

set fddi alarm

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

set fddi alarm *mod_num/port_num value*

Syntax Description

mod_num Number of the module.

port_num Number of the port.

value Value for the LER-alarm parameter. This exponential value represents the number of link errors per second (that is, $10^{-\text{value}}$ link errors per second). Valid values are between 7 and 15.

Default

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

Command Type

Switch command.

Command Mode

Privileged.

Usage Guideline

This command is not supported by the Catalyst 4000 and 2948G series switches.

Example

This example shows how to change the LER-alarm value to 10^{-11} seconds for port 1 on module 4:

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

Related Commands

set fddi cutoff

set fddi t1min

set fddi tnotify

set fddi treq

set fddi userdata

show fddi

set fddi cutoff

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

set fddi cutoff *mod_num/port_num value*

Syntax Description

mod_num Number of the module.

port_num Number of the port.

value Exponential value for the LER-cutoff parameter (that is, 10^{value} link errors per second). Valid values are between 7 and 15.

Default

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

Command Type

Switch command.

Command Mode

Privileged.

Usage Guideline

This command is not supported by the Catalyst 4000 and 2948G series switches.

Example

This example shows how to change the LER-cutoff value to 10^{-10} seconds for port 1 on module 4:

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

Related Commands

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

set fddi tlmin

Use the **set fddi tlmin** command to change the TL_MIN value for an FDDI port.

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

Syntax Description

mod_num Number of the module.

port_num Number of the port.

microseconds Number of microseconds for the TL_MIN parameter.

Default

The default value for TL_MIN is 40 microseconds.

Command Type

Switch command.

Command Mode

Privileged.

Usage Guidelines

This command is not supported by the Catalyst 4000 and 2948G series switches.

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

Example

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

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

Related Commands

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

set fddi tnotify

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

set fddi tnotify *mod_num* *time*

Syntax Description

mod_num Number of the module.

time Number of seconds for the TNotify timer. Valid times are from 2 to 30 seconds.

Default

The default value for the TNotify timer is 30 seconds.

Command Type

Switch command.

Command Mode

Privileged.

Usage Guidelines

This command is not supported by the Catalyst 4000 and 2948G series switches.

The TNotify parameter sets the interval (in seconds) between neighbor notification frames. These frames advertise FDDI module MAC addresses to neighboring devices. Usually, the default setting is sufficient.

Example

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

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

Related Commands

set fddi alarm

set fddi cutoff

set fddi tmin

set fddi treq

set fddi userdata

show fddi

set fddi treq

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

```
set fddi treq mod_num time
```

Syntax Description

mod_num Number of the module.

time Number of seconds for the TRequest value. Valid times are from 2502 to 165,000 microseconds.

Default

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

Command Type

Switch command.

Command Mode

Privileged.

Usage Guidelines

This command is not supported by the Catalyst 4000 and 2948G series switches.

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

Example

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

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

Related Commands

set fddi alarm

set fddi cutoff

set fddi tmin

set fddi tnotify

set fddi userdata

show fddi

set fddi userdata

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

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

Syntax Description

mod_num Number of the module.

userdata_string (Optional) Unique character string that identifies the node.

Default

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

Command Type

Switch command.

Command Mode

Privileged.

Usage Guidelines

This command is not supported by the Catalyst 4000 and 2948G series switches.

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

Example

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

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

Related Commands

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

set igmp

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

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

Syntax Description

enable Keyword to enable IGMP snooping on the switch.

disable Keyword to disable IGMP snooping on the switch.

Default

IGMP snooping is disabled.

Command Type

Switch command.

Command Mode

Privileged.

Usage Guidelines

This command is not supported by the Catalyst 4000 and 2948G series switches.

IGMP snooping is supported only on Catalyst 5000, 2926G, and 2926 series switches using a Supervisor Engine III with an NFFC or NFFC II installed.

