	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.  
Console> (enable)
```

Related Commands	set logging level set logging session show logging show logging buffer
-------------------------	---

set logging history

To specify the size and severity level of syslog messages sent to the syslog history table, use the **set logging history** command.

set logging history *history_table_size*

set logging history severity *history_severity_level*

Syntax Description	<i>history_table_size</i>	Size of the syslog history table; valid values are from 0 to 500.
	severity	Sets the syslog history severity level.
	<i>history_severity_level</i>	Severity level; valid values are from 0 to 7.

Defaults This command has no default settings.

Command Types Switch command

Command Modes Privileged

Usage Guidelines The Catalyst 4000 family switch holds syslog messages until the number of messages equals the defined size of the history log, once the defined size is met the messages are sent.

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)
```

This example shows how to limit syslog messages that are sent to the history log based on severity level:

```
Console> (enable) set logging history severity 5
System logging history set to severity <5>
Console> (enable)
```

Related Commands [clear logging buffer](#)
[show logging](#)