



Ethernet Port Configuration Mode Commands

Command Modes

The Ethernet Port Configuration Mode is used to create and manage Ethernet ports and their bindings between contexts.

Exec > Global Configuration > Ethernet Port Configuration

configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number) #
```



Important

The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

- [bind interface](#), on page 2
- [breakout-cable](#), on page 2
- [boxertap](#), on page 4
- [description](#), on page 4
- [do show](#), on page 5
- [end](#), on page 5
- [exit](#), on page 6
- [fault-unidirect-mode](#), on page 6
- [flow-control](#), on page 7
- [ingress-mode](#), on page 8
- [link-aggregation](#), on page 8
- [media](#), on page 12
- [medium](#), on page 13
- [preferred slot](#), on page 14
- [shutdown](#), on page 15
- [snmp trap link-status](#), on page 16
- [srp virtual-mac-address](#), on page 16
- [threshold high-activity](#), on page 17
- [threshold monitoring](#), on page 18
- [threshold rx-utilization](#), on page 19
- [threshold tx-utilization](#), on page 21

- [vlan, on page 22](#)

bind interface

Configures an association (binds) between a virtual IP interface, an SS7 or Frame Relay link to a specific context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

configure > **port ethernet** *slot_number/port_number*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

Syntax Description

[**no**] **bind interface** *interface_name context_name*

no

Indicates the virtual interface specified is to be unbound from the context.

interface_name

Specifies the name of an existing virtual interface to be bound to the context as an alphanumeric string of 1 through 79 characters. The interface must be previously defined using the Context Configuration mode **interface** command.

context_name

Specifies the name of the context to be bound to the virtual port. *context_name* must refer to a previously configured context.

Usage Guidelines

Bind an interface to a context to allow the context to provide service.

Example

The following command binds the *ethernet10* interface with the *allstar4* context:

```
bind interface ethernet10 allstar4
```

breakout-cable

Configures port breakout-cable usage for 100GBASE to 10x10GBASE SR or LR interfaces on MIO2 cards.



Important This command cannot be executed on ports equipped with CPAK 100GBASE-LR4 modules because they do not support use of breakout cables.

Product All products running on an ASR 5500 equipped with MIO2 cards and CPAK modules

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Ethernet Port Configuration

configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number) #
```

Syntax Description [no] **breakout-cable**

no

Disables breakout cable support for the 100GBASE interface on an MIO2 card.

Usage Guidelines Use this command to enable or disable the splitting of the 100GB interface on MIO2 cards into ten 10GBASE-SR or 10GBASE-LR ports using an MPO24-to-multiple LC breakout cable. This command can be executed for one or both CPAK modules (port 10 and/or 20) on the MIO2. The use of breakout cables is supported for CPAK-100G-SR10 and CPAK 10x10G-LR modules.

If you enable **breakout-cable** for CPAK ports 5/10 and/or 5/20, after synchronization the configuration will also be valid on CPAK ports 6/10 and/or 6/20.

After enabling or disabling the **breakout-cable** command, you must run the Exec mode **file synchronize** command to assure that the standby MIO2 has the same port configuration as the active MIO2. If a reboot causes the standby MIO2 to become active without synchronization, the breakout port configuration will not be valid on the newly active MIO2.

If you enable or disable cable splitting you must also reboot the system by issuing the Exec mode **reload** command.



Note After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.



Caution Issuing the **reload** command causes the system to become unavailable for session processing until the reboot process is complete.

For additional information, refer to the *MIO2 Cabling* chapter of the *ASR 5500 Installation Guide*.

Example

The following command enables support for a 100Gb interface to ten 10Gb interfaces breakout cable:

```
breakout-cable
```

boxertap

Binds a physical port to a named interface for debugging purposes.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

Syntax Description

```
[ no ] boxertap interface_name
```

no

Unbinds the physical port to the interface.

interface_name

Specifies the name of the virtual interface to be bound to the physical port as an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Bind a physical port to a named interface for debugging purposes.

