Cisco Application Performance Assurance Troubleshooting Guide

August 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number:
Text Part Number: OL-14498-01

Cisco Application Performance Assurance Troubleshooting Guide

CONTENTS

About this Guide

Revised: August 15, 2007, OL-14498-01

This preface describes who should read the *Cisco Application Performance Assurance Troubleshooting Guide*, how it is organized, its document conventions, and how to obtain documentation and technical assistance.

This guide provides information about the challenges that can be faced by the Network Enhanced Module for Application Performance Assurance (NME-APA) and the methods they should use to handle those challenges. It is intended for the administrators and engineers who are responsible for daily operation of the NME-APA.

This introduction provides information about the following topics:

Document Revision History

NME-APA Release	Part Number	Publication Date
Release 1.0	OL-14180-01	August, 2007

Organization

The major sections of this guide are as follows:

Chapter	Title	Description
Chapter 1	NME-APA Troubleshooting Concepts, page 1-1	Provides background information that can help operators to troubleshoot issues when using the Cisco Network Enhanced Module for Application Performance Assurance (NME-APA) and the Cisco Application Performance Assurance Device Console (APADC).
Chapter 2	Troubleshooting Specific Scenarios, page 2-1	Lists procedures that operators can use to troubleshoot issues when using the Cisco Network Enhanced Module for Application Performance Assurance (NME-APA) and the Cisco Application Performance Assurance Device Console (APADC).

Related Publications

Your NME-APA device and the software running on it contain extensive features and functionality, which are documented in the following resources:

- For information on installing the Device Console, refer to the *Cisco Application Performance Assurance Device Console Installation Guide.*
- For information on using the Device Console, refer to the *Cisco Application Performance Assurance Device Console User Guide.*
- For initial installation and startup information, refer to the *Cisco Network Module Enhanced Application Performance Assurance User Guide.*
- Cisco CLI software, refer to the *Cisco Application Performance Assurance CLI Reference Guide*
- For international agency compliance, safety, and statutory information for wide-area network (WAN) interfaces for the NME-APA device, refer to the *Regulatory Compliance and Safety Information for Cisco Network Enhanced Module Application Performance Assurance (NME-APA).*

- For installation of the APA Device Console, refer to the Cisco Application Performance Assurance Device Console Installation Guide
- To view Cisco documentation or obtain general information about the documentation, refer to *Obtaining Documentation.*

Conventions

This document uses the following conventions:

Table 1

Convention	Description
boldface font	Commands and keywords are in **boldface.**
italic font	Arguments for which you supply values are in *italics.*
[ ]	Elements in square brackets are optional.
{x | y | z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.
`screen font`	Terminal sessions and information that the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
`italic screen` font	Arguments for which you supply values are in *`italic screen`*font.
<>	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note.* Notes contain helpful suggestions or references to materials not covered in this manual.

Means *reader be careful.* In this situation, you might do something that could result in equipment damage or loss of data.

Means *reader be warned.* In this situation, you might do something that could result in bodily injury.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package that ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/pcgi-bin/marketplace/welcome.pl

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback**in the toolbar and select **Documentation**. After you complete the form, click **Submit**to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, page xiii as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at any time, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to http://www.cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website http://www.cisco.com/tac.

P3 and P4 level problems are defined as follows:

- P3—Your network is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, page xiii, go to http://tools.cisco.com/RPF/register/register.do.

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at http://www.cisco.com/tac/caseopen.

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

CHAPTER 1

NME-APA Troubleshooting Concepts

This module includes background information that can help operators to troubleshoot issues when using the Cisco Network Enhanced Module for Application Performance Assurance (NME-APA) and the Cisco Application Performance Assurance Device Console (APADC).

Information About the User Log

The user log is an ASCII file that can be viewed in any editor. It contains a record of system events, including startup, shutdown and errors. You can use the Logger to view the user log to determine whether or not the system is functioning properly, as well as for technical support purposes.

User logs for CADC are available on the web server at *<drive:>\SCAtE\apache-tomcat-5.5.20\logs* where *<drive:>*is the hard drive where CADC is installed, for example, *C:* or *D:* .

Three different log files are available, where *YYYYMMDD* is the date of installation of the application.

