Troubleshooting the ATM SPAs

This chapter describes techniques that you can use to troubleshoot the operation of your ATM SPAs.

- General Troubleshooting Information, on page 1
- Performing Basic Interface Troubleshooting, on page 3
- Displaying Additional ATM SPA Data, on page 5
- Using the Cisco IOS Event Tracer to Troubleshoot Problems, on page 9
- Change in Informational Alarm, on page 10
- Preparing for Online Insertion and Removal of a SPA, on page 11

General Troubleshooting Information

This section provides the following general information for troubleshooting ATM SPA cards and their SPA interface processor (SIP) carrier cards:

Interpreting Console Error and System Messages

Refer to Cisco IOS XE System Messages document.

System error messages are organized in the documentation according to the particular system facility that produces the messages. The SIP and SPA error messages use the following facility names:

- Cisco ASR 1000 Series SIP:
  - ASR1000_SIP
  - ASR1000_SIP_SPA
- Cisco WebEx Node SPA:
  - SPA_SE1
  - SPA_WMA
- Cisco WebEx Node SPA Service Engine:
  - SPA_SRVCS_ENGINE
  - SPA_SRVCS_IF
- SPA Online Insertion and Removal—SPA_OIR

Using debug Commands

This section provides details regarding debug commands used for an ATM SPA.

General debug Commands

Along with the other debug commands supported on the Cisco ASR 1000 Series Routers, you can obtain specific debug information for SPAs on the Cisco ASR 1000 Series Routers using the **debug hw-module subslot** privileged exec command.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead can affect system use.

The **debug hw-module subslot** command is intended for use by Cisco Systems technical support personnel. For more information about the debug hw-module subslot command and about other debug commands that can be used on a Cisco ASR 1000 Series Routers, refer to the Cisco IOS Debug Command Reference for your specific software.

ATM debug Commands

The following debug commands can be useful when troubleshooting specific ATM problems on an ATM interface or subinterface:

- **debug atm errors**—Displays errors that occur on an ATM interface, such as encapsulation and framing errors, as well as any errors that might occur during configuration of the ATM interfaces.
- debug atm events—Displays information about events that occur on the ATM interfaces, such as changes to the ATM SPA and ATM interface configuration, card and interface resets, and PVC creation.

Note The output of **debug atm events** can be extremely verbose and can cause problems if large numbers of ATM VCs are configured. The command should only be used when a few VCs are configured.

- debug atm oam—Displays the contents of ATM operation and maintenance (OAM) cells as they arrive from the ATM network.

Tip Use the **no debug all** command to turn off all debugging displays.

For more information about these commands, see the Cisco IOS Debug Command Reference for your specific software release.

Using show Commands

There are several **show** commands that you can use to monitor and troubleshoot the SIP and SPA cards on Cisco ASR 1000 Series Routers. For more information on these commands, see the *Performing Basic Interface*

Troubleshooting section and *Verifying the Interface Configuration* section in *Configuring the ATM SPAs* chapter.

Performing Basic Interface Troubleshooting

You can perform most of the basic interface troubleshooting using the **show interface atm**, **show atm interface atm**, and **show ip interface** commands and examining several areas of the output to determine how the interface is operating.

The following example shows an output of the **show atm interface atm** and **show ip interface** commands.

```
Router# show atm interface atm 0/2/2

Interface ATM0/2/2:
AAL enabled: AAL5, Maximum VCs: 4095, Current VCCs: 1

Max. Datagram Size: 4528
PLIM Type: SONET - 155000Kbps, TX clocking: LINE
Cell-payload scrambling: ON
sts-stream scrambling: ON
5 input, 5 output, 0 IN fast, 0 OUT fast, 0 out drop
 Avail bw = 149760
Config. is ACTIVE
Router# show ip interface atm 0/2/2.1
ATM0/2/2.1 is up, line protocol is up
  Internet address is 2.4.0.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 4470 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is disabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Distributed switching is disabled
  IP CEF switching turbo vector
  IP Null turbo vector
  Associated unicast routing topologies:
        Topology "base", operation state is UP
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
```

```
Input features: MCI Check
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
```

To verify that your interface is operating properly, complete the following steps:

SUMMARY STEPS

1. From global configuration mode, enter the **show interface atm**, **show atm interface atm**, or **show ip interface** command.
2. Verify that the interface is up.
3. Test the ability of an interface to send and receive packets.

DETAILED STEPS

Procedure

Step 1 From global configuration mode, enter the **show interface atm**, **show atm interface atm**, or **show ip interface** command.

