Summit24e3 Switch Quick Reference Guide

Accessing the Switch Commands

Command	Description
clear **s**ession <number>	Terminates a Telnet session from the switch.
config **acco**unt <username> {encrypted} {<password>}	Configures a user account password. Passwords must have a minimum of 1 character and can have a maximum of 32 characters. User names and passwords are case-sensitive.
config **ba**nner	Configures the banner string. You can enter up to 24 rows of 79-column text that is displayed before the login prompt of each session. Press [Return] at the beginning of a line to terminate the command and apply the banner. To clear the banner, press [Return] at the beginning of the first line.
config **dn**s-client **a**dd <ipaddress>	Adds a DNS name server(s) to the available server list for the DNS client. Up to three name servers can be configured.
config **dn**s-client **def**ault-domain <domain_name>	Configures the domain that the DNS client uses if a fully qualified domain name is not entered. For example, if the default domain is configured to be `foo.com`, executing `ping bar` searches for `bar.foo.com`.
config **dn**s-client **del**ete <ipaddress>	Removes a DNS server.
config **ss**h2 **k**ey {pregenerated}	Generates the SSH2 host key.
config **sys-**recovery-level [**n**one | **c**ritical | **a**ll]	Configures a recovery option for instances where an exception occurs in ExtremeWare. Specify one of the following: ■ `none` — Recovery without system reboot. ■ `critical` — ExtremeWare logs an error to the syslog, and reboots the system after critical exceptions. ■ `all` — ExtremeWare logs an error to the syslog, and reboots the system after any exception. The default setting is `none`.
config **time** <date> <time>	Configures the system date and time. The format is as follows: `mm/dd/yyyy hh:mm:ss` The time uses a 24-hour clock format. You cannot set the year past 2036.

Command	Description
config **timez**one <gmt_offset> {autodst | noautodst}	Configures the time zone information to the configured offset from GMT time. The format of `gmt_offset` is +/- minutes from GMT time. Specify: ■ `autodst` — Enables automatic Daylight Savings Time change. ■ `nosautodst` — Disables automatic Daylight Savings Time change. The default setting is `autodst`.
config **v**lan <name> **i**paddress <ip_address> {<mask>}	Configures an IP address and subnet mask for a VLAN.
create **acco**unt [admin | user] <username> {encrypted} {<password>}	Creates a user account. This command is available to admin-level users and to users with RADIUS command authorization. The username is between 1 and 32 characters, the password is between 0 and 16 characters.
create **v**lan <name>	Creates a VLAN.
delete **acco**unt <username>	Deletes a user account.
delete **v**lan <name>	Deletes a VLAN.
disable **bootp** vlan [<name> | all]	Disables BOOTP for one or more VLANs.
disable **cli-**config-logging	Disables logging of CLI commands to the Syslog.
disable **clip**aging	Disables pausing of the screen display when a show command output reaches the end of the page.
disable **id**letimeouts	Disables the timer that disconnects all sessions. Once disabled, console sessions remain open until the switch is rebooted or you logoff. Telnet sessions remain open until you close the Telnet client.
disable **po**rts <portlist>	Disables a port on the switch.
disable **ss**h2	Disables SSH2 Telnet access to the switch.
disable **te**lnet	Disables Telnet access to the switch.
enable **bootp** vlan [<name> | all]	Enables BOOTP for one or more VLANs.
enable **cli-**config-logging	Enables the logging of CLI configuration commands to the Syslog for auditing purposes. The default setting is enabled.
enable **clip**aging	Enables pausing of the screen display when `show` command output reaches the end of the page. The default setting is enabled.
enable **id**letimeouts	Enables a timer that disconnects all sessions (both Telnet and console) after 20 minutes of inactivity. The default setting is disabled.
enable **ss**h2 {port <tcp_port_number>}	Enables SSH2 Telnet sessions. By default, SSH2 uses TCP port number 22.
enable **te**lnet {port <tcp_port_number>}	Enables Telnet access to the switch. By default, Telnet uses TCP port number 23.
history	Displays the previous 49 commands entered on the switch.

Command	Description
nslookup <hostname>	Displays the IP address of the requested host.
ping {continuous} {size <start_size> {-<end_size>}} [<ip_address> | <hostname>] {from <src_address> | with record-route | from <src_ipaddress> with record-route}	Enables you to send Internet Control Message Protocol (ICMP) echo messages to a remote IP device. Specify: ■ `continuous` — Specifies ICMP echo messages to be sent continuously. This option can be interrupted by pressing any key. ■ `size` — Specifies the size of the ICMP request. If both the `start_size` and `end_size` are specified, transmits ICMP requests using 1 byte increments, per packet. If no `end_size` is specified, packets of `start_size` are sent. ■ `<ipaddress>` — Specifies the IP address of the host. ■ `<hostname>` — Specifies the name of the host. To use the `hostname`, you must first configure DNS. ■ `from` — Uses the specified source address in the ICMP packet. If not specified, the address of the transmitting interface is used. ■ `with record-route` — Decodes the list of recorded routes and displays them when the ICMP echo reply is received.
show **b**anner	Displays the user-configured banner.
show **dn**s-client	Displays the DNS configuration.
traceroute [<ip_address> | <hostname>] {from <src_ipaddress>} {ttl <TTL>} {port <port>}	Enables you to trace the routed path between the switch and a destination endstation. Specify: ■ `ip_address` — is the IP address of the destination endstation. ■ `hostname` — is the hostname of the destination endstation. To use the hostname, you must first configure DNS. ■ `from` — uses the specified source address in the ICMP packet. If not specified, the address of the transmitting interface is used. ■ `ttl` — configures the switch to trace up to the time-to-live number of the switch. ■ `port` — uses the specified UDP port number.
unconfig **sw**itch {all}	Resets all switch parameters (with the exception of defined user accounts, and date and time information) to the factory defaults. If you specify the keyword `all`, the switch erases the currently selected configuration image in flash memory and reboots. As a result, all parameters are reset to default settings.