- *jakarta_service_YYYYMMDD.log* —The Tomcat web server
- *stderr_ YYYYMMDD.log* —The CADC application error log
- *stdout_ YYYYMMDD.log* —The CADC application trace/informative log

Information About the Logging System

There are two discreet logging systems, NME-APA logging is maintained on the modules and CADC logging is maintained on the web server. CADC uses Java's Log4J logging system. The log files are located in the *\SCAtE\apache-tomcat-5.5.20\logs* directory.

Events are logged to one of two log files. After a file reaches maximum capacity, the events logged in that file are then temporarily archived. New events are then automatically logged to the alternate log file. When the second log file reaches maximum capacity, the system then reverts to logging events to the first log file, overwriting the temporarily archived information stored in that file.

Basic operations include:

- Copying the User Log to an external source

- Viewing the User Log
- Clearing the User Log
- Viewing and clearing the User Log counters

Copying the User Log

You can view a log file by copying both log files to to the local NME-APA platform disk or to any external host running an FTP server.

To copy the user log to an internal location, use the following command:

- From the NME-APA# prompt, type `logger get user-log file-name` *`target-filename`* and press **Enter**.

To copy the user log to an external source, use the following command:

- From the NME-APA# prompt, type `logger get user-log file-name` *`ftp://username:password@ipaddress/path`* and press **Enter**.

Viewing the User Log

To view the user log:

- From the prompt, type `more user-log` and press **Enter**.

  The user log appears.

Note This method is not recommended when the user log is large. Copy a large log to a file to view it (see Copying the User Log, page 1-2)

To view the CADC log:

1. Go to the path *\SCAtE\apache-tomcat-5.5.20\logs* .
2. Use a text editor to open the files.

Clearing the User Log

You can clear the contents of the user log at any time. The user log contains important information regarding the functioning of the system. It is recommended that a copy be made before the log is cleared.

To clear the user log:

1. From the prompt, type `clear logger device user-file-log` and press **Enter**.
2. The system asks `Are you sure?`
3. Type `Y` and press **Enter**.

To clear the CADC log:

- Delete the log files on the web server.

Viewing the User Log Counters

Note This not applicable to CADC logs.

There are two types of log counters:

- User log counters—Count the number of system events logged from the SCE platform since the last reboot
- Non-volatile counters—Are not cleared at boot time

To view the user log counters for the current session, use the following command:

- From the prompt, type `show logger device user-file-log counters` and press **Enter**.

  The logger lines information appears, followed by the prompt.

To view the non-volatile logger counters for both the User log file and the debug log file, use the following command:

- From the prompt, type `show logger nv-counters` and press **Enter**.

  The non-volatile log counter information appears, followed by the prompt.

To view the non-volatile counter for the user-file-log only, use the following command:

- From the prompt, type `show logger device user-file-log nv-counters` and press **Enter**.

  The user-file-log non-volatile log counter information appears, followed by the prompt.

Generating a File for Technical Support

In order for technical support to be most effective, the user should provide them with the information contained in the system logs. Use the `logger get support-file` command to generate a support file for the use of Cisco technical support staff.

For CADC, the log files maintained by the application (see Information About the User Log, page 1-1) should be made available to Cisco technical support staff.

To generate a log file for technical support:

- From the prompt, type `logger get support-file` *`filename`* and press **Enter**.

  The support information file is created using the specified filename, and the prompt appears. This operation may take some time.

Operational Status

The operational status can be displayed using the CLI command `show system operation-status`. The following table lists the operational states.

Table 1-1 Operational States

Operational Status	Description
Booting	Initial state after reset
Operational	The system becomes operational after completing the following process: • Boot is completed • Power self-tests are completed without failure • Platform configuration is applied
Warning	The system is fully operational (as above) but one of the following occurred: • Line ports (FE ports) to the link are down • The management port link is down • Temperature raised above threshold • Insufficient space on the disk **Note** If the condition that caused the platform to be in Warning state is resolved (for example, link is up) the platform reverts to Operational state.
Failure	The system is in Failure state after Boot due to one of the following conditions: • Power-on test failure • Three abnormal reboots in less than 20 minutes • The platform is configured to enter Failure mode subsequent to a failure-induced reboot (this is configurable using a CLI command) **Note** Depending on the cause of failure, the management interface and the platform configuration may or may not be active/available.

CADC Operational Status

The CADC application maintains three operational states of managed NME-APA:

- Offline—The device is unreachable by ICMP ping.
- Available—The device is reachable but has not been authenticated.
- Connected—The device is reachable and authenticated.