Example:

```
Router# show interfaces atm 0/2/2
Router# show atm interface atm 0/2/2
Router# show ip interface
0/2/2
```

Step 2 Verify that the interface is up.

Example:

```
Router# show interfaces atm 0/2/2
ATM0/2/2 is up, line protocol is up
Router# show atm interface atm 0/2/2
Interface ATM0/2/2:
AAL enabled: AAL5, Maximum VCs: 1023, Current VCCs: 1
Router# show ip interface brief
0/2/2
ATM0/2/2 unassigned YES manual up up
```

Step 3 Test the ability of an interface to send and receive packets.

Example:

```
Router# ping
```

Using the ping Command to Verify Network Connectivity

The **ping** command is a convenient way to test the ability of an interface to send and receive packets over the network.

The **ping** command sends ICMP echo request packets to a specified destination address, which should send an equal number of ICMP echo reply packets in reply. By measuring the numbering of packets that are successfully returned, as well as how long each packet takes to be returned, you can quickly obtain a rough idea of the Layer 3 to Layer 3 connectivity between two interfaces.

The IP **ping** command has the following syntax: **ping**

or **ping** *ip-address* [**repeat** *count*] [**data** *hex*] [**size** *datagram-size*]

If you enter just **ping**, the command interactively prompts you for all other parameters. Otherwise, you must specify at least a specific IP address as the destination for the ping. You can also optionally specify the following parameters:

- **repeat** *count* —Number of ICMP echo request packets to send. The default is five packets.
- **data** *hex* —The data pattern, in hexadecimal, to be sent in the ICMP echo request packets.
- **size** *datagram-size* —Specifies the size, in bytes, of the ICMP echo request packets to be sent. The range is 40 to 18024 bytes, with a default of 100 bytes.

Displaying Additional ATM SPA Data

The following sections describe additional ATM SPA data that can be displayed:

Displaying ATM SPA Hardware Information

Use the following commands to display different types of hardware and system information:

- **show version**

Displays information about the router, its system hardware and software, and the number of each type of interface that is installed.

- **show hw-module subslot fpd**

Displays information about the hardware revision of the SPA, as well as the version of the field-programmable device (FPD) that is onboard the SPA. Cisco technical engineers might need this information to debug or troubleshoot problems with a SPA installation.

- **show idprom module**

Displays the serial number and board revisions for the ATM SPA.

- **show controllers atm**

Displays information about the controller hardware for an ATM interface, including framing and alarm configuration, as well as port, packet, and channel performance statistics. The syntax is **show controllers atm** *slot* /*sublot* /*port*.

- **show diag**

Displays information about the type of port adapters that are installed in the router. The syntax is **show diag** *slot*, where *slot* is the slot number that contains the port adapter.

Displaying Information About PVCs

Use the following commands to display information about PVCs, including mapping, traffic, and VLAN configuration information:

- **show atm vp**

Displays information about the virtual paths (VPs) that are configured on the router's ATM interfaces.

- **show atm vc**

If used without any options, displays information about all of the virtual channels that are currently configured on the ATM interfaces. To display detailed information about a specific virtual connection, specify its VC descriptor (VCD) along with the command.

You can also display information about the VCs on a specific ATM interface and its subinterfaces, for example:

```
Router# show atm vc interface atm 0/2/2
```

- **show atm pvc**

Displays information about all PVCs that are currently configured on the router's ATM interfaces and subinterfaces. To display detailed information about a particular PVC, specify its VPI/VCI values. To display all PVCs on a particular ATM interface or subinterface, use the **show atm pvc interface atm** command. For example:

```
Router# show atm pvc 1/100
```

- **show atm ilmi-status**

Displays information about Layer 2 and Layer 3 mapping.

- **show atm map**

Displays the mapping between virtual circuits and Layer 3 IP addresses.

- **show atm traffic**

Displays general information about the traffic over the ATM interfaces. To display information about traffic shaping on the ATM interfaces in a particular slot, use the **show atm traffic shaping slot** command. You can also use the **show atm vc traffic** command to display traffic information for a particular VC.

Using loopback Commands

The **loopback** commands place an interface in loopback mode, which enables you to use the **ping** command to send packets through the local interface and line, so as to test connectivity. These commands are especially useful when an interface is experiencing a high number of cyclic redundancy check (CRC) errors, so that you can pinpoint where the errors are occurring.