Managing the Switch Commands

Command	Description
config **radius** [**p**rimary | **s**econdary] **se**rver [<ipaddress> | <hostname>] {<udp_port>} client-ip <ipaddress>	Configures the primary and secondary RADIUS server. Specify the following: - `[primary	secondary]` — Configure either the primary or secondary RADIUS server. - `[<ipaddress>	<hostname>]` — The IP address or hostname of the server being configured. - `<udp_port>` — The UDP port to use to contact the RADUIS server. The default UDP port setting is 1645. - `client-ip <ipaddress>` — The IP address used by the switch to identify itself when communicating with the RADIUS server. The RADIUS server defined by this command is used for user name authentication and CLI command authentication.
config **radius** [**p**rimary | **s**econdary] **sh**ared-secret {encrypted} <string>	Configures the authentication string used to communicate with the RADIUS server.
config **radius-**accounting [**p**rimary | **s**econdary] **se**rver [<ipaddress> | <hostname>] {<udp_port>} client-ip <ipaddress>	Configures the RADIUS accounting server. Specify the following: - `[primary	secondary]` — Configure either the primary or secondary RADIUS server. - `[<ipadress>	<hostname>]` — The IP address or hostname of the server being configured. - `<udp_port>` — The UDP port to use to contact the RADUIS server. The default UDP port setting is 1646. - `client-ip <ipaddress>` — The IP address used by the switch to identify itself when communicating with the RADIUS server. The accounting server and the RADIUS authentication server can be the same.
config **radius-**accounting [**p**rimary | **s**econdary] **sh**ared-secret {encrypted} <string>	Configures the authentication string used to communicate with the RADIUS accounting server.
config **snm**p **ad**d **t**rapreceiver <ipaddress> community <string>	Adds the IP address of a specified trap receiver. The IP address can be a unicast, multicast, or broadcast address. A maximum of 16 trap receivers is allowed.
config **snm**p **c**ommunity [read-only | read-write] <string>	Adds an SNMP read or read/write community string. The default `read-only` community string is `public`. The default `read-write` community string is `private`. Each community string can have a maximum of 127 characters, and can be enclosed by double quotation marks.
config **snm**p **d**elete **t**rapreceiver [<ip_address> community <string> | all]	Deletes the IP address of a specified trap receiver or all authorized trap receivers.
config **snm**p **sysc**ontact <string>	Configures the name of the system contact. A maximum of 255 characters is allowed.

Command	Description
config **snm**p **sysl**ocation <string>	Configures the location of the switch. A maximum of 255 characters is allowed.
config **snm**p **sysn**ame <string>	Configures the name of the switch. A maximum of 32 characters is allowed. The default sysname is the model name of the device (for example, `Summit24e3)`. The `sysname` appears in the switch prompt.
config **snt**p-client [**p**rimary | **s**econdary] server [<ipaddress> | <host_name>]	Configures an NTP server for the switch to obtain time information. Queries are first sent to the primary server. If the primary server does not respond within 1 second, or if it is not synchronized, the switch queries the second server.
config **snt**p-client **u**pdate-interval <seconds>	Configures the interval between polling for time information from SNTP servers. The default setting is 64 seconds.
config **tacacs** [**p**rimary | **s**econdary] **se**rver [<ipaddress> | <hostname>] {<udp_port>} client-ip <ipaddress>	Configure the server information for a TACACS+ server. Specify the following: ■ `primary | secondary` — Specifies primary or secondary server configuration. To remove a server, use the address 0.0.0.0. ■ `<ipaddress> | <hostname>` — Specifies the TACACS+ server. ■ `<udp_port>` — Optionally specifies the UDP port to be used. ■ `client-ip` — Specifies the IP address used by the switch to identify itself when communicating with the TACACS+ server.
config **tacacs** [**p**rimary | **s**econdary] **sh**ared-secret {encrypted} <string>	Configures the shared secret string used to communicate with the TACACS+ server.
config **tacacs-ac**counting [**p**rimary | **s**econdary] **se**rver [<ipaddress> | <hostname>] {<udp_port>} client-ip <ipaddress>	Configures the TACACS+ accounting server. You can use the same server for accounting and authentication.
config **tacacs-ac**counting [**pr**imary | secondary] **sh**ared-secret {encrypted} <string>	Configures the shared secret string used to communicate with the TACACS+ accounting server.
disable **radius**	Disables the RADIUS client.
disable **radius-**accounting	Disables RADIUS accounting.
disable **snm**p **a**ccess	Disables SNMP on the switch. Disabling SNMP access does not affect the SNMP configuration (for example, community strings).
disable **snm**p **t**raps	Prevents SNMP traps from being sent from the switch. Does not clear the SNMP trap receivers that have been configured.
disable **snt**p-client	Disables SNTP client functions.
disable **tacacs**	Disables TACACS+.
disable **tacacs-ac**counting	Disables TACACS+ accounting.
disable **tacacs-au**thorization	Disables CLI command authorization.