Offline

Check if the device can be pinged from the server running the CADC application.

If the device is reachable from the server, check the application logs to see why the device failed to become “Available”.

Available

If CADC fails to “Connect” to the managed NME-APA, perform the following:

1. Go to **Admin >Admin User Management**.
2. Verify that the NME-APA you are trying to connect is included under the “Configured Devices” for the CADC user trying to connect to the NME-APA.
3. Click on the device name under “Configured Devices” for the CADC user.
4. Verify that the device username on CADC also exists on the NME-APA through Telnet.
5. Verify that the passwords for the device user on CADC and NME-APA are identical.
6. Check the application logs for any error messages.

Connected

Only one managed device can be in this stateat any one time.

Check the application logs if the user is unable to "Disconnect" from NME-APA. If the problem persists, restart the Tomcat Windows service and the SCAtE MySQL Windows service. If this does not solve the problem, restart the server.

Signature, Protocol, and Service IDs

For protocol classification troubleshooting, the first thing is to make sure that appropriate signature, protocol, and service ID values are correct in the RDR report. The following table contains the values for the new protocols introduced in the Excelsior project for reference.

Table 1-2 Signature, Service, and Protocol IDs

Protocol / Traffic Type	Signature ID (defined by Excelsior)	Protocol ID (defined by CADC)	Service ID (defined by CADC)
PROTOCOL_TYPE_ORACLE	0x20010000	4000	400
PROTOCOL_TYPE_CITRIX	0x20020000	4001	401
PROTOCOL_TYPE_CITRIX_ICA	0x20020100	4001	401
PROTOCOL_TYPE_CITRIX_CGP	0x20020200	4001	401

Table 1-2 Signature, Service, and Protocol IDs (continued)

Protocol / Traffic Type	Signature ID (defined by Excelsior)	Protocol ID (defined by CADC)	Service ID (defined by CADC)
PROTOCOL_TYPE_CITRIX_IMA	0x20020300	4001	401
PROTOCOL_TYPE_CITRIX_SBM	0x20020400	4001	401
PROTOCOL_TYPE_SAP	0x20030000	4002	402
PROTOCOL_TYPE_AIM	0x20040000	714	28
PROTOCOL_TYPE_AIM_TEXT	0x20040100	714	28
PROTOCOL_TYPE_AIM_VOICE	0x20040200	714	28
PROTOCOL_TYPE_AIM_VIDEO	0x20040300	714	28
PROTOCOL_TYPE_AIM_MEDIA_CHAT	0x20040400	714	28
PROTOCOL_TYPE_AIM_FILEXFER	0x20040500	714	28
PROTOCOL_TYPE_AIM_PICSHARE	0x20040600	714	28
PROTOCOL_TYPE_AIM_GAME	0x20040700	714	28
PROTOCOL_TYPE_MS_EXCHANGE	0x20050000	4004	4
PROTOCOL_TYPE_GOOGLE_TALK	0x20060000	1030	28
PROTOCOL_TYPE_GOOGLE_TALK_VOICE	0x20060100	1030	28
PROTOCOL_TYPE_GOOGLE_TALK_FILEXFER	0x20060200	1030	28
PROTOCOL_TYPE_VOICE_YAHOO	0x050B0000	45	37

Table 1-2 Signature, Service, and Protocol IDs (continued)

Protocol / Traffic Type	Signature ID (defined by Excelsior)	Protocol ID (defined by CADC)	Service ID (defined by CADC)
PROTOCOL_TYPE_CHAT_YAHOO_MESSENGER	0x0B020000	40	28
PROTOCOL_TYPE_MSSQL	0x20070000	4006	403
PROTOCOL_TYPE_ACTIVEX	0x20080000	4007	404
PROTOCOL_TYPE_MSN_MESSENGER	0x20090000	883	28
PROTOCOL_TYPE_MSN_MESSENGER_TEXT	0x20090100	883	28
PROTOCOL_TYPE_MSN_MESSENGER_VOICE	0x20090200	883	28
PROTOCOL_TYPE_MSN_MESSENGER_VIDEO	0x20090300	883	28
PROTOCOL_TYPE_MSN_MESSENGER_EMAIL	0x20090400	883	28
PROTOCOL_TYPE_MSN_MESSENGER_FILEXFER	0x20090500	883	28
PROTOCOL_TYPE_MSN_MESSENGER_GAME	0x20090600	883	28
PROTOCOL_TYPE_MSN_MESSENGER_WHITEBOARD	0x20090700	883	28

Debug Flags for Protocol Libraries

The following flags can be used to collect debug traces for a specific protocol library.

