

# Table of Contents

<b><u>Uses of Network Management for Monitoring the IP Packet Blocks Input Queue PSIRT Advisory</u></b> .....	1
<u>Document ID: 44104</u> .....	1
<u>Introduction</u> .....	1
<u>Prerequisite</u> .....	1
<u>Problem Statement</u> .....	1
<u>Problem Characteristics</u> .....	2
<u>Network Management Options Summary</u> .....	3
<u>Network Management Methodologies</u> .....	4
<u>Device Availability Monitoring</u> .....	4
<u>Device MIB Monitoring</u> .....	4
<u>Cisco Service Assurance Agent</u> .....	4
<u>RMON Alarm and Events</u> .....	6
<u>Overview</u> .....	6
<u>Example RMON Alarm and Events Configuration</u> .....	6
<u>Event–MIB</u> .....	7
<u>Overview</u> .....	7
<u>Example Event–MIB Configuration</u> .....	8
<u>CiscoWorks RME Network</u> .....	9
<u>Using CiscoWorks RME Network Show Commands</u> .....	9
<u>Scripted CiscoWorks RME Network Show Commands</u> .....	11
<u>Related Information</u> .....	12

# Uses of Network Management for Monitoring the IP Packet Blocks Input Queue PSIRT Advisory

Document ID: 44104

---

## **Introduction**

### **Prerequisite**

- Problem Statement
- Problem Characteristics
- Network Management Options Summary

### **Network Management Methodologies**

- Device Availability Monitoring
- Device MIB Monitoring
- Cisco Service Assurance Agent

### **RMON Alarm and Events**

- Overview
- Example RMON Alarm and Events Configuration

### **Event-MIB**

- Overview
- Example Event-MIB Configuration

### **CiscoWorks RME Network**

- Using CiscoWorks RME Network Show Commands
- Scripted CiscoWorks RME Network Show Commands

### **Related Information**

---

## **Introduction**

This paper provides network management options for detection of the input queue issue.

The IP Packet Blocks Input Queue PSIRT advisory is posted at

- <http://www.cisco.com/warp/customer/707/advisory.html>
- <http://www.cisco.com/warp/customer/707/cisco-sa-20030717-blocked.shtml>

**Note:** Keep in touch with your Sales account team, TAC representative, and/or Advanced Services Network Consulting Engineer for information as it becomes available.

## **Prerequisite**

### **Problem Statement**

This issue manifests itself as an input queue blockage, also known as a wedge condition, where incoming packets terminating on a router are not accepted. Eventually routing table updates expire and cause routing issues. ARP cache entries eventually expire and traffic stops. In the time frame between when the input queue gets wedged and routing/ARP problems occur, traffic transiting through the router still occurs normally.

Network management solutions focus on certain indicators for warning that the issue is occurring, with the intention of stopping it before the condition becomes terminal to proper operation of the router. The monitoring solutions can also be used to identify routers that have already succumbed to the issue and are no

longer passing traffic.

## Problem Characteristics

### Monitoring Input Queue Drops

You can monitor an interface input queue for dropped packets through the following SNMP MIB object.

```
.1.3.6.1.4.1.9.2.2.1.1.26
locIfInputQueueDrops OBJECT-TYPE
    -- FROM OLD-CISCO-INTERFACES-MIB
    SYNTAX          Integer
    MAX-ACCESS      read-only
    STATUS          Mandatory
    DESCRIPTION     "The number of packets dropped because the
                    input queue was full."
 ::= { iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) cisco(9) local(2) linterf
```

You can use the IOS **show interface X** command to reveal the interface queue statistics.

```
router>show interface
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1eXX.XXXX (bia 00e0.1eXX.XXXX)
  Internet address is XXX.XXX.XXX.XXX/XX
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 3/75, 42 drops
```

Output may also look like the following:

```
Router>show interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is 0050.500e.f1e0 (bia 0050.500e.f1e0)
  Internet address is 172.16.1.9/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:41, output 00:00:07, output hang never
  Last clearing of "show interface" counters 00:07:18
  Input queue: 76/75/1091/0 (size/max/drops/flushes); Total output drops: 0
                    ^^^^^^^^^^^^^^^^^^ ----> blocked
```

The input queue values are important.

