



# Serial Link Parameter Monitoring and Control

---

This feature monitors parameters on various physical links (PA-4T, PA-4T+, PA-8T-XX, PA-A3-XX, PA-MC-8T1 and PA-MC-8E1) and sends traps/execute control actions based on the values of the monitored parameters. This feature is supported on FSIP.

## Feature Specifications for the Serial Link Parameter Monitoring and Control

---

### Feature History

Release	Modification
12.3(1)	This feature was introduced.

---

### Supported Platforms

For platforms supported in Cisco IOS Release 12.3(1), consult Cisco Feature Navigator.

---

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Additional References, page 3](#)
- [Command Reference, page 5](#)
- [Information About Serial Link Parameter Monitoring and Control, page 2](#)



---

**Corporate Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

# Information About Serial Link Parameter Monitoring and Control

To configure Serial Link Parameter Monitoring and Control, you need to understand the following concepts:

- [Monitoring, page 2](#)
- [Major and Minor Monitoring Intervals, page 2](#)
- [Restart Delay, page 3](#)
- [Restart Attempts, page 3](#)

## Monitoring

This feature is designed to monitor the occurrences of various parameters on the PA-4T+, PA-8T-232, PA-8T-V35, PA-A3-T3/E3/OC3, PA-MC-8T1/E1, CX-FSIP8 port adapters in Cisco 7500 series routers. The monitoring algorithm counts the occurrences of these error and non-error parameters in a configurable monitoring time interval. It also compares the counts with configured thresholds (low and high); if the count of a parameter exceeds the configured lower threshold, then a trap is sent identifying the corresponding parameter and the interface. If the count of a parameter exceeds the configured higher threshold in the monitoring interval, a trap is sent.

The link is shut down if the restart mechanism is enabled; subsequently, in an attempt to make the link operational again, the link is restarted (after a configurable restart delay). If the link is not brought up this would be considered as a failed restart attempt. Another attempt will be made to restart the link after another restart delay and so on. Also if the high threshold is reached/exceeded again, within the first major monitoring interval since the link was brought up, the link will be shut down again. This would also be considered as a failed restart attempt.

The number of consecutive failed restart attempts could be configured to have an upper limit which when exceeded would cause the link to be shut permanently.

The word trap and notification have been used interchangeably while discussing the traps that are sent when a particular threshold is reached/exceeded. The CISCO-IF-MONITOR-NOTIF MIB will be used to send the traps. Information of the last trap sent from a particular interface could be obtained via this MIB. The MIB would also maintain the total number of traps sent by the SNMP agent (this particular router). This count would be included in the trap sent to the NMS. NMSs should track the value of this object (cIfMonNotifCount) received in each notification. If the difference in the value of this object across two consecutive notifications is more than one, a notification has been delayed, dropped, lost or routed out of sequence. The only reliable way to recover such notifications is via the NOTIFICATION-LOG-MIB. The NMS should preferably configure/create a log in the NOTIFICATION-LOG-MIB to capture notifications sent when a particular threshold is reached/exceeded. If possible, a named log should be created. When a notification loss is detected, the NMS can then poll the log to determine which notification was lost.

## Major and Minor Monitoring Intervals

A major monitoring interval consists of a number of minor monitoring intervals. Every minor monitoring interval the parameter count for the last major monitoring interval is compared with the predefined (high or low) thresholds. You can set the number of minor intervals per major interval using the **link monitor samples** command.

## Restart Delay

The restart delay is the amount of time which the software waits before it attempts to restart a link that was shut down. This usually occurs because the high threshold limit for a particular parameter on the link was reached or exceeded in the monitoring interval and the shut down configuration option was enabled (i.e., the restart mechanism is enabled). Another attempt will be made to restart the link after another restart delay if the link was not brought up in the previous attempt.

## Restart Attempts

The restart attempt specifies the upper limit on number of allowed consecutive failed restart attempts. The link is shut down if the restart mechanism is enabled and the high threshold has been reached or exceeded; subsequently, in an attempt to make the link operational again, the link is restarted (after a configurable restart delay). If the link is not brought up this would be considered as a failed restart attempt. Another attempt will be made to restart the link after another restart delay and so on. Also, if the high threshold is reached/exceeded again, within the first major monitoring interval since the link was brought up, the link will be shut down again. This would also be considered as a failed restart attempt. The number of back-to-back failed restart attempts could be configured to have an upper limit which when exhausted would cause the link to be shut permanently since no more attempts will be made to restart the link.