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

Examples

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

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

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

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

Related Commands

clear igmp statistics

show igmp statistics

set interface

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

```
set interface {sc0 | sl0 | me1} {up | down}  
set interface sc0 [vlan] [ip_addr] [netmask] [broadcast]]]  
set interface sl0 slip_addr dest_addr  
set interface me1 [ip_addr] [netmask] [broadcast]]]  
set interface trap {sc0 | sl0 | me1} enable | disable
```

Syntax Description

sc0	Keyword to specify the in-band interface.
sl0	Keyword to specify the SLIP interface.
me1	Keyword to specify the me1 interface.
up	Keyword to bring the interface into operation.
down	Keyword to bring the interface out of operation.
<i>vlan</i>	(Optional) Number of the VLAN to be assigned to the interface.
<i>ip_addr</i>	(Optional) IP address.
<i>netmask</i>	(Optional) Subnet mask.
<i>broadcast</i>	(Optional) Broadcast address.
<i>slip_addr</i>	IP address of the console port.
<i>dest_addr</i>	IP address of the host to which the console port will be connected.
trap	Keyword to specify the standard SNMP link trap operation on any interface.
enable	Keyword to enable the standard SNMP link trap operation on any interface.
disable	Keyword to disable the standard SNMP link trap operation on any interface.

Default

The default configuration has the in-band interface (sc0) in VLAN 1 with the IP address, subnet mask, and broadcast address set to 0.0.0.0. The default configuration for the SLIP interface (sl0) is that the IP address and broadcast address are set to 0.0.0.0.0.

Command Type

Switch command.

Command Mode

Privileged.

Usage Guidelines



Caution On the Catalyst 4000 and 2948G series 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. When the CLI command brings up the two interfaces in conflict with this statement, me1 is kept or brought up, and sc0 is brought down as a side effect. The only exception is when me1 and sc0 both have IP address 0.0.0.0. In this case, me1 is brought down and sc0 is brought up to allow the BOOTP protocol to run over sc0.

The Catalyst 5000, 4000, 2948G, 2926G, and 2926 series switches support two IP management interfaces. The synergy interface is called sc0, and it is an inband management port on VLAN 1. An inband management port is attached to the switching fabric of the switch. The second supported interface is a slip interface, called sl0, which can be configured on a serial port. The slip interface is an out-of-band management port because it is not attached to the switching fabric and no traffic is switched over it.

The Catalyst 4000 and 2948G series switches also support a third type of management interface: an out-of-band (OOB) Ethernet interface. The me1 interface is a valid interface when configuring and displaying routes and gateways. If multiple interfaces are configured on a Catalyst 4000 or 2948G series switch, the supervisor engine software determines which interface to use when performing standard transmission and reception of IP packets based on the local routing table. The operations that use this functionality include **copy tftp** (for image downloads), outgoing **ping** and **telnet**, and SNMP. No CLI changes are necessary to enable these operations to utilize me1.

The OOB management Ethernet interface, me1, uses the **set interface me1** command to configure its IP address, netmask, and broadcast. Although me1 resides on the supervisor engine module, port information is not displayed for me1 by any **show module** or **show port** CLI command. It is an interface and it can only be configured or accessed through interface CLI commands.

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

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

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

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

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

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

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

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

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

```
Console> (enable) set interface me1 171.69.199.68 255.255.255.0  
set interface me1 171.69.199.68 255.255.255.0  
Interface me1 IP address and netmask set.  
Console> (enable)
```

This example shows how to specify the standard SNMP link trap operation on the sc0 interface.

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

Related Commands

show interface

slip

set ip alias

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

```
set ip alias name ip_addr
```

Syntax Description

name Name of the alias being defined.

ip_addr IP address of the alias being defined.

Default

The default configuration has one IP alias (0.0.0.0) configured as the default.

Command Type

Switch command.

Command Mode

Privileged.

Example

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

```
Console> (enable) set ip alias mercury 192.122.174.234  
IP alias added.  
Console> (enable)
```

Related Commands

clear ip alias

show ip alias

set ip dns

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

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

Syntax Description

enable Keyword to enable DNS.

disable Keyword to disable DNS.