The default value for most interfaces is 75 packets per input queue. A value of 3/75/0/0 means that there are three packets held in the input queue, 75 packet capacity, 0 packets dropped, and the input queue was flushed 0 times. The input queue size can be modified in the router configuration with the interface-level **hold-queue XX in** command. If your command output shows a number other than the 75 packet default, the key thing to remember is if the Input Queue values are X / Y / (increasing number) / # and X > Y, you may be experiencing the issue from the PSIRT advisory and should contact the Cisco TAC.

If the input queue is wedged, process-switched packets start to drop due to the lack of queue space and the third value increments. This third value in the **show** command can be monitored through SNMP and is reflected in the `locIfInputQueueDrops` MIB object.

## Monitoring Incoming ARP Packets

If an interface input queue wedges, it stops responding to process-switched packets such as ARP. ARP traffic can be monitored with the following SNMP MIB object.

```
.1.3.6.1.4.1.9.2.2.1.1.106
locIfarpInPkts OBJECT-TYPE
    -- FROM OLD-CISCO-INTERFACES-MIB
    SYNTAX          Counter
    MAX-ACCESS      read-only
    STATUS          Mandatory
    DESCRIPTION     "Arp protocol input packet count"
 ::= { iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) cisco(9) local(2) linterf
```

In a properly operating Ethernet segment PCs and Servers routinely ARP for other devices. When the sought after device is on the same segment the router does not respond to the ARP request. A router responds to an ARP if it is routing traffic for the requested device. Even if the router isn't responding to the ARP it increments its `locIfarpInPkts` counter as it sees the incoming packets.

If the interface becomes wedged, this counter no longer increments despite broadcast ARPs continuing to be sent on the segment.

```
OLD-CISCO-INTERFACES-MIB::locIfarpInPkts.1 = Counter32: 13
OLD-CISCO-INTERFACES-MIB::locIfarpInPkts.1 = Counter32: 34
OLD-CISCO-INTERFACES-MIB::locIfarpInPkts.1 = Counter32: 48
OLD-CISCO-INTERFACES-MIB::locIfarpInPkts.1 = Counter32: 70
OLD-CISCO-INTERFACES-MIB::locIfarpInPkts.1 = Counter32: 89
OLD-CISCO-INTERFACES-MIB::locIfarpInPkts.1 = Counter32: 104
```

(Interface Input Queue Wedged)

```
OLD-CISCO-INTERFACES-MIB::locIfarpInPkts.1 = Counter32: 121
OLD-CISCO-INTERFACES-MIB::locIfarpInPkts.1 = Counter32: 121
OLD-CISCO-INTERFACES-MIB::locIfarpInPkts.1 = Counter32: 121
OLD-CISCO-INTERFACES-MIB::locIfarpInPkts.1 = Counter32: 121
&
```

## Network Management Options Summary

There are a few network management features that may be used to provide network monitoring for this advisory.

1. Device Availability Monitoring
2. SNMP MIB object monitoring
3. Cisco Service Assurance Agent (Cisco SAA)
4. RMON Alarm and Events
5. Event-MIB
6. CiscoWorks RME Network Show Commands and CLI scripting

# Network Management Methodologies

## Device Availability Monitoring

The issue manifests itself as the interface input queue filling up and not releasing queued packets, resulting in a wedged interface condition. Once the interface input queue is filled and not accepting any more process-switched packets the interface starts to drop process-switched packets and features that require time-based updates such as routing updates, and ARP cache updates fail. Traffic that is transiting the router still flows until the ARP cache timers expire (within four hours per entry). Device Availability Monitoring is as simple as ping tests to the device. Many applications perform this function well, such as CiscoWorks RME Availability Monitor, HP Openview Network Node Manager, Tivoli Netview, and What sUp Gold. Device Availability Monitoring is necessary in any network management solution, but may be less effective in this situation as the pings or availability probes only fail when the interface stops passing traffic. The follow-on solutions that monitor Input Queue Drops and ARP packets give an earlier warning since those occur before the device/interface becomes totally unavailable.

## Device MIB Monitoring

When an interface input queue fills and packets are dropped the `locIfInputQueueDrops` MIB object increments.

ARP packets are also dropped, these can be monitored through the `locIfarpInPkts` MIB object.

Network Management Servers can monitor the remote device to baseline the counter statistics and alarm when the counter values increase unexpectedly.