Note Debug flags can be used only if a special SML debug image is loaded into the NME-APA. The release image is not compatible with debug flags.

The CLI command to apply the debug flag is under config ->Interface Linecard 0:

`Tunnable PL_PT_ShowDebugReportForModule[Flag Value] value TRUE`

The protocol library debug flag values are listed in the following table.

Table 1-3 Debug Flags for Protocol Libraries

Debug Flag	Value
public const uint16 PL_ALL_MODULES	0
public const uint16 PL_UNIFICATION	1
public const uint16 PL_COMMON	2
public const uint16 PL_VOICE_SKYPE	3
public const uint16 PL_MAIL_SMTP	4
public const uint16 PL_BEHAVIORAL	5
public const uint16 PL_YAHOO	6
public const uint16 PL_VOICE_RTP	7
public const uint16 PL_VOICE_DINGOTEL	8
public const uint16 PL_P2P	9
public const uint16 PL_VOICE_SIP	10
public const uint16 PL_RTSP	11
public const uint16 PL_FTP	12
public const uint16 PL_HTTP	13
public const uint16 PL_MMS	14
public const uint16 PL_TFTP	15
public const uint16 PL_MAIL_IMAP	16
public const uint16 PL_MAIL_MIME	17
public const uint16 PL_NNTP	18
public const uint16 PL_MAIL_POP3	19
public const uint16 PL_SSL	20
public const uint16 PL_DHCP	21
public const uint16 PL_RADIUS	22
public const uint16 PL_H323	23
public const uint16 PL_MGCP	24
public const uint16 PL_PTT	25
public const uint16 PL_RTCP	26
public const uint16 PL_SDP	27
public const uint16 PL_SKINNY	28
public const uint16 PL_SMPP	29
public const uint16 PL_WAP	30
public const uint16 PL_DNS	31
public const uint16 PL_SSDP	32

Table 1-3 Debug Flags for Protocol Libraries (continued)

Debug Flag	Value
public const uint16 PL_AGG_AGING	33
public const uint16 PL_BASIC	34
public const uint16 PL_HITLESS_UPGRADE	35
public const uint16 PL_CUWORLD	36
public const uint16 PL_ICQ	37
public const uint16 PL_JABBER	38
public const uint16 PL_STUN	39

Note PL_HITLESS_UPGRADE (35) will be used for the new features added in hitless upgrade.

Debug Flags for SML Components

The following flags can be used to collect debug traces for a software component in the Excelsior SML application.

Note Debug flags can be used only if a special SML debug image is loaded into the NME-APA. The release image is not compatible with debug flags.

The CLI command to apply the debug flag is under config ->Interface Linecard 0:

`Tunnable APP_PT_ShowDebugReportForModule[`*`Flag Value`*`] value TRUE`

The SML component debug flag values are listed in the following table.

Table 1-4 Debug Flags for SML Components

Debug Flag	Value
public const uint16 APP_ALL_MODULES	0
public const uint16 APP_MAIN	1
public const uint16 APP_UNIFICATION	2
public const uint16 APP_CLASSIFY	3
public const uint16 APP_EXTERN_CALLBACKS	4
public const uint16 APP_LISTNERS	5
public const uint16 APP_PARTY	6
public const uint16 APP_HANDLERS	7
public const uint16 APP_REPORTS	8
public const uint16 APP_MAX_MODULE	9

CHAPTER 2

Troubleshooting Specific Scenarios

This module includes procedures that operators can use to troubleshoot issues when using the Cisco Network Enhanced Module for Application Performance Assurance (NME-APA) and the Cisco Application Performance Assurance Device Console (APADC).

Accessing the NME-APA module

You can access the NME-APA module:

- by telnet
- through the ISR router
- through a web-based application (APADC)

  APADC is the preferred method of access.

How to Access the NME-APA Module via Telnet

You can access the NME-APA module by Telnet.

Step 1 Configure the IP address from the ISR router.