Example

The following command binds the *ggsn01* interface to the boxertap port.

```
boxertap ggsn01
```

description

Allows you to enter descriptive text for this configuration.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description **description** *text*
no description

no

Clears the description for this configuration.

text

Enter descriptive text as an alphanumeric string of 1 to 100 characters.

If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

Usage Guidelines The description should provide useful information about this configuration.

do show

Executes all **show** commands while in Configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **do show**

Usage Guidelines Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character | is only available if the command is valid in the Exec mode.



Caution There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **end**

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description `exit`

Usage Guidelines Use this command to return to the parent configuration mode.

fault-unidirect-mode

Configures the unidirectional mode that generates fault messages for the connection's peer when local faults are detected and remote faults are received.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Ethernet Port Configuration

configure > **port ethernet** *slot_number/port_number*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

Syntax Description `[no] fault-unidirect-mode (clause-46 | clause-66)`

no fault-unidirect-mode

Disables fault message generation.

(clause-46 | clause-66)

clause-46: On local fault reception, continuous remote faults are sent. On remote fault reception, continuous idles are sent. [IEEE 802.3, Clause 46, Reconciliation Sublayer (RS) and 10 Gigabit Media Independent Interface (XGMII)]

clause-66: On local fault reception, frame transmit is continued, remote fault indication is sent during Inter-Frame Gap (IFG). On remote fault reception, frame transmit is continued. [IEEE 802.3, Clause 66, Extensions of the 10 Gb/s Reconciliation Sublayer (RS), 100BASE-X PHY, and 1000BASE-X PHY for unidirectional transport]

Usage Guidelines Configure the unidirectional mode that generates fault messages for the connection's peer when local faults are detected and remote faults are received.

Example

After flow control has been disabled, use the following command to enable flow control:

```
fault-unidirect-mode clause-46
```

flow-control

Enables and disables flow control on the ASR 5000 Quad Gig-E line card (QGLC) and 10-Gig-E line card (XGLC).

Product

PDSN
SGSN
GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number) #
```

Syntax Description

```
[ no ] flow-control
```

no

Disables flow control on the specified port.

Usage Guidelines

Flow control is enabled by default on the QGLC and can be disabled using the **no** command on a per-port basis. This command does not work on the Fast Ethernet Line Card (FELC) and Gigabit Ethernet Line Card (GELC/GLC2) which do not support flow control.

**Important**

Flow control must be enabled on all XGLCs in the chassis. To prevent XGLC shutdowns, you should also enable flow control at 6Gbps on the peer ports of all routers in your network that connect with the ASR 5000.

Example

After flow control has been disabled, use the following command to enable flow control:

```
flow-control
```

ingress-mode

Labels this port as an ingress port (incoming traffic).

Product

IPSG
SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

Syntax Description

[no] **ingress-mode**

no

Disables ingress port tag.

Usage Guidelines

Use this command to label this port in order for the session manager to recognize the interface from which IP data packets are being received. This command should be used in single context configurations. In single context configurations, the ingress port can only be identified if labeled.



Important

For IPSG context and service rules, regardless of number of contexts in the configuration, **ingress-mode** CLI command must be configured for ASR5500 and VPC-SI or VPC-DI platforms. This is done to give precedence to the two matching flows. For example, cases when IPv4SA or IPv4DA both are matched for the ingress packet, then if the incoming interface is designated as ingress, the lookup will be performed in the order of IPv4SA first and then IPv4DA. But if the **ingress-mode** is not set, priority is given to the IPv4DA flow. This is true only for ASR5500 and later platforms such as VPC-SI and VPC-DI.



Important

It is recommended to enable the **ingress-mode** configuration for IPv6 traffic to avoid packet drops.



Important

Do not enable this command for downlink interfaces. This command should only be applied to uplink interfaces.

link-aggregation

Aggregates ports on ASR 5500 Management Input/Output (MIO) cards, and sets related parameters in accordance with IEEE 802.3ad.

Product

WiMAX
 PDSN
 HA
 FA
 GGSN
 SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

Syntax Description

In releases prior to StarOS 21.26:

```
link-aggregation { distribution { block | random | rotate | simple } |
lacp { active | passive } [ rate { auto | fast | slow } ] [ timeout {
long | short } ] | master { global group group_number | group group_number |
local group group_number } | member { global group group_number | group
group_number | local group group_number [ min-link number_links mode {
non-redundant | redundant } ] } | redundancy { standard | switched } [
hold-time sec ] [ preferred slot { card_number | none } ] | toggle-link }
no link-aggregation [ toggle-link ]
default link-aggregation { distribution | lacp | redundancy | toggle-link
}
```

From StarOS 21.26 and later releases:

```
link-aggregation { distribution { block | random | rotate | simple } |
lacp { active | passive } [ rate { auto | fast | slow } ] [ timeout {
long | short } ] | primary { global group group_number | group group_number |
local group group_number } | member { global group group_number | group
group_number | local group group_number [ min-link number_links mode {
non-redundant | redundant } ] } | redundancy { standard | switched } [
hold-time sec ] [ preferred slot { card_number | none } ] | toggle-link }
no link-aggregation [ toggle-link ]
default link-aggregation { distribution | lacp | redundancy | toggle-link
}
```

```
distribution { block | random | rotate | simple }
```



Important The **distribution** keyword is not supported on the ASR 5500.

Configures link aggregation distribution and controls how a Link Aggregation Group (LAG) hash map is generated. This method is required for Equal Cost Multi-Path (ECMP) routing over LAG. Set this option on

the primary port for use with the whole group. The following list defines the distribution options (assuming port index 0,1,2,3 were selected):

block: Blocks of the same port index (Example: 0000111122223333)

random: Based on pseudo random number

rotate: Repetition of rotated port index (Example: 0123123023013012...)

simple: Repetition of all selected port indexes (Example: 0123012301230123...)

lacp { active | passive }

Configures the Link Aggregation Control Protocol (LACP). Set this option on the master port for use with the whole group.

active mode sends out LACP packets periodically. This is the default setting.

passive mode only responds to LACP packets received.

rate { auto | fast | slow }

Configures the rate at which the LACP sends packets.

auto: rate is controlled by the peer

fast: 1 second

slow: 30 seconds (Default) [ASR 5000 only]

timeout { long | short }

Configures LACP timeout events. Set this option on the master port for use with the whole group.

long: Set LACP to long timeout (30 seconds)

short: Set LACP to short timeout (3 seconds)

master { global group *group_number* | group *group_number* | local group *group_number* }

This command creates the Master port for the aggregated group.

global: Set group global across slots.

group *group_number*: Set link aggregation group number. The *group_number* must be an integer from 1 through 1023.

local: Set group local within same slot.

member { global group *group_number* | group *group_number* | local group *group_number* }

This command makes the port a member of the aggregated group.

global: Set group global across slots.

group *group_number*: Set link aggregation group number. The *group_number* must be an integer from 1 through 1023.

local: Set group local within same slot.

min-link *number_links*

Important This feature is only supported on the ASR 5500.

Specifies that a Link Aggregation Group (LAG) is up /usable only when a minimum number of links are available for aggregation. This guarantees that a minimum amount of bandwidth is available for use.

The *number_links* specifies the minimum number of links required to avoid a LAG switchover. It is an integer from 1 through 255.

When this feature is enabled, a LAG is not usable when the number of links in a LAG goes below the configured min-link value. Switchover to another LAG bundle (if available) automatically occurs when the number of links in the current active bundle goes below the configured min-link value.

mode { non-redundant | redundant }

Important This feature is only supported on the ASR 5500.

Specifies whether the LAG is configured in *non-redundant* (Active-Active mode) or *redundant* (Active-Standby) mode.

redundancy { standard | switched } [hold-time *sec*] [preferred slot { *card_number* | none }]

Connects ASR 5500 MIOs to different Ethernet switches. The master port must be set to make this effective for the group.

standard: Treats all cards in the group as one group. (Default)

switched: Assumes cards are connected to different switches. [ASR 5000 only]

hold-time *sec*: Sets the amount of time to hold (in seconds) before switching between cards. Applies to standard and switched modes. The *sec* must be an integer from 0 through 3600. Default: 10

preferred slot { *card_number* | none }: Specifies the preferred behavior for a LAG using two Ethernet switches. Applies to standard and switched modes. The *card_number* is an integer with value 5 or 6 on an ASR 5500.

When a card number is specified, system behavior varies based on the card type. For MIO (ASR 5500) card, the preferred slot is selected for the initial timeout period to make the selection of an Ethernet switch less random.

none: Specifies no preferred slot.

toggle-link

Important The **toggle-link** keyword is not supported on the ASR 5500.

Set to toggle link on port switch.

default

Restores the default values.

no

This command deletes the Ethernet port from any group it might be in. If the port was the Master of a group, the whole group would be deleted.

Usage Guidelines

Configure from one to four ports on a QGLC (vertical aggregation) or the single port on XGLCs (horizontal aggregation), or traffic ports on an MIO card to be in an aggregation group that links to an aggregation group on a remote Ethernet switch. Very large files can be downloaded across all ports in a group, which makes for a faster download when compared to serial downloads over a single link.

Related **link-aggregation** commands are described in the *Card Configuration Mode Commands* and *Global Configuration Mode Commands* chapters of this guide. For additional information, also refer to the *System Administration Guide*.

Example

The following example configures the port to be part of Master Group 2:

```
link aggregation master group 2
```

media

This command configures the port interface type. (ASR 5000 only)

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

configure > **port ethernet** *slot_number/port_number*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

Syntax Description

```
media { rj45 | sfp }
```

rj45

Sets the physical interface to a copper RJ-45 connector.

sfp

Sets the physical interface connection to optical Small Form Factor (SFP) gigabit via an SFP transceiver.

Usage Guidelines

Set the media option when the physical cabling interface is changed.

Example

The following command sets the physical interface to RJ-45:

```
media rj45
```

medium

Configures the port speed and communication mode. (ASR 5000 only)

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

Syntax Description

```
medium { auto | speed { 10 | 100 | 1000 | 10000 } duplex { full | half } }
```

```
{ auto | speed { 10 | 100 | 1000 | 10000 } duplex { full | half } }
```

Default: **auto**

Optionally sets the speed of the interface and the communication mode.

auto: Configures the interface to auto-negotiate the interface speed.

speed { **10** | **100** | **1000** | **10000** }: Specifies the speed to use at all times.

duplex { **full** | **half** }: Sets the communication mode of the interface to either **full** or **half** duplex.

**Important**

Ethernet networking rules dictate that if a device whose interface is configured to auto-negotiate is communicating with a device that is manually configured to support full duplex, the first device will negotiate to the manually configured speed of the second device but will only communicate in half duplex mode.

Usage Guidelines

Set the medium options when the physical interface changes.

**Important**

The **speed** keyword in the **medium** command is not supported on the ASR 5500.

Example

The following command configures the port's speed and communication mode to be auto-negotiated.

```
medium auto
```

The following command configures the port's interface speed to gigabit with full duplex communication.