Tools that perform SNMP MIB object collection are usually performance management solutions, such as HP Openview Network Node Manager, Concord eHealth suite, InfoVista, and MRTG.

This type of solution is moderately easy to implement, but requires extensive, periodic polling of the network in order to quickly determine if input queues are wedged. In a large-scale environment, centralized polling at high rates may prove to increase network traffic undesirably.

## Cisco Service Assurance Agent

### Cisco Service Assurance Agent

Cisco Service Assurance Agent (SAA) is an availability and latency monitoring tool that is built into Cisco IOS. The feature has been available since IOS Release 11.2 in its most basic state of an IP pinger through the `ICMPEcho` operation.

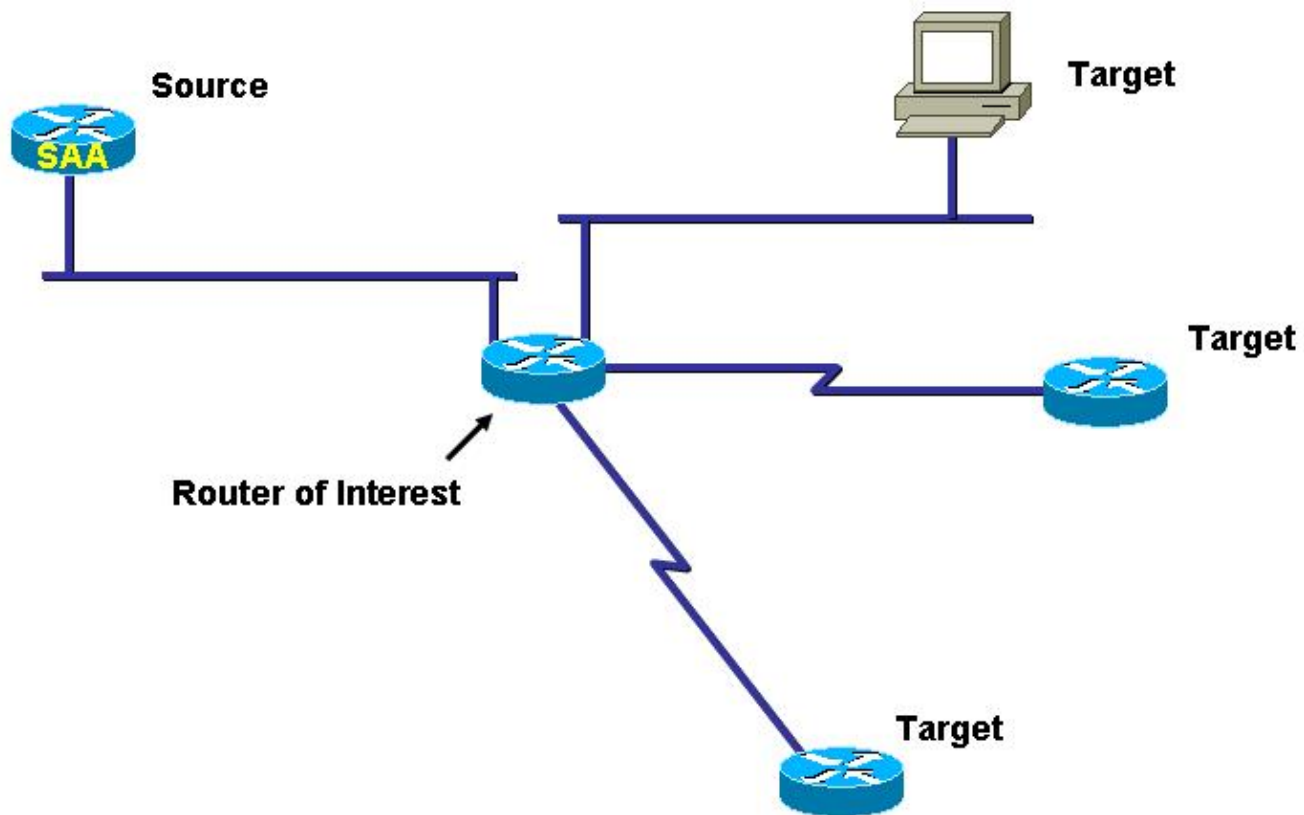
Cisco SAA is an excellent synthetic traffic generator that can be used to send ping packets from a source router, through a router of interest and to a target IP address. If the Cisco SAA operation fails the source router can send an SNMP trap to a fault management station, such as Cisco Info Center, Micromuse Netcool, HP Openview Network Node Manager, and Tivoli Netview.