Command	Description
enable **radius**	Enables the RADIUS client. When enabled, all CLI logins are sent to the RADIUS servers for authentication. When used with a RADIUS server that supports ExtremeWare CLI authorization, each CLI command is sent to the RADIUS server for authentication before it is executed.
enable **radius-**accounting	Enables RADIUS accounting. The RADIUS client must also be enabled.
enable **snm**p **a**ccess	Turns on SNMP support for the switch.
enable **snm**p **t**raps	Turns on SNMP trap support.
enable **snt**p-client	Enables Simple Network Time Protocol (SNTP) client functions.
enable **tacacs**	Enables TACACS+. Once enabled, all CLI logins are sent to one of the two TACACS+ server for login name authentication and accounting.
enable **tacacs-ac**counting	Enables TACACS+ accounting. If accounting is use, the TACACS+ client must also be enabled.
enable **tacacs-au**thorization	Enables CLI command authorization. When enabled, each command is transmitted to the remote TACACS+ server for authorization before the command is executed.
show **radius**	Displays the current RADIUS client configuration and statistics.
show **sn**tp-client	Displays configuration and statistics for the SNTP client.
show **tacacs**	Displays the current TACACS+ configuration and statistics.
show **tacacs-**accounting	Displays the current TACACS+ accounting client configuration and statistics.
telnet [<ipaddress> | <hostname>] {<port_number>}	Enables a Telnet session on the switch. Up to eight active Telnet sessions can access the switch concurrently. You can Telnet to a switch by entering the IP address of the switch or the hostname of the switch. The Telnet session defaults to port 23.
unconfig **m**anagement	Restores default values to all SNMP-related entries.
unconfig **tacacs** {server [primary | secondary]}	Unconfigures the TACACS+ client configuration.
unconfig **tacacs-**accounting {server [primary | secondary]}	Unconfigures the TACACS+ accounting client configuration.

Configuring Ports on a Switch Commands

Command	Description
config **p**orts <portlist> **a**uto **off** {speed [10 | 100 | 1000]} **d**uplex [**h**alf | **f**ull]	Changes the configuration of a group of ports. Specify the following: - `auto off` — The port will not autonegotiate the settings. - `speed` — The speed of the port (for 10/100 Mbps or 100/1000 Mbps ports only). - `duplex` — The duplex setting (half- or full-duplex).
config **p**orts <portlist> **a**uto **on**	Enables autonegotiation for the particular port type; 802.3u for 10/100 Mbps ports or 802.3z for Gigabit Ethernet ports.
config **p**orts <portlist> **d**isplay-string <string>	Configures a user-defined string for a port. The string is displayed in certain `show` commands (for example, `show port all info`). The string can be up to 16 characters.
config **sh**aring address-based [mac_source | mac_destination | mac_source_destination | ip_source | ip_destination | ip_source_destination]	Configures the part of the packet examined by the switch when selecting the egress port for transmitting load-sharing data. This feature is available using the address-based load-sharing algorithm, only.
disable **e**dp ports <portlist>	Disable EDP on one or more ports.
disable **p**orts <portlist	Disables a port. Even when disabled, the link is available for diagnostic purposes.
disable **p**orts <portlist>	Disables a port. Even when disabled, the link is available for diagnostic purposes.
disable **sh**aring <port>	Disables a load-sharing group of ports.
enable **e**dp ports <portlist>	Enables the generation and processing of EDP messages on one or more ports. The default setting is enabled.
enable **p**orts <portlist>	Enables a port.
enable **sh**aring <port> grouping <portlist> {address-based}	Defines a load-sharing group of ports. The ports specified in `<portlist>` are grouped to the master port. The optional load-sharing algorithm, address-based, uses addressing information as criteria for egress port selection.
restart **p**orts <portlist>	Resets autonegotiation for one or more ports by resetting the physical link.
show **e**dp	Displays EDP information.
show **p**orts {<portlist>} **col**lisions	Displays real-time collision statistics.
show **p**orts {<portlist>} **con**figuration	Displays the port configuration.
show **p**orts {<portlist>} **i**nfo {detail}	Displays detailed system-related information.
show **p**orts {<portlist>} **p**acket	Displays a histogram of packet statistics.
show **p**orts {<portlist>} **r**xerrors	Displays real-time receive error statistics.
show **p**orts {<portlist>} **s**tats	Displays real-time port statistics.
show **p**orts {<portlist>} **t**xerrors	Displays real-time transmit error statistics.

Command	Description
show **p**orts {<portlist>} **u**tilization	Displays real-time port utilization information. Use the [Spacebar] to toggle between packet, byte, and bandwidth utilization information.
show **sh**aring address-based	Displays the address-based load sharing configuration.
unconfig **p**orts <portlist> **d**isplay-string <string>	Clears the user-defined display string from a port.
unconfig **p**orts <portlist> **r**edundant <portlist>	Clears a previously configured software-controlled redundant port.

VLAN Commands

Command	Description
config **v**lan <name> **d**elete **p**ort <portlist> {tagged | untagged} {nobroadcast}	Deletes one or more ports from a VLAN.
config **v**lan <name> **i**paddress <ipaddress> {<mask>}	Assigns an IP address and an optional mask to the VLAN.
config **v**lan <name> **t**ag <vlanid>	Assigns a numerical VLANid. The valid range is from 1 to 4095.
config **v**lan <old_name> **na**me <new_name>	Renames a previously configured VLAN.
create **v**lan <name>	Creates a named VLAN.
delete **v**lan <name>	Removes a VLAN.
show **vl**an {<name>}	Displays summary information about each VLAN, which includes: ■ Name ■ VLANid ■ How the VLAN was created ■ IP address ■ STPD information ■ QoS profile information ■ Ports assigned ■ Tagged/untagged status for each port ■ How the ports were added to the VLAN ■ Number of VLANs configured on the switch
unconfig **v**lan <name> **i**paddress	Resets the IP address of the VLAN.