```
medium speed 1000 duplex full
```

preferred slot

Assigns revertive or non-revertive control to port redundancy auto-recovery. (ASR 5x00 only)

Default: non-revertive operation

Product

PDSN
FA
HA
SGSN
GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

configure > **port ethernet** *slot_number/port_number*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

Syntax Description

[**no**] **preferred slot** *slot_number*

no

Disables revertive or auto-recovery operation for the selected port.

preferred slot *slot_number*

Identifies the physical chassis slot where the ASR 5500 MIO card is installed.

Usage Guidelines

This command enables or disables revertive port redundancy, wherein after a port failover, when the original port is restored to service (such as link up) the system will return service to that port automatically.

Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue an Exec mode **link-aggregation port switch to** command to return service to the original port.

This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual line card, SPIO, or an MIO card.



Important

This command is not supported on all platforms.

Example

For ASR 5000:

The following command identifies the chassis slot 17 where the line card or SPIO card is installed.

preferred slot 17

For ASR 5500:

The following command identifies the chassis slot 5 where the MIO card is installed.

preferred slot 5

shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, the port is enabled with the use of the **no** keyword.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number) #
```

Syntax Description

[**no**] **shutdown**

no

Enables the port and places it in service.

Usage Guidelines

Shuts down a port prior to re-cabling and/or other maintenance activities.

This command powers down the ports on MIO/UMIO cards (ASR 5500).

To enable a port (bring it into service) use the **no** keyword.

Example

Use the following command to disable the port:

shutdown

Use the following command to enable the port for service:

no shutdown

snmp trap link-status

Enables or disables the generation of an SNMP trap for link status changes.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

configure > **port ethernet** *slot_number/port_number*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

Syntax Description

[**no**] **snmp trap link-status**

no

Disables the sending of traps for link status changes.

Usage Guidelines

Enable link status change traps when a monitoring facility can use the information or if there are troubleshooting activities in progress.

Example

Use the following command to disable sending of traps:

```
no snmp trap link-status
```

srp virtual-mac-address

Configures the Standby Router Protocol (SRP) virtual MAC address for the port on an ICSR chassis.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

configure > **port ethernet** *slot_number/port_number*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

Syntax Description

srp virtual-mac-address *mac_address*
no srp virtual-mac-address

no

Disables the SRP virtual MAC addressing for Ethernet ports. The block of virtual MAC addresses is not saved.

mac_address

Enables SRP virtual addressing for the specified MAC address. The MAC address should be specified as six groups of two hexadecimal digits separated by hyphens. For example, 01-23-45-67-89-ab.

Usage Guidelines

The SRP virtual MAC address is applied to the port when the chassis is in SRP ACTIVE state. The default is **no srp virtual-mac-address**.



Important This command is not supported on all platforms.

Example

Use the following command to enable the SRP's virtual MAC addressing:

```
srp virtual-mac-address 09-33-48-67-99-ae
```

threshold high-activity

Configures thresholds for high port activity for the port.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

Syntax Description

```
threshold high-activity high_thresh [ clear low_thresh ]
```

high_thresh

Specifies the high threshold high port activity percentage that must be met or exceeded within the polling interval to generate an alert or alarm. The percentage is expressed as an integer from 0 through 100. Default: 50

clear

Allows the configuration of the low threshold.

low_thresh

Specifies the low threshold high port activity percentage that maintains a previously generated alarm condition. If the activity percentage falls below the low threshold within the polling interval, a clear alarm will be generated. The percentage is expressed as an integer from 0 through 100. Default: 50



Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

High port activity thresholds generate alerts or alarms based on the utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis.

Alerts or alarms are triggered for high port activity based on the following rules:

- **Enter condition:** Actual percent utilization of a port is greater than High Threshold.
- **Clear condition:** Actual percent utilization of a port is less than Low Threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command in the *Global Configuration Mode Commands* chapter to configure the polling interval and the **threshold monitoring** command in this chapter to enable thresholding for this value.

Example

The following command configures a high port utilization threshold percent of 70 and a low threshold percent of 50 for a system using the Alarm thresholding model:

```
threshold high-activity 70 clear 50
```

threshold monitoring

Enables or disables thresholding for port-level values.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

Syntax Description

[no] **threshold monitoring**

no

Disables threshold monitoring for port-level values. This is the default setting.