More background on the Cisco SAA feature can be found at:

- <http://www.cisco.com/go/saa>
- <http://www.cisco.com/warp/customer/732/Tech/nmp/saa/docs/networkers2002.pdf>

## Example Cisco SAA Deployment

We need to configure the Cisco SAA feature on a source router to send traffic streams from it, through routers of interest, to IP-enabled devices or targets.



If the source cannot reach the target, then it is possible that the intermediary router(s) has a wedged interface and the ARP cache has expired resulting in no transit traffic occurring.

Cisco SAA is similar to device availability monitoring solutions when the target device is set as the Router of Interest.

Cisco SAA performs path and service availability when the target is an IP-enabled device that requires the SAA operation to send traffic through the Router of Interest.

## Example Cisco SAA Configuration

In order to complete this section we must have a source router to send synthetic traffic from. This can be an existing router or we can re-use a decommissioned, low-end router for this task. We must also have the IP address of the target device.

In this example we are building an SAA collection to send 10 64-byte ping packets to a target IP of 10.1.2.3. The threshold for latency is one second (1000ms). If the packet times-out or we get three consecutive

responses over one second, a trap be fired to the trap receiver defined in the source router config.

```
rtr 1
  type echo protocol ipIcmpEcho 10.1.2.3
  num-packets 10
  request-data-size 64
  threshold 1000
rtr reaction-configuration 1 timeout-enable threshold-type consecutive 3 threshold-falling
rtr schedule 1 start-time now
```

Cisco SAA can also be configured with the CiscoWorks Internetwork Performance Monitor application from the Routed WAN (RWAN) Bundle.

## RMON Alarm and Events

### Overview

The RMON Alarm and Events feature has been in IOS since release 11.1. Even though most routers don't support the full RMON-1 specification, they support the reduced Alarm and Events categories.

For tips on configuring this feature through IOS commands:

<http://www.cisco.com/warp/customer/477/RMON/18.html>

For tips on configuring this feature through SNMP:

[http://www.cisco.com/warp/customer/477/RMON/alarm\\_event.shtml](http://www.cisco.com/warp/customer/477/RMON/alarm_event.shtml)

### Example RMON Alarm and Events Configuration

The locIfInputQueueDrops MIB object is also known to IOS as lifEntry.26. The following IOS configuration statements define an RMON event that sends an SNMP trap and an RMON alarm that invoke the event when the input queue drop counter starts to increase. Ensure that your router configuration has an `snmp-server host #.#.#.#` statement to direct SNMP traps to your event console.

```
rmon event 1 trap public description "Interface Queue Drop Event" owner noc
rmon alarm 1 lifEntry.26.1 60 delta rising-threshold 2 1 falling-threshold 1 owner noc
rmon alarm 1 lifEntry.26.2 60 delta rising-threshold 2 1 falling-threshold 1 owner noc
&
rmon event 2 trap public description "Interface ARP Packets In Stopped" owner noc
rmon alarm 2 lifEntry.106.1 60 delta rising-threshold 3 falling-threshold 0 2 owner noc
rmon alarm 2 lifEntry.106.2 60 delta rising-threshold 3 falling-threshold 0 2 owner noc
```

**Note:** The SNMP interface index (ifindex) value in **bold** needs to correspond with the interface you wish to monitor. You may need several `rmon alarm` entries to manage a router with many interfaces. RMON alarms do not support wild-carding of the monitored index. If this is desired and the router is running a more recent version of IOS, then the Event-MIB solution may be better suited.

To determine the interfaces and index values on the router, poll the `ifDescr` MIB object.

If the threshold values in *italics* are too aggressive and alarm too often, change the number to reflect your environment. In general, you shouldn't be experiencing input queue drops if the system is properly queuing and flushing packets. However, there may be cases where there are some queue drops that don't reflect the condition in this PSIRT advisory. On an Ethernet segment with many PCs and servers you should get a sizable number of ARP broadcasts.