FDB Commands

Command	Description
clear **f**db	Clears all FDB entries.
config **fd**b agingtime <number>	Configures the FDB aging time. The range is 15 through 1,000,000 seconds. The default value is 300 seconds. A value of 0 indicates that the entry should never be aged out.
create **f**dbentry <mac_address> vlan <name> [blackhole | <portlist>] }	Creates an FDB entry. Specify the following: ■ `mac_address` — Device MAC address, using colon separated bytes. ■ `name` — VLAN associated with MAC address. ■ `blackhole` — Configures the MAC address as a blackhole entry. ■ `portlist` — Port numbers associated with MAC address. If more than one port number is associated with a permanent MAC entry, packets are multicast to the multiple destinations.
delete **f**dbentry <mac_address> vlan <name>	Deletes a permanent FDB entry.
show **f**db {<mac_address> | vlan <name> | <portlist> | permanent}	Displays the switch FDB contents.

Status Monitoring and Statistics Commands

Command	Description
clear **c**ounters	Clears all switch statistics and port counters.
clear **l**og {static}	Clears the log. If `static` is specified, the critical log messages are also cleared.
config **l**og **d**isplay {<priority>}	Configures the real-time log display. Options include: ■ `priority` — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, emergency, error, alert, warning, notice, info, and debug. If not specified, informational priority messages and higher are displayed.
config **sysl**og {**a**dd} <host name/ip> <facility> {<priority>}	Configures the syslog host address and filters messages sent to the syslog host. Up to 4 syslog servers can be configured. Options include: ■ `host name/ip`— The IP address or name of the syslog host. ■ `facility` — The syslog facility level for local use (local0 - local7). ■ `priority` — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, emergency, alert, error, warning, notice, info, and debug. If not specified, only critical priority messages and are sent to the syslog host.
config **sysl**og **d**elete <host name/ip> <facility> {<priority>	Deletes a syslog host address. ■ `facility` — The syslog facility level for local use (local0 - local7). ■ `priority` — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, emergency, alert, error, warning, notice, info, and debug. If not specified, only critical priority messages and are sent to the syslog host.
config **sys-**recovery-level [**n**one | **c**ritical | **a**ll]	■ `none` — Configures the level to recovery without a system reboot. ■ `critical` — Configures ExtremeWare to log an error into the syslog and automatically reboot the system after a critical exception. ■ `all` — Configures ExtremeWare to log an error into the syslog and automatically reboot the system after any exception. The default setting is `none`. *Extreme Networks recommends that you set the system recovery level to* `critical`*. This allows ExtremeWare to log an error to the syslog and automatically reboot the system after a critical exception.*
disable **cli-**config-logging	Disables configuration logging.

Command	Description
disable **log** display	Disables the log display.
disable **rm**on	Disables the collection of RMON statistics on the switch. The default setting is disabled.
disable **sy**slog	Disables logging to a remote syslog host.
enable **cli-**config-logging	Enables the logging of CLI configuration commands to the Syslog for auditing purposes. The default setting is enabled.
enable **log** display	Enables the log display.
enable **rm**on	Enables the collection of RMON statistics on the switch. The default setting is disabled.
enable **sy**slog	Enables logging to a remote syslog host.
show **di**ag	Displays software diagnostics.
show **l**og {<priority>}	Displays the current snapshot of the log. Options include: ■ `priority` — Filters the log to display message with the selected priority or higher (more critical). Priorities include critical, emergency, alert, error, warning, notice, info, and debug. If not specified, all messages are displayed.
show **l**og **co**nfig	Displays the log configuration, including the syslog host IP address, the priority level of messages being logged locally, and the priority level of messages being sent to the syslog host.
show **me**mory {detail}	Displays the current system memory information. Specify the `detail` option to view task-specific memory usage.
show **sw**itch	Displays the current switch information, including: ■ sysName, sysLocation, sysContact ■ MAC address ■ Current time and time, system uptime, and time zone ■ Operating environment (fans) ■ NVRAM configuration information ■ Scheduled reboot information

Command	Description
show **te**ch-support	Displays the output for the following commands: ■ show version ■ show switch ■ show config ■ show diag ■ show gdb ■ show iparp ■ show ipfdb ■ show ipstats ■ show iproute ■ show ipmc cache detail ■ show igmp snooping detail ■ show memory detail ■ show log It also displays the output from internal debug commands. This command disables the CLI paging feature.
show **ve**rsion	Displays the hardware and software versions currently running on the switch.

STP Commands

Command	Description
config **st**pd <stpd_name> **a**dd **v**lan <name>	Adds a VLAN to the STPD.
config **st**pd <stpd_name> **f**orwarddelay <value>	Specifies the time (in seconds) that the ports in this STPD spend in the listening and learning states when the switch is the Root Bridge. The range is 4 through 30. The default setting is 15 seconds.
config **st**pd <stpd_name> **h**ellotime <value>	Specifies the time delay (in seconds) between the transmission of BPDUs from this STPD when it is the Root Bridge. The range is 1 through 10. The default setting is 2 seconds.
config **st**pd <stpd_name> **m**axage <value>	Specifies the maximum age of a BPDU in this STPD. The range is 6 through 40. The default setting is 20 seconds. Note that the time must be greater than, or equal to 2 * (Hello Time + 1) and less than, or equal to 2 * (Forward Delay –1).
config **st**pd <stpd_name> **po**rts **c**ost <value> <portlist>	Specifies the path cost of the port in this STPD. The range is 1 through 65,535. The switch automatically assigns a default path cost based on the speed of the port, as follows: ■ For a 10 Mbps port, the default cost is 100. ■ For a 100 Mbps port, the default cost is 19.
config **st**pd <stpd_name> **po**rts **p**riority <value> <portlist>	Specifies the priority of the port in this STPD. By changing the priority of the port, you can make it more or less likely to become the root port. The range is 0 through 31. The default setting is 16. A setting of 0 indicates the lowest priority.
config **st**pd <stpd_name> **pr**iority <value>	Specifies the priority of the STPD. By changing the priority of the STPD, you can make it more or less likely to become the root bridge. The range is 0 through 65,535. The default setting is 32,768. A setting of 0 indicates the highest priority.
create **s**tpd <stpd_name>	Creates an STPD. When created, an STPD has the following default parameters: ■ Bridge priority — 32,768 ■ Hello time — 2 seconds ■ Forward delay — 15 seconds
delete **s**tpd <stpd_name>	Removes an STPD. An STPD can only be removed if all VLANs have been deleted from it. The default STPD, s0, cannot be deleted.
*| **di**sable **ign**ore-**b**pdu **v**lan <name>	Allows the switch to recognize STP BPDUs.
disable **ign**ore-stp **v**lan <name>	Allows a VLAN to use STP port information.
disable **st**pd [<stpd_name> | all]	Disables the STP mechanism on a particular STPD, or for all STPDs.