Step 2 Telnet to the NME-APA module, to get the CLI login prompt.

Step 3 Execute the CLI commands based on the level (5, 10, or 15) being enabled.

The CLI debug commands can only be executed under level 15 (ROOT level).

How to Access the NME-APA Module via the ISR Router

You can access the NME-APA module through the ISR router.

Step 1 Run the ISR session command, `service-module integrated-Service-Engine <slot/0>session`. (The term `shellConn` is used for referring to the NME-APA console.)

All the engineering commands are used for debugging purpose. They should be used with care so that they do not interfere with live traffic.

How to Access the NME-APA Module via APADC

You can access the NME-APA module by APADC.

Step 1 Click on the APADC icon on the desktop of the server.

For the first-time login, use username: root, password: cisco.

APADC Login Fails

First time login fails

First time login (username: root, password: cisco) fails.

Step 1 Verify that MySQL is correctly installed.

Verify that the *C:\ mysql-enterprise-5.0.44-win32* folder exists.

Step 2 Verfiy that the MySQL Windows service is running.

Check under Windows services that SCAtE-MySQL is running.

Step 3 Query the MySQL dbase.

- username: scate
- password: scate
- dbase: scate
- table: scate_user

Step 4 Validate the table.

Verify that a row exists in this table with:

- username=root

- password=Cisco

Problem Persists

If the problem persists, completely uninstall and reinstall APADC.

Subsequent login fails

Step 1 Verify that MySQL is correctly installed.

Verify that the *C:\ mysql-enterprise-5.0.44-win32* folder exists.

Step 2 Verfiy that the MySQL Windows service is running.

Check under Windows services that SCAtE-MySQL is running.

Step 3 Query the MySQL dbase.

- username: scate
- password: scate
- dbase: scate
- table: scate_user

Step 4 Validate the table.

Verify that a row exists in this table with username and password.

Step 5 Try a different scate user login.

Step 6 Go to Admin; delete and add the user that failed to login.

Problem Persists

If the problem persists, completely uninstall and reinstall APADC.

Warning **This will delete all of the saved data on the application.**

ISR/NME-APA Platform Troubleshooting

The NME-APA does not come up

Step 1 Verify that the NME-APA has a service-module IP address and default gateway configured on the ISR.

The NME-APA does not power up

Step 1 Verify that the NME-APA is firmly seated in the ISR slot and that the retaining screws are tightened.

Step 2 Make sure the slot being used can support the NME-APA card.

Step 3 Verify that you are not attempting to use an NME-APA-E3 card in an ISR 2800 or an NME-APA-E2 card in an ISR 3800.

During installation of the NME-APA image, the NME-APA card does not come up

Step 1 Check the IOS version on the ISR using the **show version** command.

Step 2 Make sure that the IOS version supports the NME-APA card.

Step 3 If the IOS version does not support the NME-APA card, update the ISR IOS image to a version that supports the NME-APA card.

Cannot ping the NME-APA management interface from the ISR Router

Step 1 Verify that there is a valid route to and from the NME-APA. (This might require a static route to the NME-APA on the ISR if the Integrated Service Engine interface is set to ip unnumbered.)

Cannot Telnet to NME-APA management interface from other station

Step 1 Verify that there is a valid route to and from the NME-APA.

Step 2 Use the NME-APA ShellConn command **i** to see whether the telnetServer process is up and running.

Step 3 If the telnetServer process is not running, leave the card in its current state for DEs to debug.

During installation of the NME-APA image, an error is received

During installation of the NME-APA image, the following error is received:

```
Pycurl.error: invalid return value for write callback
Error: Operation Aborted.
```

Step 1 The package name has the wrong extension. Change the extension to .pkg.

The NME-APA does not see any diverted traffic

Step 1 From the ISR IOS CLI run `show running-config interface integrated-Service-Engine <slot/0>`. If `!SCE traffic-management Disabled` appears in the output, the NME-APA card is currently not enabled. Wait a few minutes and then try again. Also, verify that you have the correct card for this ISR model.

Step 2 Make sure that traffic diversion is enabled on the designated interface. You should see that the configuration, service-module apa traffic-management monitor, is set to that interface.

Step 3 Make sure that traffic is arriving from the designated interface. (Use the ISR IOS CLI `show interfaces <fastEthernet or GigabitEthernet><slot><port>counters`. The counters should increase when you pump the traffic. If there is no increase, the traffic is not getting to the ISR chassis.)