An SNMP trap notification coming from this RMON Alarm and Event configuration for input queue drops increasing would appear as:

```
YYYY-MM-DD HH:MM:SS router.cisco.com [10.0.0.1] (via 10.1.0.10) TRAP, SNMP v1, community p
RFC1271-MIB::rmon Enterprise Specific Trap (RMON-MIB::risingAlarm) Uptime: DDD day
RFC1271-MIB::alarmIndex.3 = INTEGER: 3
RFC1271-MIB::alarmVariable.3 = OID: OLD-CISCO-INTERFACES-
MIB::locIfInputQueueDrops.1
RFC1271-MIB::alarmSampleType.3 = INTEGER: deltaValue(2)
RFC1271-MIB::alarmValue.3 = INTEGER: 56
RFC1271-MIB::alarmRisingThreshold.3 = INTEGER: 2
```

**Note:** Your SNMP trap receiver application might format the message differently.

This trap indicates that we passed a rising threshold of two on the locIfInputQueueDrops.1 (index .1) interface.

An SNMP trap notification coming from this RMON Alarm and Event configuration for input ARP packets stalling would appear as:

```
YYYY-MM-DD HH:MM:SS router.cisco.com [10.0.0.1] (via 10.1.0.10) TRAP, SNMP v1, community p
RFC1271-MIB::rmon Enterprise Specific Trap (RMON-MIB::fallingAlarm) Uptime: DDD day
RFC1271-MIB::alarmIndex.2 = INTEGER: 2
RFC1271-MIB::alarmVariable.2 = OID: OLD-CISCO-INTERFACES-
MIB::locIfarpInPkts.1
RFC1271-MIB::alarmSampleType.2 = INTEGER: deltaValue(2)
RFC1271-MIB::alarmValue.2 = INTEGER: 0
RFC1271-MIB::alarmFallingThreshold.2 = INTEGER: 0
```

This trap indicates that we passed a falling threshold of 0 on the locIfarpInPkts.1 (index .1) interface. Essentially, our ARP packet counter is no longer incrementing.

**Note:** If you receive both traps on your event console, simultaneously, it correlates to a higher probability that the interface is wedged and the PSIRT advisory condition is possibly impacting your router.

## Event-MIB

### Overview

The Event MIB provides the ability for a router to self-monitor MIB objects without the need of an external network management system to perform periodic polls. The device can watch internal MIB objects and initiate simple actions whenever a trigger condition is met (for example, an SNMP trap can be generated when an object is modified or a threshold value is passed). When notifications are triggered by events, the Network Management System (NMS) does not need to constantly poll managed devices to find out if something has changed.

More information on Event-MIB can be obtained at:

- <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtevent.htm>

**Note:** This functionality is only available in recent versions of IOS.

Release	Modification
	Event MIB Support was introduced

12.1(3)T, 12.0(12)S	
12.2 (4)T	Event MIB Persistence is introduced  Event MIB is made compliant with RFC 2981
12.2 (4)T3	Support was added for the Cisco 7500 series

Customers on the initial release need to use the experimental (draft) MIB definition and will not get persistence of the MIB settings. In this situation the MIB settings need to be reset when a device is reloaded.

Customers on the 12.2(4)T and follow-on releases are able to use the RFC-compliant MIB definition and get persistence with the MIB settings across device reloads. These customers should note the follow document to ensure persistence of their settings across a device reload:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmibpr1.htm>

## Example Event-MIB Configuration

You must use SNMPset actions to the router in order to configure this feature. In the example below, the freely available net-snmp tools from <http://www.net-snmp.com> are used on a network management station to configure the feature on the router. Other tools and network management applications can perform a similar SNMPset function.