Default

DNS is disabled.

Command Type

Switch command.

Command Mode

Privileged.

Examples

This example shows how to enable DNS:

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

This example shows how to disable DNS:

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

Related Command

show ip dns

set ip dns domain

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

```
set ip dns domain name
```

Syntax Description

name Default DNS domain name.

Default

This command has no default setting.

Command Type

Switch command.

Command Mode

Privileged.

Usage Guideline

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

Example

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

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

Related Commands

clear ip dns domain

show ip dns

set ip dns server

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

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

Syntax Description

ip_addr IP address of the DNS server.

primary (Optional) Keyword to configure a DNS server as the primary server.

Default

This command has no default setting.

Command Type

Switch command.

Command Mode

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.

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

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) set ip dns server 171.69.2.132 primary  
171.69.2.132 added to DNS server table as primary server.
```

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

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.
```

Related Commands

clear ip dns server

show ip dns

set ip fragmentation

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

set ip fragmentation {enable | disable}

Syntax Description

enable Keyword to permit fragmentation for IP packets bridged between FDDI and Ethernet networks.

disable Keyword to disable fragmentation for IP packets bridged between FDDI and Ethernet networks.

Default

The default value is IP fragmentation enabled.

Command Type

Switch command.

Command Mode

Privileged.

Usage Guideline

If IP fragmentation is disabled, packets are dropped.

Example

This example shows how to disable IP fragmentation:

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

Related Commands

show bridge
show ip route

set ip permit

Use the **set ip permit** command to enable or disable the IP permit list. Use the **set ip permit *ip_addr*** command to specify an IP address to be added to the IP permit list.

```
set ip permit {enable | disable}  
set ip permit ip_addr [mask]
```

Syntax Description

enable	Keyword to enable the IP permit list.
disable	Keyword to disable the 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.

Default

The IP permit list is disabled.

Command Type

Switch command.

Command Mode

Privileged.

Usage Guidelines

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

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

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

Examples

This example shows how to enable the IP permit list:

```
Console> (enable) set ip permit enable  
IP permit list enabled.  
WARNING!! IP permit list has no entries.  
Console> (enable)
```

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

```
Console> (enable) set ip permit 172.100.101.102  
172.100.101.102 added to IP permit list.  
Console> (enable)
```

This example shows how to add an IP address using an IP alias or host name to the IP permit list:

```
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 the IP permit list:

```
Console> (enable) set ip permit 172.160.161.0 255.255.192.0  
172.160.128.0 with mask 255.255.192.0 added to IP permit list.  
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

set ip permit
show ip permit

set ip redirect

Use the **set ip redirect** command to enable or disable ICMP redirect messages on the Catalyst 5000, 4000, 2948G, 2926G, and 2926 series switches.

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

Syntax Description

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

Default

The default configuration has ICMP redirect enabled.

Command Type

Switch command.

Command Mode

Privileged.

Example

This example shows how to deactivate ICMP redirect messages:

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

Related Commands

show ip route
show netstat

set ip route

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

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

Syntax Description

<i>destination</i>	IP address, IP alias of the network, or specific host to be added. Use default as the destination to set the new entry as the default route.
<i>gateway</i>	IP address or IP alias of the router.
<i>metric</i>	(Optional) Value used to indicate the number of hops between the switch and the gateway.
primary	(Optional) Keyword used with the Multiple Default IP Gateways feature to specify the default IP gateway with the highest priority.

Default

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

Command Type

Switch command.

Command Mode

Privileged.

Usage Guidelines

You can configure up to three default gateways. The primary is the highest priority. If a primary is not designated, priority is based on the order of input. If two primary definitions are entered, the second definition becomes the primary and the first definition is now the secondary default IP gateway.

The Multiple Default IP Gateways feature is not supported by the Catalyst 4000 and 2948G series switches.

Example

This example shows how to add three default routes to the IP routing table and provides an explanation following each step. The **show ip route** command is used to check each addition.