The following describes different loopback tests:

Using the loopback diagnostic Command to Create a Local Loopback

To perform a local loopback test, in which the transmit data is looped back to the receive data at the physical (PHY) layer, use the **loopback diagnostic** command on an ATM interface. This loopback tests connectivity on the local ATM interface, verifying that the interface's framing circuitry and segmentation and reassembly

(SAR) circuitry is operating correctly. This loopback, however, does not test the interface's optics circuitry and ports.

Tip If an ATM interface is currently connected to another ATM interface and passing traffic, shut down the remote ATM interface before giving the **loopback diagnostic** command on the local ATM interface. Otherwise, the remote interface continues to send traffic to the local interface, and the remote network could also start reporting interface and network errors.

SUMMARY STEPS

1. Router# **configure terminal**
2. Router(config)# **interface atm** *slot* /*subslot/port*
3. Router(config-if)# **loopback diagnostic**
4. Router(config-if)# **atm clock internal**
5. Router(config-if)# **end**
6. Router# **show interface atm** *slot* /*subslot/port*
7. Router(config-if)# **ping** *ip-address* [**repeat** *count*] [**data** *hex*] [**size** *datagram-size*]
8. Router# **show interface atm** *slot* /*subslot/port*
9. Router(config)# **interface atm** *slot* /*subslot/port*
10. Router(config-if)# **no loopback diagnostic**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **interface atm** *slot* /*subslot/port*	Enters interface configuration mode for the indicated port on the specified ATM SPA card.
Step 3	Router(config-if)# **loopback diagnostic**	Puts the ATM interface into the local loopback mode, so that data that is transmitted out the interface is internally routed back into the receive data line.
Step 4	Router(config-if)# **atm clock internal**	Specifies that the AMT interface should derive its clocking from its local oscillator, which is required, because the loopback command isolates the interface from the network and from the clocking signals that are derived from the network line.
Step 5	Router(config-if)# **end**	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	Router# **show interface atm** *slot* /*subslot/port*	(Optional) Verifies that the interface has been configured for loopback mode. The output should show the words "loopback set" when the interface is operating in loopback mode.

	Command or Action	Purpose
Step 7	Router(config-if)# **ping** *ip-address* [**repeat** *count*] [**data** *hex*] [**size** *datagram-size*]	Sends an ICMP echo request packet to the specified IP address. • *ip-address* —Destination IP address for the ICMP echo request packet. Because the interface has been put into loopback mode, the exact IP address does not matter—any valid IP address can be specified. • **repeat** *count* —(Optional) Specifies the number of ICMP echo request packets to be sent. The default is 5. • data hex—(Optional) The data pattern, in hexadecimal, to be sent in the ICMP echo request packets. • **size** *datagram-size* —(Optional) Specifies the size, in bytes, of the ICMP echo request packets to be sent. The range is 40 to 18024 bytes, with a default of 100 bytes. **Note** Because the interface is in loopback mode, the ping command will report that it failed. This is to be expected.

Step 8	Router# **show interface atm** *slot* /*subslot/port*	Displays interface statistics, including whether any CRC or other errors occurred during the ping test. For example:
		`Router# show interface atm 5/0/1`
		`...`
		`Received 0 broadcasts, 0 runts, 0 giants, 0 throttles`
		`5 input errors, 5 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort`
		`...`
		`Router#`

Step 9	Router(config)# **interface atm** *slot* /*subslot/port*	Enters interface configuration mode for the indicated port on the specified ATM SPA card.
Step 10	Router(config-if)# **no loopback diagnostic**	Removes the local loopback and return the ATM interface to normal operations. **Note** Remember to restore the proper clocking on the local ATM interface and to reenable the remote ATM interface.