Command	Description
disable **st**pd **p**orts <portlist>	Disables STP on one or more ports. Disabling STP on one or more ports puts those ports in *forwarding* state; all BPDUs received on those ports will be disregarded.
enable **ign**ore-**b**pdu vlan <name>	Configures the switch to ignore STP BPDUs, which prevents ports in the VLAN from becoming part of an STPD. This command is useful when you have a known topology with switches outside your network, and wish to keep the root bridge within your network. The default setting is disabled.
enable **ign**ore-**s**tp vlan <vlan name>	Configures the switch to ignore the STP protocol, and not block traffic for the VLAN(s). This command is useful when multiple VLANs share the same physical ports, but only some of the VLANs require STP protection. The default setting is disabled.
enable **st**pd {<stpd_name>}	Enables the STP protocol for one or all STPDs. The default setting is disabled.
enable **st**pd **p**orts {<portlist>}	Enables the STP protocol on one or more ports. If STPD is enabled for a port, bridge protocol data units (BPDUs) will be generated on that port if STP is enabled for the associated STPD. The default setting is enabled.
show **st**pd {<stpd_name>}	Displays STP settings.
show **st**pd <stpd_name> **p**orts <portlist>	Displays the STP state of a port.
unconfig **st**pd {<stpd_name>}	Restores default STP values to a particular STPD or to all STPDs.

IP Unicast Routing Commands

Command	Description
clear **ipa**rp {<ipaddress> | vlan <name>}	Removes dynamic entries in the IP ARP table. Permanent IP ARP entries are not affected.
clear **ipf**db {<ipaddress> <netmask> | vlan <name>]	Removes the dynamic entries in the IP forwarding database. If no options are specified, all IP FDB entries are removed.
config **bo**otprelay **a**dd <ipaddress>	Adds the IP destination address to forward BOOTP packets.
config **bo**otprelay **d**elete [<ipaddress> | **a**ll]	Removes one or all IP destination addresses for forwarding BOOTP packets.
config **ipa**rp **a**dd <ipaddress> <mac_address>	Adds a permanent entry to the ARP table. Specify the IP address and MAC address of the entry.
config **ipa**rp **d**elete <ipaddress>	Deletes an entry from the ARP table. Specify the IP address of the entry.
config **ipa**rp **t**imeout <minutes>	Configures the IP ARP timeout period. The default setting is 20 minutes. A setting of 0 disables ARP aging. The maximum aging time is 32 minutes.
config **ipr**oute **a**dd **d**efault <gateway> {<metric>}	Adds a default gateway to the routing table. A default gateway must be located on a configured IP interface. If no metric is specified, the default metric of 1 is used. Use the unicast-only or multicast-only options to specify a particular traffic type. If not specified, both unicast and multicast traffic uses the default route.
config **ipr**oute **d**elete <**i**paddress> <mask> <gateway>	Deletes a static address from the routing table.
config **ipr**oute **d**elete **b**lackhole <ipaddress> <mask>	Deletes a `blackhole` address from the routing table.
config **ipr**oute **d**elete **d**efault <gateway>	Deletes a default gateway from the routing table.
config **ipr**oute **p**riority [rip | bootp | icmp | static] <priority>	Changes the priority for all routes from a particular route origin.
config **ir**dp [**m**ulticast | **b**roadcast]	Configures the destination address of the router advertisement messages. The default setting is `multicast`.
config **ir**dp <mininterval> <maxinterval> <lifetime> <preference>	Configures the router advertisement message timers, using seconds. Specify: ■ `mininterval` — The minimum amount of time between router advertisements. The default setting is 450 seconds. ■ `maxinterval` — The maximum time between router advertisements. The default setting is 600 seconds. ■ `lifetime` — The default setting is 1,800 seconds. ■ `preference` — The preference level of the router. An ICMP Router Discover Protocol (IRDP) client always uses the router with the highest preference level. Change this setting to encourage or discourage the use of this router. The default setting is 0.