The example monitors the locIfInputQueueDrops MIB object for increases. However, the same methodology could be used to watch locIfarpInPkts. Ensure that your router configuration has an snmp-server host ###.###.### statement to direct SNMP traps to your event console.

```
#Configure the Trigger Entries
## First destroy any other rows called Wedge.1 that might exist
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerEntryStatus.5.87.101.100.103.101.49 i 6
## Create the new Trigger row entry called Wedge.1 5 is create & wait
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerEntryStatus.5.87.101.100.103.101.49 i 5
## Create a row in the table for the SNMP MIB object we want to monitor
## in this case locIfInputQueueDrops numerically .1.3.6.1.4.1.9.2.2.1.1.26
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerValueID.5.87.101.100.103.101.49 o .1.3.6.1.4.1.9.2.2.1.1.26

## Create a row in the table that says we will wildcard ie. Look at all interfaces
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerValueIDWildcard.5.87.101.100.103.101.49 i 1

## Create a row that will specify the type of test as BITS 2 or Threshold
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerTest.5.87.101.100.103.101.49 b 2

## Create a row that will specify how frequently the router will poll itself
## in this case every 60 sec (u for unsigned integer)
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerFrequency.5.87.101.100.103.101.49 u 60

## Create a row that will specify the sample type in this case integer 2 is DeltaValue
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerSampleType.5.87.101.100.103.101.49 i 2

## Create a row that will set the TriggerEnabled status to 1 (Active)
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerEnabled.5.87.101.100.103.101.49 i 1

## Create a row that will set the TriggerEntryStatus to 1 (Active) it was previously in
## a 5 (createAndWait) status
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerEntryStatus.5.87.101.100.103.101.49 i 1
```

```

# Configure the Event Entries
## First destroy any other rows called Wedge.event that might exist
snmpset -c RW-COMM-STRING DEVICEIP mteEventEntryStatus.5.87.101.100.103.101.101.118.101.11

## Create a new Event table entry called Wedge.event 5 is create & wait
snmpset -c RW-COMM-STRING DEVICEIP mteEventEntryStatus.5.87.101.100.103.101.101.118.101.11

## Create an Event action of bits 0 (Notification) or trap
snmpset -c RW-COMM-STRING DEVICEIP mteEventActions.5.87.101.100.103.101.101.118.101.110.11

## Set the Event Enabled status to integer 1 (True)
snmpset -c RW-COMM-STRING DEVICEIP mteEventEnabled.5.87.101.100.103.101.101.118.101.110.11
## Set the Event Entry Status to integer 1 (Active)
snmpset -c RW-COMM-STRING DEVICEIP mteEventEntryStatus.5.87.101.100.103.101.101.118.101.11

# Set the Delta Threshold values
# For this example the delta thresholds are 5 dropped packets rising and
# 1 dropped packets falling

## Set the Delta value for rising thresholds to 5
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerThresholdDeltaRising.5.87.101.100.103.101.49
## Set the rising Event owner to Wedge
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerThresholdDeltaRisingEventOwner.5.87.101.100.1
## Set the Threshold Rising Event to trigger the event event
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerThresholdDeltaRisingEvent.5.87.101.100.103.10
## Set the Delta value for falling thresholds to 2
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerThresholdDeltaFalling.5.87.101.100.103.101.49
## Set the falling Event owner to Wedge
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerThresholdDeltaFallingEventOwner.5.87.101.100.1
## Set the Threshold Falling Event to trigger the event event
snmpset -c RW-COMM-STRING DEVICEIP mteTriggerThresholdDeltaFallingEvent.5.87.101.100.103.1

```

Monitor with the **show management event** command or use **debug management event mib**.