Step 1 Set up the sc0 interface.

```
Console> (enable) set interface sc0 172.20.59.25 255.255.255.0  
Interface sc0 IP address and netmask set.
```

A default gateway is configured using sc0. Notice that the Nmp determines that this gateway is out of the sc0 interface. The me1 and sl0 interfaces have not been configured yet.

Step 2 Set up the second default interface.

```
Console> (enable) set ip route default 172.20.59.1
Route added.
```

```
Console> (enable) show ip route
Fragmentation  Redirect  Unreachable
-----
enabled        enabled   enabled
```

Destination	Gateway	Flags	Use	Interface
default	172.20.59.1	UG	0	sc0
172.20.59.0	172.20.59.25	U	0	sc0
default	default	U	0	me1
default	default	UH	0	s10

The me1 interface is configured.

```
Console> (enable) set interface me1 171.69.199.68 255.255.255.0
Interface me1 IP address and netmask set.
```

Step 3 Set up the third default gateway.

```
Console> (enable) set route default 171.69.199.1
Route added.
```

```
Console> (enable) show ip route
Fragmentation  Redirect  Unreachable
-----
enabled        enabled   enabled
```

Destination	Gateway	Flags	Use	Interface
default	172.20.59.1	UG	0	sc0
default	172.69.199.1	G	0	me1
172.20.59.0	172.20.59.25	U	0	sc0
171.69.199.0	171.69.199.68	U	0	me1
default	default	UH	0	s10

```
Console> (enable)
```

The supervisor engine software determines that this default gateway is through me1, without any extra input from the network manager. Notice that the flags on the second default gateway configured (second line in the route table) do not include a "U" to show that the interface is up. When multiple default gateways are configured (a maximum of three), only the primary gateway will be up. If no primary gateway was specified (as in this example) the priority is based on the order of input. That is why the default gateway out sc0 is up.

Note The network manager does not have to add extra arguments to **set ip route** commands to utilize the me1 interface. After the interface is configured, the supervisor engine software determines which routes and gateways will use the me1 interface.

Related Commands

clear ip route

show ip route

set ip unreachable

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

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

Syntax Description

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

Default

The default has ICMP unreachable messages enabled.

Command Type

Switch command.

Command Mode

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.

Example

This example shows how to disable ICMP unreachable messages:

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

Related Command

show ip route

set length

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

```
set length number [default]
```

Syntax Description

- number** Number of lines to display on the screen; valid values are 0 and 5 to 512. 0 turns off the scrolling feature.
- default** (Optional) Keyword to set the number of lines in the terminal display screen for the current administration session and all other sessions. This keyword is only available in privileged mode.

Default

The default value is 24 lines upon starting a session. When the value is changed in a session, it applies only to that session. When you use the **clear config** command, the number of lines in the terminal display screen is reset to the factory default of 100.

Command Type

Switch command.

Command Mode

Privileged.

Usage Guidelines

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

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

Examples

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

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

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

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

set logging buffer

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

set logging buffer *buffer_size*

Syntax Description

buffer_size Size of the buffer; valid values are 1 to 500.

Default

The default value is 500.

Command Type

Switch command.

Command Mode

Privileged.

Example

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

show logging

show logging buffer

set logging console

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

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

Syntax Description

enable Keyword to enable system message logging to the console.

disable Keyword to disable system message logging to the console.

Default

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

Command Type

Switch command.

Command Mode

Privileged.

Examples

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

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

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

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

Related Commands

set logging level

set logging session

show logging

show logging buffer

set logging history

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

set logging history *syslog_history_table_size*

Syntax Description

syslog_history_table_size Size of the syslog history table; valid values are 0 to 500.

Default

This command has no default setting.

Command Type

Switch command.

Command Mode

Privileged.

Example

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

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

Related Command

show logging

set logging level

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

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

Syntax Description

facility Value for the type of system messages to capture. Facility types are shown in Table 2-5.

severity Value for the severity level of system messages to capture. Severity level definitions are shown in Table 2-6.

default (Optional) Keyword to cause the specified logging level to apply to all sessions. If **default** is not used, the specified logging level applies only to the current session.