Usage Guidelines

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (such as high-activity) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. Thresholding helps identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the `starentMIB(8164).starentTraps(2)` section of the *SNMP MIB Reference*. The generation of specific SNMP traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.
- **Logs:** The system provides a facility called `threshold` for which active and event logs can be generated. As with other system facilities, logs are generated. Log messages pertaining to the condition of a monitored value are generated with a severity level of `WARNING`.
- **Alarm System:** High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists and/or a condition clear alarm is generated.

"Outstanding" alarms are reported to through the system's alarm subsystem and are viewable through the system's CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

Table 1: Thresholding Reporting Mechanisms by Model

Model	SNMP Traps	Logs	Alarm System
Alert	X	X	
Alarm	X	X	X

This command enables thresholding for port-level values. Refer to the **threshold high-activity**, **threshold rx-utilization**, and **threshold tx-utilization** commands in this chapter for information on configuring these values. In addition, refer to the **threshold poll** command in the *Global Configuration Mode Commands* chapter for information on configuring the polling interval over which these values are monitored.

threshold rx-utilization

Configures thresholds for receive port utilization.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number) #
```

Syntax Description `threshold rx-utilization high_thresh [clear low_thresh]`

high_thresh

Specifies the high threshold receive port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. The percentage is expressed as an integer from 0 through 100. Default: 80

clear

Allows the configuration of the low threshold.

low_thresh

Specifies the low threshold receive port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a Clear Alarm will be generated. The percentage is expressed as an integer from 0 through 100. Default: 80



Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis.



Important Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive **or** transmit utilization threshold be configured.

Alerts or alarms are triggered for receive port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for received data is greater than High Threshold
- **Clear condition:** Actual percent utilization of a port for received data is less than Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command in the *Global Configuration Mode Commands* chapter to configure the polling interval and the **threshold monitoring** command in this chapter to enable thresholding for this value.

Example

The following command configures a receive port high utilization threshold percent of 70 and a low threshold percent of 50 for an system using the Alarm thresholding model:

```
threshold rx-utilization 70 clear 50
```

threshold tx-utilization

Configures thresholds for transmit port utilization.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

configure > **port ethernet** *slot_number/port_number*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number) #
```

Syntax Description

threshold tx-utilization *high_thresh* [**clear** *low_thresh*]

high_thresh

The high threshold transmit port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. The percentage is expressed as an integer from 0 through 100. Default: 80

clear

Allows the configuration of the low threshold.

low_thresh

The low threshold transmit port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated. The percentage is expressed as an integer from 0 through 100. Default: 80



Important

This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis.



Important

Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive **or** transmit utilization threshold be configured.

Alerts or alarms are triggered for transmit port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for transmit data is greater than High Threshold
- **Clear condition:** Actual percent utilization of a port for transmit data is less than Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command in the *Global Configuration Mode Commands* chapter to configure the polling interval and the **threshold monitoring** command in this chapter to enable thresholding for this value.

Example

The following command configures a transmit port high utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold tx-utilization 70 clear 50
```

vlan

Enters VLAN Configuration mode. Creates VLAN if necessary.

Product

HA
HSGW
PDSN
P-GW
SAEGW
SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

Syntax Description

```
vlan vlan_id [ inline-process | subscriber-vlan ] [ -noconfirm ]
```

vlan_id

Specifies a VLAN identifier as an integer from 1 through 4094. If this identifier does not already exist you are prompted to confirm the identifier an a new one is created.

inline-process

Specifies that this VLAN will be used for inline processing.

subscriber-vlan

Specifies that this VLAN will be used for subscriber-based processing.

-noconfirm

Specifies that the command must execute without any prompts and confirmation from the user.

Usage Guidelines

Use this command to specify an existing VLAN ID or create a new VLAN ID and enter the VLAN Configuration mode.

For additional information, refer to the *VLAN Configuration Mode Commands* chapter.

Example

The following command creates the VLAN ID 234.

```
vlan 234
```

```
Are you sure? [Yes|No]: y
```