Command	Description
config **u**dp-profile <profile_name> **a**dd <udp_port> [vlan <name> | ipaddress <dest_ipaddress>]	Adds a forwarding entry to the specified UDP-forwarding profile name. All broadcast packets sent to `<udp_port>` are forwarded to either the destination IP address (unicast or subnet directed broadcast) or to the specified VLAN as an all-ones broadcast.
config **u**dp-profile <profile_name> **d**elete <udp_port> [vlan <name> | ipaddress <dest_ipaddress>]	Deletes a forwarding entry from the specified `udp-profile` name.
config **v**lan <name> **u**dp-profile <profile_name>	Assigns a UDP-forwarding profile to the source VLAN. Once the UDP profile is associated with the VLAN, the switch picks up any broadcast UDP packets that matches with the user configured UDP port number, and forwards those packets to the user-defined destination. If the UDP port is the DHCP/BOOTP port number, appropriate DHCP/BOOTP proxy functions are invoked.
create **u**dp-profile <profile_name>	Creates a UDP-forwarding profile. You must use a unique name for the UDP-forwarding profile.
delete **u**dp-profile <profile_name>	Deletes a UDP-forwarding profile.
disable **bootp** vlan [<name> | all]	Disables the generation and processing of BOOTP packets.
disable **bootpr**elay	Disables the forwarding of BOOTP requests.
disable **ic**mp **pa**rameter-problem {vlan <name>}	Disables the generation of ICMP parameter-problem messages. If a VLAN is not specified, the command applies to all IP interfaces.
disable **i**cmp **po**rt-unreachables {vlan <name>}	Disables the generation of ICMP port unreachable messages. If a VLAN is not specified, the command applies to all IP interfaces.
disable **ic**mp **r**edirects {vlan <name>}	Disables the generation of ICMP redirect messages. If a VLAN is not specified, the command applies to all IP interfaces.
disable **ic**mp **time-**exceeded {vlan <name>}	Disables the generation of ICMP time exceeded messages. If a VLAN is not specified, the command applies to all IP interfaces.
disable **ic**mp **times**tamp {vlan <name>}	Disables the generation of ICMP timestamp messages. If a VLAN is not specified, the command applies to all IP interfaces.
disable **ic**mp **un**reachables {vlan <name>}	Disables the generation of ICMP network unreachable messages and host unreachable messages. If a VLAN is not specified, the command applies to all IP interfaces.
disable **ic**mp **us**eredirects	Disables the changing of routing table information when an ICMP redirect message is received.
disable **ipf**orwarding {vlan <name>}	Disables routing for one or all VLANs.
disable **ipf**orwarding **b**roadcast {vlan <name>}	Disables routing of broadcasts to other networks.
disable **ip-**option **u**se-router-alert	Disables the generation of the router alert IP option.
disable **ipr**oute sharing	Disables load sharing for multiple routes.
disable **ir**dp {vlan <name>}	Disables the generation of router advertisement messages on one or all VLANs.
disable **loo**pback-mode **v**lan [<name> | all]	Disables loopback-mode on an interface.

Command	Description
enable **bootp v**lan [<name> | all]	Enables the generation and processing of BOOTP packets on a VLAN to obtain an IP address for the VLAN from a BOOTP server. The default setting is enabled for all VLANs.
enable **bootpr**elay	Enables the forwarding of BOOTP and Dynamic Host Configuration Protocol (DHCP) requests.
enable **ic**mp **pa**rameter-problem {vlan <name>}	Enables the generation of ICMP parameter problem packet (type 12) when the switch cannot properly process the IP header or IP option information. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.
enable **ic**mp **po**rt-unreachables {vlan <name>}	Enables the generation of ICMP port unreachable messages (type 3, code 3) when a TPC or UDP request is made to the switch, and no application is waiting for the request, or access policy denies the request. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.
enable **ic**mp **r**edirects {vlan <name>}	Enables the generation of an ICMP redirect message (type 5) when a packet must be forwarded out on the ingress port. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.
enable **ic**mp **time-**exceeded {vlan <name>}	Enables the generation of an ICMP time exceeded message (type 11) when the TTL field expires during forwarding. IP multicast packets do not trigger ICMP time exceeded messages. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.
enable **ic**mp **times**tamp {vlan <name>}	Enables the generation of an ICMP timestamp response (type 14, code 0) when an ICMP timestamp request is received. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.
enable **ic**mp **un**reachables {vlan <name>}	Enables the generation of ICMP network unreachable messages (type 3, code 0), and host unreachable messages (type 3, code 1) when a packet cannot be forwarded to the destination because of unreachable route or host.ICMP packet processing on one or all VLANs. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.
enable **ic**mp **us**eredirects	Enables the modification of route table information when an ICMP redirect message is received. This option applies to the switch when it *is not configured for routing*. The default setting is disabled.
enable **ipf**orwarding {vlan <name>}	Enables IP routing for one or all VLANs. If no argument is provided, enables routing for all VLANs that have been configured with an IP address. The default setting for `ipforwarding` is disabled.
enable **ipf**orwarding **b**roadcast {vlan <name>}	Enables forwarding IP broadcast traffic for one or all VLANs. If no argument is provided, enables broadcast forwarding for all VLANs. To enable, `ipforwarding` must be enabled on the VLAN. The default setting is disabled.
enable **ip-**option **u**se-router-alert	Enables the switch to generate the router alert IP option with routing protocol packets.