Examples

The following sample output shows a local loopback being set with the loopback diagnostic command:

```
Router# configure terminal
Router(config)# interface atm 0/2/2
Router(config-if)# loopback diagnostic
Router(config-if)# atm clock internal
Router(config-if)# end
Router# show interface atm 0/2/2
ATM0/2/2 is up, line protocol is up
  Hardware is ATM SPA, address is 000a.f330.2a80 (bia 000a.f330.2a80)
  MTU 4470 bytes, sub MTU 4470, BW 149760 Kbit, DLY 80 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback set
  Encapsulation(s): AAL5
  4095 maximum active VCs, 21 current VCCs
  VC idle disconnect time: 300 seconds
  Signalling vc = 1, vpi = 0, vci = 5
         UNI Version = 4.0, Link Side = user
  6 carrier transitions
  Last input 01:47:05, output 00:00:01, output hang never
  Last clearing of "show interface" counters 01:03:35
  Input queue: 0/75/33439/80 (size/max/drops/flushes); Total output drops: 963306
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     9502306 packets input, 6654982829 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     27827569 packets output, 21072150159 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Using the loopback line Command

If an ATM interface can perform a local loopback successfully, without reporting errors, you can next try a line loopback (**loopback line** command) to determine if packet errors are being generated by the ATM network between the local and remote router. In a line loopback, the interface on the remote router is configured with the loopback line command, so that it reflects every packet that it receives back to the originating router. The local router then generates traffic with the ping command to determine whether the line through the network is generating the packet errors.

Using the Cisco IOS Event Tracer to Troubleshoot Problems

Note This feature is intended for use as a software diagnostic tool and should be configured only under the direction of a Cisco Technical Assistance Center (TAC) representative.

The Event Tracer feature provides a binary trace facility for troubleshooting Cisco IOS software. This feature gives Cisco service representatives additional insight into the operation of the Cisco IOS software and can be useful in helping to diagnose problems in the unlikely event of an operating system malfunction or, in the case of redundant systems, route processor switchover.

Event tracing works by reading informational messages from specific Cisco IOS software subsystem components that have been preprogrammed to work with event tracing, and by logging messages from those components into system memory. Trace messages stored in memory can be displayed on the screen or saved to a file for later analysis.

The SPAs currently support the “spa” component to trace SPA OIR-related events.

For more information about using the Event Tracer feature, refer to the following URL: http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/evnttrcr.html

Change in Informational Alarm

This section discusses the change in the informational alarm output, which is displayed when alarms are displayed for POS or an ATM interface. The change in Informational alarm is implemented in Cisco IOS Release 12.2(33)XNE. The prerequisite for viewing informational alarms is to enable the logging alarm informational command as below:

```
Router(config)# logging alarm informational
```

Old Behavior

Before implementing this change, the SONET informational logs on the ATM SPA were displayed with POS appended in the alarm string as below:

```
*May 7 05:37:37.838: %ASR1000_RP_SONET_ALARM-6-POS: ASSERT CRITICAL ATM1/3/0 Section Loss
of Signal Failure
*May 7 05:37:37.838: %ASR1000_RP_SONET_ALARM-6-POS: ASSERT CRITICAL ATM1/3/0 Threshold Cross
 Alarm - B2
*May 7 05:37:37.838: %ASR1000_RP_SONET_ALARM-6-POS: ASSERT CRITICAL ATM1/3/0 Threshold Cross
 Alarm - B3
```

New Behavior

After implementing this change, from Cisco IOS Release 12.2(33)XNE, for a POS or ATM SPA, when there are alarms for an interface, the informational message will appear with a generic string “SONET” instead of containing interface specific (POS) information as below.

```
*Jun 8 08:07:28.168: %ASR1000_RP_SONET_ALARM-6-SONET: ASSERT CRITICAL ATM0/3/0 Section Loss
 of Signal Failure
*Jun 8 08:07:56.164: %ASR1000_RP_SONET_ALARM-6-SONET: ASSERT CRITICAL ATM0/3/0 Threshold
Cross Alarm - B1
*Jun 8 08:07:56.164: %ASR1000_RP_SONET_ALARM-6-SONET: ASSERT CRITICAL ATM0/3/0 Threshold
Cross Alarm - B2
*Jun 8 08:07:56.164: %ASR1000_RP_SONET_ALARM-6-SONET: ASSERT CRITICAL ATM0/3/0 Signal Degrade
 Alarm
*Jun 8 08:07:56.164: %ASR1000_RP_SONET_ALARM-6-SONET: ASSERT CRITICAL ATM0/3/0 Threshold
Cross Alarm - B3
```

Preparing for Online Insertion and Removal of a SPA

The Cisco ASR 1000 Series Aggregation Services Routers support online insertion and removal (OIR) of the SIP, in addition to each of the SPAs. Therefore, you can remove a SIP with its SPAs still intact, or you can remove a SPA independently from the SIP, leaving the SIP installed in the router.

This means that a SIP can remain installed in the router with one SPA remaining active, while you remove another SPA from one of the SIP subslots. If you are not planning to immediately replace a SPA into the SIP, then be sure to install a blank filler plate in the subslot. The SIP should always be fully installed with either functional SPAs or blank filler plates.

For more information about activating and deactivating SPAs in preparation for OIR, see the *the Troubleshooting the SIP* chapter.