The link has to be brought up again if monitoring of parameters on the link needs to be resumed for a link, which is down. If the restart attempts is set to '0' then no attempt will be made to restart the link once it is brought down by the algorithm.

## Additional References

For additional information related to Serial Link Parameter Monitoring and Control, refer to the following references:

## Related Documents

Related Topic	Document Title
Additional router configuration commands	<i>Cisco IOS Configuration Fundamentals Command Reference</i> , Release 12.3

## Standards

Standards <sup>1</sup>	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

1. Not all supported standards are listed.

## MIBs

MIBs <sup>1</sup>	MIBs Link
<ul style="list-style-type: none"> <li>CISCO-IF-MONITOR-NOTIF-MIB</li> <li>NOTIFICATION-LOG-MIB</li> </ul>	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

1. Not all supported MIBs are listed.

## RFCs

RFCs <sup>1</sup>	Title
<ul style="list-style-type: none"> <li>RFC 3014</li> </ul>	<i>Notification Log MIB</i>

1. Not all supported RFCs are listed.

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

# Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3 command reference publications.

## New Commands

- [debug link monitor](#)
- [link monitor](#)
- [link restart](#)
- [link monitor samples](#)
- [show interface link monitor](#)
- [show link monitor debug](#)
- [snmp-server enable traps if-monitor](#)
- [snmp trap if-monitor](#)

# debug link monitor

To display the statistics of the executing process, use the **debug link monitor** command in privileged EXEC mode. To disable **debug link monitor**, use the **no** form of this command.

**debug link monitor**

**no debug link monitor**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.3(1)	This command was introduced.

**Usage Guidelines** This command is used to display the statistics, which are used for debugging the status of the various conditions occurred during execution of the monitoring process.

**Examples** The following example enables link monitoring statistics:

```
Router# debug link monitor
%DEBUG-ENABLED Error Rate Link Monitor
```

The following example disables link monitoring statistics:

```
Router# no debug link monitor
%DEBUG-DISABLED Error Rate Link Monitor
```

Related Commands	Command	Description
	<b>aebug all</b>	Enables debugging for link monitoring.
	<b>no debug all</b>	Disables debugging for link monitoring.
	<b>clear counters</b>	Clears show interface counters on all interfaces.
	<b>show link monitor debug</b>	Show link monitor error statistics.

# link monitor

To set error rate limits and monitoring interval, use the **link monitor** command in interface configuration mode. To disable **link monitor**, use the **no** form of this command.

**link monitor** {**aborts** | **crc** | **disc** | **drops** | **flaps** | **frame-reject** | **frmr** | **runts** | **sabm**}

**no link monitor** {**aborts** | **crc** | **disc** | **drops** | **flaps** | **frame-reject** | **frmr** | **runts** | **sabm**}

**link monitor** {**aborts** | **crc** | **disc** | **drops** | **flaps** | **frame-reject** | **frmr** | **runts** | **sabm**} *interval*

**link monitor** {**aborts** | **crc** | **disc** | **drops** | **flaps** | **frame-reject** | **frmr** | **runts** | **sabm**} *interval* **threshold high** *high* **low** *low*

## Syntax Description

<b>aborts</b>	Set threshold limits for aborted packet.
<b>crc</b>	Set threshold limits for crc errors in received packets.
<b>disc</b>	Set threshold for received disconnect command.
<b>drops</b>	Set threshold limits for input packets dropped.
<b>flaps</b>	Set threshold limits for link flaps.
<b>frame-reject</b>	Set threshold limits for rejected HDLC frames.
<b>frmr</b>	Set threshold for frame rejects.
<b>runts</b>	Set threshold limits for dropped frame runts.
<b>sabm</b>	Set threshold limit for received SABM commands.
<i>interval</i>	5-600 seconds.
<i>high</i>	1-100000.
<i>low</i>	1-100000.

## Defaults

<i>interval</i>	60 seconds.
<i>high</i>	Varies; dependent on parameter.
<i>low</i>	Varies; dependent on parameter.

## Command Modes

Global configuration.

## Command History

Release	Modification
12.3(1)	This command was introduced.

---

**Usage Guidelines**

If the Major interval or high/low thresholds are not mentioned then their default values are used. The user will get the option to reset the value to the default or keep it as the previously set value if and only if the user has previously set the value which is something other than the default and the user does not enter the value while changing other parameters.