Step 4 Use the NME-APA CLI `show interface fastEthernet 0/1 counters` to see whether traffic has been diverted to NME-APA from ISR. The output will indicate whether the packets are diverted to NME-APA or are discarded by NME-APA.

APADC Application Troubleshooting

Connect Screen Troubleshooting

Cannot connect to “Available” device

Step 1 Go to **Admin >Admin User Management**.

Step 2 Verify that the logged-in scate user appears in the “User” column.

Step 3 Verify that the NME-APA trying to connect is a “configured device” for the scate user.

Step 4 Click on the device name in the “configured device” column.

Step 5 Verify that the device user name is correctly configured and is the same as the username configured on the NME-APA (by Telnet).

Step 6 If the problem persists, create a new user account on the device and use this account to connect to the device by configuring it under **Admin >Admin User Management**.

Step 7 Click **Help**, to review integrated help for more details.

Step 8 If the problem persists, report to Cisco Systems, Inc.

Cannot disconnect a “Connected” device

Step 1 Select the device and delete it.

Step 2 Reset the device.

Step 3 Click **Help**, to review integrated help for more details.

Step 4 If the problem persists, report to Cisco Systems, Inc.

Cannot add a device

Step 1 Verify that there are no more than five devices already added to the APADC application.

Step 2 If more than five devices are already added to the APADC application, delete an existing device to add a new device.

Step 3 Verify the correct network address for the device to be added.

Step 4 Click **Help**, to review integrated help for more details.

Step 5 If the problem persists, report to Cisco Systems, Inc.

Device stays “Offline”

Step 1 Ping the device from the web server running APADC.

Step 2 Restart the Tomcat Windows service from **Windows Administrative Tools > Services**.

Step 3 Restart the application server.

Step 4 Click **Help**, to review integrated help for more details.

Step 5 If the problem persists, report to Cisco Systems, Inc.

Device Configuration Screens Troubleshooting

Cannot access Device Configuration Screen

Step 1 Verify that at least one device is in the "Connected" state.

Step 2 Verify that the user role allows access to this screen. Refer to the SFS for details.

Device Configuration is erased

Step 1 Click **Save**before toggling to a different tab after making configuration changes.

Step 2 Click **Apply** to commit configuration data to NME-APA.

Step 3 Any configuration on a tab is lost if it is not saved before user moves to a different tab.

Step 4 Click **Help**, to review integrated help for more details.

Step 5 If the problem persists, report to Cisco Systems, Inc.

Apply fails

Step 1 Verify that the "Connected " device is still available and alive.

Step 2 Click **Help**, to review integrated help for more details.

Step 3 If the problem persists, report to Cisco Systems, Inc.

Retrieve fails

Step 1 Verify that the "Connected" device is still available and alive.

Step 2 Click **Help**, to review integrated help for more details.

Step 3 If the problem persists, report to Cisco Systems, Inc.

Fault Management Screen Troubleshooting

Notification is not received

Step 1 Verify that the Notification is not suppressed:

a. Go to the Fault Configuration screen.

b. Look for the Notification ID for the missing notification.

c. Verify that the Notification ID is present in the table.

d. Check to see that the “Suppressed” column has the value “No”, rather than “Yes”.

Step 2 Click “Refresh” .

Step 3 Verify that NME-APA is sending a Notification.

Step 4 Click **Help**, to review integrated help for more details.

Step 5 If the problem persists, report to Cisco Systems, Inc.

Statistics Screen Troubleshooting

Statistics Screen Problems

Step 1 All Statistics are accumulated via SNMP queries. See SNMP Troubleshooting on APADC, page 2-16.

Installation Screen Troubleshooting

Install process fails with the error ‘Cannot connect to device’

Step 1 Ensure the Web user has credentials on the device as a level-15 user. (If the device user corresponding to the Web user has a level 0/5/10 credentials, the install process will fail.)

Install process fails with the error "Image file type and file mismatch"

The image file type selected for install (pqi or pqb) must have a filename extension of *.pqi* or *.pqb* . The files are not transferred from the user PC to the scate server if a filename mismatch occurs. (Further semantic checks are performed in the next stage of the process to verify that the image files are of the expected type.)

Step 1 Verify that the installation file has the correct filename extension.