Command	Description
enable **ipr**oute sharing	Enables load sharing if multiple routes to the same destination are available. Only paths with the same lowest cost are shared. The default setting is disabled.
enable **ir**dp {vlan <name>}	Enables the generation of ICMP router advertisement messages on one or all VLANs. The default setting is enabled.
enable **loo**pback-mode **v**lan [<name> | all]	Enables a loopback mode on an interface. If loopback is enabled, the router interface remains in the UP state, even if no ports are defined in the VLAN. As a result, the subnet is always advertised as one of the available routes.
rtlookup [<ipaddress> | <hostname>]	Performs a look-up in the route table to determine the best route to reach an IP address.
show **ipa**rp {<ipaddress | vlan <name> | **pe**rmanent}	Displays the IP Address Resolution Protocol (ARP) table. You can filter the display by IP address, VLAN, or permanent entries.
show **ipc**onfig {vlan <name>}	Displays configuration information for one or all VLANs.
show **ipf**db {<ipaddress> <netmask> | vlan <name> }	Displays the contents of the IP forwarding database (FDB) table. If no option is specified, all IP FDB entries are displayed.
show **ipr**oute {priority | vlan <vlan> | **pe**rmanent | <ipaddress> <netmask> | route-map | origin [direct | blackhole | bootp | icmp} {sorted}	Displays the contents of the IP routing table, the route origin priority, or the route origin route map.
show **ips**tats {vlan <name>}	Displays IP statistics for the CPU of the system.
show **u**dp-profile {<profile_name>}	Displays the profile names, input rules of UDP port, destination IP address, or VLAN and the source VLANs to which the profile is applied.
unconfig **ic**mp	Resets all ICMP settings to the default values.
unconfig **ir**dp	Resets all router advertisement settings to the default values.
unconfig **u**dp-profile vlan [<name> | all]	Removes the UDP-forwarding profile configuration for one or all VLANs.

Interior Gateway Routing Protocol Commands

Command	Description
config **ri**p **a**dd **v**lan [<name> | all]	Configures RIP on an IP interface. When an IP interface is created, per-interface RIP configuration is disabled by default.
config **ri**p **d**elete **v**lan [<name> | all]	Disables RIP on an IP interface. When RIP is disabled on the interface, the parameters are not reset to their defaults.
config **ri**p **g**arbagetime {<seconds>}	Configures the RIP garbage time. The timer granularity is 10 seconds. The default setting is 120 seconds.
config **ri**p **ro**utetimeout {<seconds>}	Configures the route timeout. The default setting is 180 seconds.
config **ri**p **rx**mode [**n**one | **v1**only | **v2**only | **a**ny] {vlan <name>}	Changes the RIP receive mode for one or all VLANs. Specify: ■ `none` — Drop all received RIP packets. ■ `v1only` — Accept only RIP v1 format packets. ■ `v2only` — Accept only RIP v2 format packets. ■ `any` — Accept both RIP v1 and v2 packets. If no VLAN is specified, the setting is applied to all VLANs. The default setting is `any`.
config **ri**p **t**xmode [**n**one | **v1**only | **v1**comp | **v2**only] {vlan <name>}	Changes the RIP transmission mode for one or all VLANs. Specify: ■ `none` — Do not transmit any packets on this interface. ■ `v1only` — Transmit RIP v1 format packets to the broadcast address. ■ `v1comp` — Transmit RIP v2 format packets to the broadcast address. ■ `v2only` — Transmit RIP v2 format packets to the RIP multicast address. If no VLAN is specified, the setting is applied to all VLANs. The default setting is `v2only`.
config **ri**p **u**pdatetime {<seconds>}	Changes the periodic RIP update timer. The default setting is 30 seconds.
config **ri**p **v**lan [<name> | **a**ll] **c**ost <number>	Configures the cost (metric) of the interface. The default setting is 1.
disable **ri**p	Disables RIP.
disable **ri**p **a**ggregation	Disables the RIP aggregation of subnet information on a RIP v2 interface.
disable **ri**p **e**xport [static | direct] metric <metric> {tag <number>}	Disables the distribution of non-RIP routes into the RIP domain.
disable **ri**p **o**riginate-default	Disables the advertisement of a default route.
disable **ri**p **p**oisonreverse	Disables poison reverse.
disable **ri**p **s**plithorizon	Disables split horizon.
disable **ri**p **t**riggerupdates	Disables triggered updates.

Command	**Description**
enable **ri**p	Enables RIP. The default setting is disabled.
enable **ri**p **a**ggregation	Enables aggregation of subnet information on interfaces configured to send RIP v2 or RIP v2-compatible traffic. The switch summarizes subnet routes to the nearest class network route. The following rules apply when using RIP aggregation: ■ Subnet routes are aggregated to the nearest class network route when crossing a class boundary. ■ Within a class boundary, no routes are aggregated. ■ If aggregation is enabled, the behavior is the same as in RIP v1. ■ If aggregation is disabled, subnet routes are never aggregated, even when crossing a class boundary. The default setting is disabled.
enable **ri**p **e**xport [static | direct] metric <metric> {tag <number>}	Enables RIP to redistribute routes from other routing functions. Specify one of the following: ■ `static` — Static routes ■ `direct` — Interface routes (only interfaces that have IP forwarding enabled are exported) The `metric` range is 0-15. If set to 0, RIP uses the route metric obtained from the route origin.
enable **ri**p **o**riginate-default {always} cost <metric> {tag <number>}	Configures a default route to be advertised by RIP if no other default route is advertised. If `always` is specified, RIP always advertises the default route to its neighbors. If `always` is not specified, RIP adds a default route if there is a reachable default route in the route table.
enable **ri**p **p**oisonreverse	Enables the split horizon with poison-reverse algorithm for RIP. The default setting is enabled. If you enable poison reverse and split horizon, poison reverse takes precedence.
enable **ri**p **s**plithorizon	Enables the split horizon algorithm for RIP. Default setting is enabled.
enable **ri**p **t**riggerupdates	Enables triggered updates. *Triggered update*s are a mechanism for immediately notifying a router's neighbors when the router adds or deletes routes, or changes the metric of a route. The default setting is enabled.
show **ri**p {**d**etail}	Displays RIP configuration and statistics for all VLANs.
show **ri**p **s**tat {**d**etail}	Displays RIP-specific statistics for all VLANs.
show **ri**p **s**tat **v**lan <name>	Displays RIP-specific statistics for a VLAN.
show **ri**p **v**lan <name>	Displays RIP configuration and statistics for a VLAN.
unconfig **ri**p {**v**lan <name>}	Resets all RIP parameters to match the default VLAN. Does not change the enable/disable state of the RIP settings. If no VLAN is specified, all VLANs are reset.