While configuring thresholds, all three values (interval, high and low threshold) should be configured together otherwise the default will be taken for the ones that are not actually configured. The high threshold should not be less than the lower threshold.

The X.25 parameters can be configured for monitoring only if X.25 is configured on the interface. X25 cannot be configured on the ATM port adaptors. When X.25 encapsulation is disabled, the timers for the configured X.25 parameters will continue to run. However, the parameter values will not be monitored which would imply that traps will not be sent. The user has to explicitly disable monitoring for any parameter in order to completely stop monitoring (which includes stopping the timers).

---

**Examples**

The following example shows setting the aborts interval and high and low thresholds:

```
Router(config-if)#link monitor aborts interval 100 threshold high 300 low 50
Router(config-if)#link monitor aborts
High Threshold  current: 300  default: 100
Reset the high threshold to the default value? [no]: yes
Low Threshold  current: 50  default: 10
Reset the low threshold to the default value? [no]:
Major Interval current: 100  default: 60
Reset the major interval to the default value? [no]:
```

# link restart

To set the restart delay and restart attempts for the current link, use the **link restart** command in interface configuration mode. To disable **link restart**, use the **no** form of this command.

**link restart** *attempts delay*

**no link restart**

## Syntax Description

<i>attempts</i>	Set restart attempts.
<i>delay</i>	Set restart delay in seconds.

## Defaults

The default restart delay is 300 seconds.

## Command Modes

Interface configuration.

## Command History

Release	Modification
12.3(1)	This command was introduced.

## Usage Guidelines

If any parameter (delay or attempts) is not explicitly mentioned, the default will be taken. The user will get the option to reset the value to the default or keep it as the previously set value if and only if the user has previously set the value which is something other than the default and the user does not enter the value while changing other parameters.

If the 'attempts' is configured as 0 then the link will be shut permanently the very first time the high threshold is reached/crossed. The delay value is of no use in this case.

The link has to be brought up again via **no shut** if monitoring of parameters on the link needs to be resumed for a link, which is brought down permanently by the restart mechanism.

If the link has been brought down by the link monitoring feature and the user enters **shut** or **no link restart** before a restart attempt is made, then the restart attempt will not be made and the link will continue to be down.

## Examples

The following example shows the restart delay being set to 60 and the restart attempts to 10:

```
Router(config-if)#link restart delay 60 attempts 10
```

# link monitor samples

To set the number of minor intervals per major interval, use the **link monitor samples** command in global configuration mode. To disable **link monitor samples**, use the **no** form of this command.

**link monitor** {**samples** | **parameters**} *interval*

**no link monitor samples**

## Syntax Description

<i>interval</i>	Minor intervals per major monitoring interval.
<b>samples</b>	Set the number of minor intervals per major interval.
<b>parameters</b>	Enable Link Monitoring for all configured parameters.

## Defaults

The default restart delay is 300 seconds.

## Command Modes

Global configuration.

## Command History

Release	Modification
12.3(1)	This command was introduced.

## Usage Guidelines

These commands can be used to fine tune the feature.

## Examples

The following example shows setting the number of minor intervals per major interval to 5:

```
Router(config)#link monitor samples 5
```

# show interface link monitor

To show the link monitoring and restart configuration for all configured parameters for that interface., use the **show interface link monitor** command in EXEC configuration mode.

**show interface** *interface name* **link {monitor | value}**

Syntax Description	monitor	value
	Shows the link monitoring and restart configuration for all configured parameters for that interface.	Shows the various parameter values in the last major monitoring interval. This command will display only the values for configured parameters.

**Defaults** No default behavior or values.

**Command Modes** EXEC configuration.

Command History	Release	Modification
	12.3(1)	This command was introduced.

**Usage Guidelines** Use this command to show the various parameter values in the last major monitoring interval.

**Examples** The following example shows the output from link monitoring on a serial interface:

```
Router#show interface serial 0/0/0 link monitor
LINK PARAMETER MONITOR CONFIGURATION

Enabled-Parameter  High-Threshold  Low-Threshold  Monitor-Interval(seconds)
  aborts             35                13                30
  crc                 10000             10                60
  input-drops        1000              500               60
  flaps               3                  2                  60
  frame-rejects      100                10                60
  runts               10000             10                60
Restart-Delay(seconds) 60   Restart-Attempts 2
Number of Minor intervals per Major interval 5
```

The following example shows the output from link monitoring on a serial interface:

```
Router#show interface serial 0/0/0 link value
  aborts           : 0
  crc              : 0
  input-drops      : 0
  flaps            : 0
  frame-rejects    : 0
  runts            : 0
```

# show link monitor debug

To show the various statistics of the link monitoring and restart feature, use the **show link monitor debug** command in global configuration mode.