Traffic Management Screen Troubleshooting

Cannot apply TM configuration to device

Step 1 Check the server log for a connection-related exception.

```
2007-07-25 11:09:11,929  INFO [http-8080-Processor20] com.pcube.apps.engage.Engage -
Sending configuration to SCE ...
connection to SCE failed: server refused connection: unable to open connections - max
number of sessions exceeded
com.pcube.apps.engage.ConnectionFailedException: server refused connection: unable to open
connections - max number of sessions exceeded
    at com.pcube.apps.engage.Connection.login(Connection.java:414)
    at com.pcube.apps.engage.Engage.login(Engage.java:138)
    at com.cisco.scabb.servconf.mgmt.SCABB.login(SCABB.java:81)
    at
com.cisco.scate.web.mgt.tm.ServiceConfigManager.applyServiceConfig(ServiceConfigManager.ja
va:115)
    at
com.cisco.scate.web.ui.tm.service.ClassTreeAction.showClassTree(ClassTreeAction.java:159)
```

If there is such a connection-related exception and reapplying the TM config to the device still fails, the connection between the SCAtE server and the device is maxed out.

Step 2 Restart the SCAtE server (Tomcat).

Reporting Screen Troubleshooting

- Report fails to generate output (PROCESS_ERROR), page 2-12

RDR retrieval ("RetrieveNow") fails

Step 1 Verify that the "Connected " device is still available and alive.

Step 2 Verify that it is possible to FTP to the NME-APA from the APADC server using the device username and password associated with the APADC user from the Admin screen.

If this step fails, refer to Device Configuration Screens Troubleshooting, page 2-7 and verify users configured on the device. Retrieval will fail if an FTP attempt is made with a username and password that do not exist on the NME-APA device.

Step 3 Verify that enough hard-disk space is available on the APADC server.

Can not "Activate" scheduled task

Step 1 Verify that the task has not expired.

if the start time is in the past, make sure that the difference between current time and the task start time is greater than the task recurrences times task interval.

Step 2 Verify that the NME-AP device is still available and alive.

Step 3 Verify that it is possible to FTP to the NME-APA from the APADC server using the username "admin" and enable15 password.

If this step fails, refer to Device Configuration Screens Troubleshooting, page 2-7, and reconfigure the enable15 password on the device.

Step 4 Verify that enough hard-disk space is available on the APADC server.

Cannot "Add" a scheduled task

Step 1 Verify that at least one NME-AP device is added to APADC.

Step 2 Only one scheduled task can be added at a time. If there is a task, delete the task and try again.

RDR Retrieval continues to be in "In Progress" state

Step 1 Verify that the NME-AP device is still available and alive.

Step 2 Verify that it is possible to FTP to the NME-APA from the APADC server using the username "admin" and enable15 password.

Step 3 Verify that enough hard-disk space available on the SCAtE server

If this step fails, refer to Device Configuration Screens Troubleshooting, page 2-7, and reconfigure the enable15 password on the device.

Step 4 Check the server logs for OutOfMemory Errors.

Restart the Tomcat server in the case of such errors.

No "Last Retrieval" information is displayed

Step 1 Verify that the *<SCATE_ROOT_DIR>/scate-config/rdrloader.xml* file exists and is not empty.

Step 2 Try "RetrieveNow" to see if the information gets updated.

If the information is notupdated, there could be problems retrieving data from the NME-APA. See RDR retrieval ("RetrieveNow") fails, page 2-10.

Step 3 If there is a "Scheduled Task", make sure that it is still active.

Report fails to generate output (PROCESS_ERROR)

Step 1 Verify that report parameters do not contain invalid characters.

Step 2 Open a command prompt, `cd` to the SCA Reporter folder and run the report command.

The report command line can be found in the scate log. It should be as follows:

```
reportercmd -o
../apache-tomcat-5.5.20/webapps/ROOT/report_results/Global_Bandwidth_per_IM_type[1]--NME-A
PA--2007-Aug-01-13-23-58 -format jpeg -template "Global Bandwidth per IM type" -params
"numhours=24;im_message_type=MSN TEXT;seip=10.6.1.19;starttime=;link=Link 1,Link
0;avgdata=false;units=Kbit/s;endtime=;trafficdir=Both Directions;" -dbuser scate
-dbpassword scate -dburl "jdbc:mysql://localhost:3306/scateinfra" -dbdriver
"com.mysql.jdbc.Driver" -policysce 10.6.1.19
```

Step 3 Remove all optional parameters and try again.