Traps are sent from the router and appear on your SNMP Trap Receiver (Cisco Info Center, HP Openview, Tivoli Netview, and net-snmp snmptrapd) as defined in your router configuration snmp-server host IP statement:

```

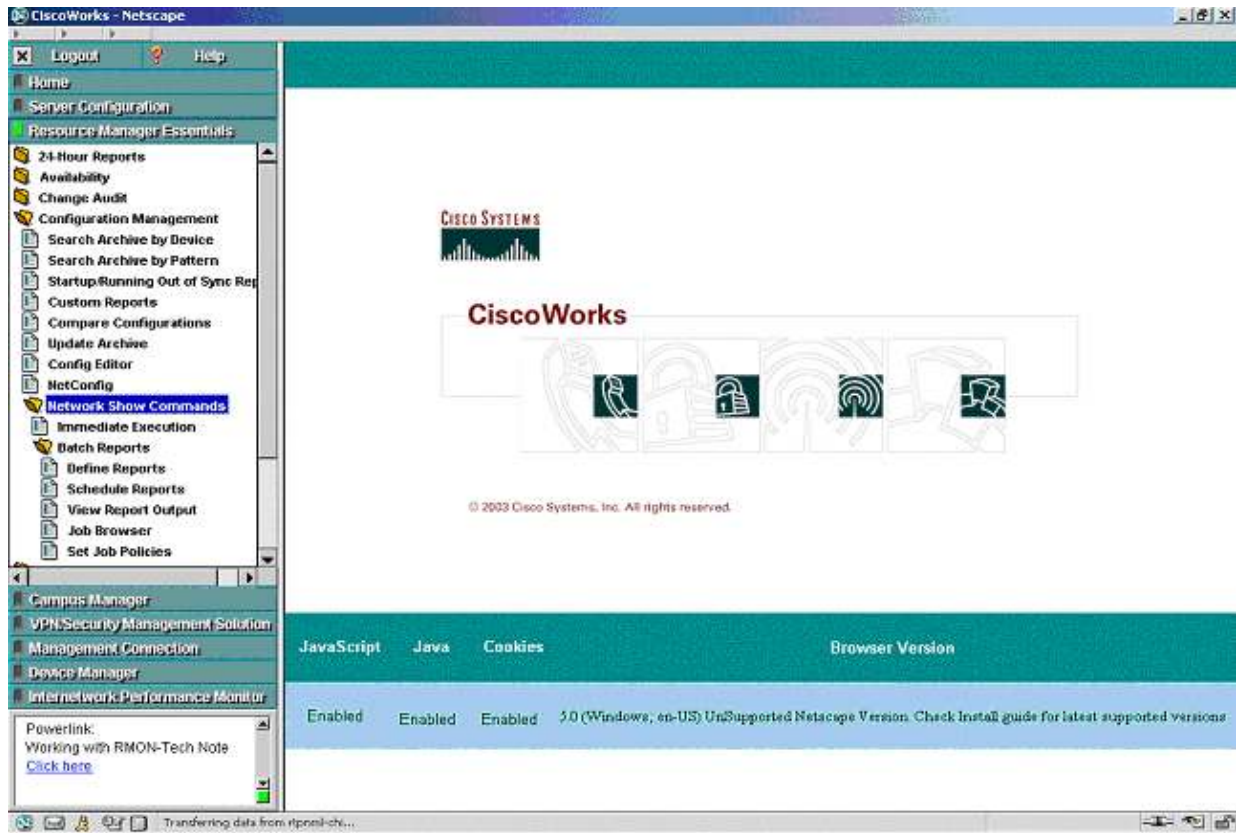
YYYY-MM-DD HH:MM:SS router.cisco.com [10.0.0.1] (via 10.1.0.10) TRAP, SNMP v1, community p
DISMAN-EVENT-MIB::dismanEventMIBNotificationPrefix Enterprise Specific Trap (DISMAN
DISMAN-EVENT-MIB::mteHotTrigger.0 = STRING: 1
DISMAN-EVENT-MIB::mteHotTargetName.0 = STRING:
DISMAN-EVENT-MIB::mteHotContextName.0 = STRING:
DISMAN-EVENT-MIB::mteHotOID.0 = OID: OLD-CISCO-INTERFACES-MIB::locIfInputQueueDrop
DISMAN-EVENT-MIB::mteHotValue.0 = INTEGER: 0