## show link monitor debug

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC configuration.

Command History	Release	Modification
	12.3(1)	This command was introduced.

**Usage Guidelines** The statistics include the IPC messages sent to and received from the VIPs. It also includes the malloc failures, the number of times the link monitoring structure was found NULL, and the number of times the configuration of the RSP was not sent to the VIP during bootup of the VIP.

**Examples** The following example shows the output from link monitoring on a serial interface:

```
Router#show link monitor debug
Link Monitor Error Statistics

CONF STRUCTURE FOUND NULL.....0
CONF STRUCTURE MALLOC FAIL.....0
IPC SENT TOTAL.....25
IPC RECV TOTAL.....3
CCB CMD SENT TOTAL.....94
LOVE LETTER RECV TOTAL.....1
IPC SEND FAILURE.....1
IPC RECV FAILURE.....0
CCB CMD SEND FAILURE.....0
LOVE LETTER RECV FAILURE.....0
CONFIG RESEND TO LC FAIL.....0
CHUNK ELEMENT FREE FAIL.....0
CHUNK ELEMENT MALLOC FAIL.....0
ELEMENTS IN TRAP QUEUE.....0
TRAP FAIL ENQUEUE.....0
WATCHED QUEUE CREATED
CHUNK CREATED
```

[Table 1](#) describes the significant fields shown in the display.

**Table 1** *show link monitor debug Field Descriptions*

<b>Field</b>	<b>Description</b>
Conf Structure Found Null	This specifies the number of times the link monitor sub-block was found to be NULL.
Conf Structure Malloc Fail	This specifies the number of times we were unable to allocate memory for the link monitor sub-block structure.
Config Resend To LC Fail	This specifies the number of times we failed to resend the configuration to the linecard.
Chunk Element Free Fail	This specifies the number of chunk elements that were not freed properly.
Chunk Element Malloc Fail	This specifies the number of chunk element requests that were rejected. This is also the number of traps that were dropped.
Elements In Trap Queue	This specifies the number of traps which are currently enqueued in the link monitor queue (waiting to be sent out).
Trap Fail Enqueue	This specifies the number traps that were not enqueued in the link monitor queue. The traps which are not enqueued are dropped.
Watched Queue Created	This specifies if the link monitor queue is created or not. If this is not created, the traps will not be sent out.
Chunk Created	This specifies if the chunk of memory is created or not. If this is not created, the traps will not be sent out.

# snmp-server enable traps if-monitor

To enable or disable the generation of a family of traps, use the **snmp-server enable traps if-monitor** command in global configuration mode. To disable **snmp-server enable traps if-monitor**, use the **no** form of this command.

**snmp-server enable traps if-monitor**

**no snmp-server enable traps if-monitor**

---

**Syntax Description** This command has no arguments or keywords.

---

**Defaults** No default behavior or values.

---

**Command Modes** Global configuration.

---

Command History	Release	Modification
	12.3(1)	This command was introduced.

---



---

**Usage Guidelines** The if-monitor option enables the if-monitor red/yellow threshold traps for the link monitor feature. To enable the traps for a particular interface, the traps would have to be explicitly enabled on that interface in addition to the global command.

---

**Examples** The following shows using the **snmp-server enable traps if-monitor** to enable if-monitor traps on all interfaces:

```
Router(config)#snmp-server enable traps if-monitor
```

# snmp trap if-monitor

To enable the if-monitor traps for a particular interface, use the **snmp trap if-monitor** command in interface configuration mode. To disable **snmp trap if-monitor**, use the **no** form of this command.

**snmp trap if-monitor**

**no snmp trap if-monitor**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default behavior or values.

## Command Modes

Interface configuration.

## Command History

Release	Modification
12.3(1)	This command was introduced.

## Usage Guidelines

Traps will be sent for a particular interface only if both the global and the interface commands are enabled.

## Examples

The following shows using the **snmp-server enable traps if-monitor** to enable if-monitor traps on all interfaces:

```
Router(if-config)#snmp-server enable traps if-monitor
```

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

■ snmp trap if-monitor