Table 2-5 Facility Types

Facility Name	Definition
cdp	Cisco Discovery Protocol
mcast	Multicast
dtp	Dynamic Trunk Protocol
dvlan	Dynamic VLAN
earl	Encoded Address Recognition Logic
fddi	Fiber Distributed Data Interface
ip	Internet Protocol
pruning	VTP pruning
snmp	Simple Network Management Protocol
spantree	Spanning-Tree Protocol
sys	System
tac	Terminal Access Controller
tcp	Transmission Control Protocol
telnet	Terminal Emulation Protocol
tftp	Trivial File Transfer Protocol
vtp	Virtual Terminal Protocol
vmps	VLAN Membership Policy Server
kernel	Kernel
fileSYS	File System
drip	Dual Ring Protocol
pagp	Port Aggregation Protocol

Table 2-5 Facility Types (continued)

Facility Name	Definition
mgmt	Management
mls	Multilayer Switching
protfilt	Protocol Filter
security	Security

Table 2-6 Severity Level Definitions

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

Default

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

Command Type

Switch command.

Command Mode

Privileged.

Example

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

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

Related Commands

- show logging**
- show logging buffer**

set logging server

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

```

set logging server { enable | disable }
set logging server ip_addr
set logging server facility server_facility_parameter
set logging server severity server_severity_level
set logging history syslog_history_table_size

```

Syntax Description

enable	Keyword to enable system message logging to configured syslog servers.
disable	Keyword to disable system message logging to configured syslog servers.
<i>ip_addr</i>	IP address of the syslog server to be added to the configuration. An IP alias or a host name that can be resolved through DNS can also be used.
facility	Keyword to set the type of system messages to capture.
<i>server_facility_parameter</i>	Value to specify the logging facility of syslog server; valid values are local0, local1, local2, local3, local4, local5, local6, local7, and syslog.
severity	Keyword to set the severity level of system messages to capture.
<i>server_severity_level</i>	Value to specify the severity level of system messages to capture; valid values are 0 through 7. Severity level definitions are shown in Table 2-6.
<i>syslog_history_table_size</i>	Value that specifies the syslog history table size; valid values are 0 through 500, 0 prevents any history from being retained.

Default

By default, no syslog servers are configured to receive system messages.

Command Type

Switch command.

Command Mode

Privileged.

Examples

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

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

This example shows how to add a syslog server to the system logging server table:

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

This example shows how to set the syslog server facility to local7:

```
Console> (enable) set logging server facility local7  
System logging server facility set to <local7>  
Console> (enable)
```

This example shows how to set the syslog server severity level to 4:

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

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

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

Related Commands

clear logging server

show logging

set logging session

Use the **set logging session** command to enable or disable the sending of system logging messages to the current login session.

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

Syntax Description

enable Keyword to enable the sending of system logging messages to the current login session.

disable Keyword to disable the sending of system logging messages to the current login session.

Default

Default configuration is disabled for log session, “all” for facility and “0” for severity.

Command Type

Switch command.

Command Mode

Privileged.

Examples

This example shows how to prevent system logging messages from being sent to the current login session:

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

This example shows how to cause system logging messages to be sent to the current login session:

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

Related Commands

set logging buffer

set logging level

show logging

show logging buffer

set logging timestamp

Use the **set logging timestamp** command to enable or disable the timestamp display on system logging messages.

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

Syntax Description

enable Keyword to enable the timestamp display.

disable Keyword to disable the timestamp display.

Default

By default, system message logging to the current login session is enabled.

Command Type

Switch command.

Command Mode

Privileged.

Examples

This example shows how to enable the timestamp display:

```
Console> (enable) set logging timestamp enable  
System logging messages timestamp will be enabled.  
Console> (enable)
```

This example shows how to disable the timestamp display:

```
Console> (enable) set logging timestamp disable  
System logging messages timestamp will be disabled.  
Console> (enable)
```

Related Commands

show logging