IP Multicast Routing Commands

Command	Description
clear **ig**mp **s**nooping {**v**lan <name>}	Removes one or all IGMP snooping entries.
clear **ipm**c **c**ache {<group> {<source> <netmask>}}	Resets the IP multicast cache table. If no options are specified, all IP multicast cache entries are flushed.
config **ig**mp <query_interval> <query_response_interval> <last_member_query_interval>	Configures the IGMP timers. Timers are based on RFC2236. Specify the following: ■ `query_interval` — The amount of time, in seconds, the system waits between sending out General Queries. The range is 1 to 2,147,483,647 seconds (68 years). The default setting is 125 seconds. ■ `query_response_interval` — The maximum response time inserted into the periodic General Queries. The range is 1 to 25 seconds. The default setting is 10 seconds. ■ `last_member_query_interval` — The maximum response time inserted into a Group-Specific Query sent in response to a Leave group message. The range is 1 to 25 seconds. The default setting is 1 second.
config **ig**mp **s**nooping <router_timeout> <host_timeout>	Configures the IGMP snooping timers. Timers should be set to approximately 2.5 times the router query interval in use on the network. Specify the following: ■ `router_timeout` — The interval, in seconds, between the last time the router was discovered and the current time. The range is 10 to 2,147,483,647 seconds (68 years). The default setting is 260 seconds. ■ `host_timeout` — The interval, in seconds, between the last IGMP group report message from the host and the current time. The range is 10 to 2,147,483,647 seconds (68 years). The default setting is 260 seconds.
config **ipm**c **c**ache timeout <seconds>	Configures the aging time for multicast cache entries. The default setting is 300 seconds.
disable **igm**p {**v**lan <name>}	Disables the router-side IGMP processing on a router interface. No IGMP query is generated, but the switch continues to respond to IGMP queries received from other devices. If no VLAN is specified, IGMP is disabled on all router interfaces.
disable **igm**p **s**nooping	Disables IGMP snooping. IGMP snooping can be disabled only if IP multicast routing is not being used. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given VLAN.
disable **ipm**cforwarding {**v**lan <name>}	Disables IP multicast forwarding.
enable **igm**p {**v**lan <name>}	Enables IGMP on a router interface. If no VLAN is specified, IGMP is enabled on all router interfaces. The default setting is enabled.

Command	Description
enable **igm**p **s**nooping {forward-mcrouter-only}	Enables IGMP snooping on the switch. If `forward-mcrouter-only` is specified, the switch forwards all multicast traffic to the multicast router, only. Otherwise, the switch forwards all multicast traffic to any IP router.
enable **ipm**cforwarding {<vlan <name}	Enables IP multicast forwarding on an IP interface. If no options are specified, all configured IP interfaces are affected. When new IP interfaces are added, `ipmcforwarding` is disabled by default.
show **ig**mp **s**nooping {**v**lan <name>} {**d**etail}	Displays IGMP snooping registration information, and a summary of all IGMP timers and states.
show **ipm**c **c**ache {detail} {<group>} {<source> <netmask>}}	Displays the IP multicast forwarding cache.
unconfig **ig**mp	Resets all IGMP settings to their default values and clears the IGMP group table.

Software Upgrade and Boot Commands

Command	Description
config **dow**nload **s**erver [**p**rimary | **s**econdary] [<hostname> | <ipaddress>] <filename>	Configures the TFTP server(s) used by a scheduled incremental configuration download.
download **b**ootrom [<hostname> | <ipaddress>] <filename>	Downloads a BOOT ROM image from a TFTP server. The downloaded image replaces the BOOT ROM in the onboard FLASH memory. *If this command does not complete successfully it could prevent the switch from booting.*
download **c**onfiguration [<hostname> | <ipaddress>] <filename> {incremental}	Downloads a complete configuration. Use the `incremental` keyword to specify an incremental configuration download.
download **c**onfiguration **c**ancel	Cancels a previously scheduled configuration download.
download **c**onfiguration **e**very <hour>	Schedules a configuration download. Specify the hour using a 24-hour clock, where the range is 0 to 23.
download **i**mage [<ipaddress> | <hostname>] <filename> {primary | secondary}	Downloads a new image from a TFTP server over the network. If no parameters are specified, the image is saved to the current image.
reboot {time <date> <time> | cancel}	Reboots the switch at the date and time specified. If you do not specify a reboot time, the reboot happens immediately following the command, and any previously scheduled reboots are cancelled. To cancel a previously scheduled reboot, use the `cancel` option.
save {configuration} {primary | secondary}	Saves the current configuration to nonvolatile storage. You can specify the primary or secondary configuration area. If not specified, the configuration is saved to the primary configuration area.
show **c**onfiguration	Displays the current configuration to the terminal. You can then capture the output and store it as a file.
upload **co**nfiguration [<ipaddress> | <hostname>] <filename> {every <time>}	Uploads the current run-time configuration to the specified TFTP server. If `every <time>` is specified, the switch automatically saves the configuration to the server once per day, at the specified time. If the time option is not specified, the current configuration is immediately uploaded.
upload **co**nfiguration **c**ancel	Cancels a previously schedule configuration upload.
use **c**onfiguration [**p**rimary | **s**econdary]	Configures the switch to use a particular configuration on the next reboot. Options include the primary configuration area or the secondary configuration area.
use **i**mage [**p**rimary | **s**econdary]	Configures the switch to use a particular image on the next reboot.