```

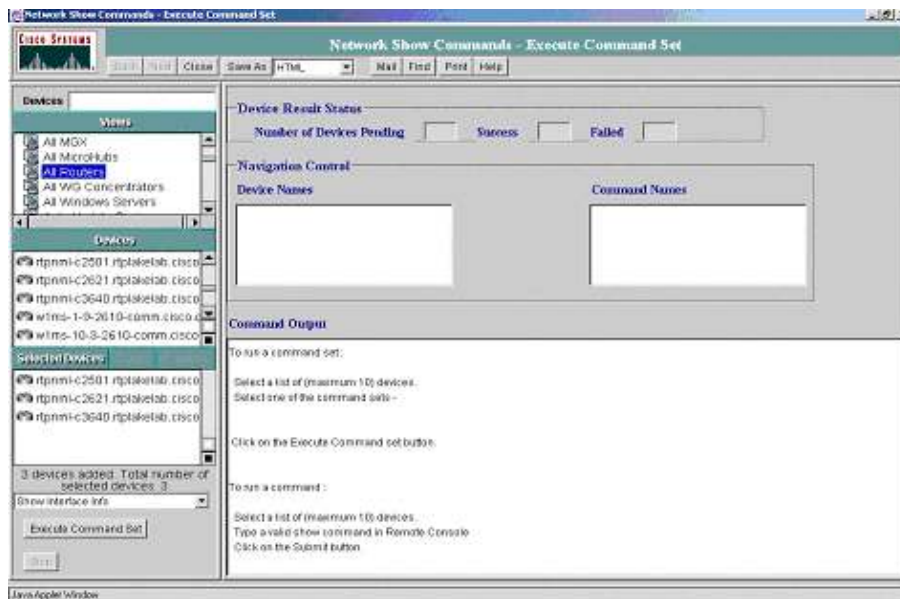
## CiscoWorks RME Network

### Using CiscoWorks RME Network Show Commands

As mentioned in the PSIRT advisory and before in this document, using the **show interface** command reveals if the interface input queue is wedged. It may be difficult or inefficient for many larger customers to constantly telnet/SSH into their routers to check the **show interface** statistics. CiscoWorks Resource Manager Essentials (RME) has a capability called Network Show Commands that may be used to issue these CLI commands to groups of devices and collect the output for analysis, scripting or emailing.



Selecting the **Immediate Execution** option allows for a group of devices to be issued a command en masse. The Batch Reports capability allows the network administrator to periodically run these reports.



The Web GUI only allows the user to run a command set on 10 devices at a time. The CLI version of network **show** commands (**cwconfig netshowbatch**), does not have this limitation and is more appropriate for programmatic monitoring.

## Scripted CiscoWorks RME Network Show Commands

A Perl script has been created that works with the CiscoWorks RME applications. It uses the device and credential information in the RME database to poll devices. You can also use the script in a programmatic fashion with cron jobs.

The script is available from your TAC or Advanced Services representative or download it from the Cisco Open Source Initiative (COSI) page at:

- <http://sourceforge.net/projects/cosi-nms> look for Queue Wedge Report script
- [http://prdownloads.sourceforge.net/cosi-nms/queue\\_wedge.pl?download](http://prdownloads.sourceforge.net/cosi-nms/queue_wedge.pl?download)

The script uses the Network Show commands CLI to automatically query all IOS devices in the network for potential input queue problems. Once you download this script, you must edit a few of the variables at the top before running it.

\$USER	SHOULD be set to a user in CiscoWorks that has access to the "Show Interface Info" Network Show command set
\$PASSWD	SHOULD be set to that user's CiscoWorks password
\$USE_SSH	CAN be set to either "yes" or "no" depending on whether or not you want Network Show Commands to try to SSH to the devices
\$IGNORE_FAILURES	CAN be set to "yes" or "no" depending on whether or not you want the script to include devices Network Show Commands could not contact in its report
\$RECIPIENTS	SHOULD be set to a comma separated list of email addresses. Each address will receive a copy of the resulting input queue report
\$FROM	(optional) You can set this to an address at your organization to which users can reply if they have questions about the report
\$MAIL_SERVER	mandatory for Windows, but can be left blank on Solaris. Set this to an SMTP server that can relay mail.
\$RUN EVERY	optional variable on Windows. If this is set to a positive value, then the script will sleep the specified number of seconds then begin execution again. A recommended value is 1800 to run every thirty minutes. This might need

to be a larger interval for very large IOS networks.
--

On Solaris, do a **chmod 755** after downloading to make the script executable.

**Note:** Root access is required to run this script.

On Windows you must run the script with the command:

```
NMSROOT\bin\perl.exe path\to\queue_wedge.pl
```

Where NMSROOT is the path where CiscoWorks is installed. On Solaris, you can simply run the script by name.

By default, the report looks for devices in the network that have at least one packet in their input queues. If it finds such a device, the device name, interface, current queue depth, and maximum queue depth is mailed to the specified recipients. If the interface is currently wedged, the text "(WEDGED)" appends the line in the report.

The script can be scheduled to run periodically on Solaris using cron.

For example, to schedule the script to run every 30 minutes, put the following in your root user's crontab:

```
0,30 * * * * /path/to/queue_wedge.pl
```

This polling frequency may be too aggressive for very large IOS networks. Adjust as needed.

---

## Related Information

- [Technical Support – Cisco Systems](#)

---

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Nov 16, 2005

Document ID: 44104

---