Cannot create report instance

Step 1 Traffic management configuration *must* be applied by APADC. Verify that the NME-APA TM was configured using the APADC. Verify that the *scateinfra.INI_VALUES* table in MySQL is not empty.

Step 2 Verify that the "Last Retrieval" information (Device IP and time) on the Data Retrieval page is not "Unknown".

Step 3 Verify that there is RDR data in the DB. If the DB is empty, go to the RDR Retrieval page and perform "RetrieveNow".

"Run report JPEG" is disabled for certain reports

Step 1 This behavior is by design. A few report types do not support the JPEG format and so "Run Report JPEG" is disabled. CSV reports can be generated for these report types.

Report results are empty

Step 1 Traffic management configuration *must* be applied by APADC. Verify that NME-APA TM was configured using the APADC. Verify that the *scateinfra.INI_VALUES* table is not empty in the MySQL database.

Step 2 Verify that the "Last Retrieval" was done within the last 24 hours.

Step 3 Verify that there is RDR data in the DB.

Step 4 Verify that the APADC server time zone is set correctly.

Report fails to generate output (PROCESS_ERROR)

Step 1 Verify that the report parameters do not contain invalid characters.

Step 2 Open a command prompt, `cd` to the SCA Reporter folder and run the report execution command. The report execution command line can be found in the scate log.

Step 3 If the previous step successfully generates a report result, remove all optional parameters and try again.

User Management Screen Troubleshooting

Users not matched between Scate and Device after apply

Step 1 Check the server log for errors after applying. Since the UM creates users by importing the whole list from Scate, there might be a conflict with the existing users.

Error stating FTP not available when retrieving or applying

Step 1 Try again. A new FTP connection to the device will be created to continue the operation.

Admin Screen Troubleshooting

The Admin Screen is used to:

- Add/Edit/Delete new APADC users
- Add/Edit/Delete new devices to APADC users
- Program device username, password, and access-level to APADC users

Cannot Add a new APADC user

Step 1 Verify that the maximum number of APADC users (100) has not been reached.

Traffic Classification Troubleshooting

No RDRs after pushing the traffic

Step 1 Make sure that traffic is diverted to NME-APA and not discarded by NME-APA.

See The NME-APA does not see any diverted traffic, page 2-5.

Step 2 Make sure that the packets are not filtered (bypassed or dropped) by NME-APA.

Use the NME-APA CLI `debug slot 0 ppc 0 func RC_Cls` to keep track of the counters. If the numbers for `drop` or `bypass` increase after the traffic is sent, packets have been filtered.

The `filtered traffic` from SCAtE is used to configure the flow filter. For example, DNS packets are bypassed by default, so no RDRs will be generated by DNS traffic.

You can also use the CLI command, `debug slot 0 ppc 0 show-counters`.

Step 3 Ensure that the line card is not shut down.

Step 4 Make sure that the SML application is installed.

Use the NME-APA CLI `show version` to see whether the information about SML application is displayed.

Step 5 If the SML application is not installed, install the PQI file from the SCAtE.

Step 6 Make sure that traffic is delivered to SML Application.

Check the value of `Traversed PDUs` from the output of the NME-APA ShellConncommand, `debug slot 0 ppc 0 func sr`. If the value is 0, the SML application is not receiving traffic and no RDRs will be generated. In this case, it is possible that the traffic is not classified as a flow in SCOS. Turn on the debugging flag for the HwSim module.

1. Before you push traffic, enter the shellConn command, `LC_CS_on`
2. After the traffic is pushed, enter the ShellConn command, `LC_CS_off`

Note This command should be used in a controlled environment; it may interfere with live traffic.

The log is in the file `/root/tffs0/cs.txt`. Send this file to DEs for analysis.

Step 7 Save the RDRs.

The RDRs can either be saved to a file (default) or sent to an external entity such as the CM or rdrHandler. If the destination IP address of the RDR-Formatter is configured, the RDRs are sent to the external entity. Otherwise, they are saved to a file. See RDR File Troubleshooting, page 2-15 for details.

Some RDRs are not received

Step 1 If the traffic has been processed by SML application, make sure that the corresponding RDRs are enabled in the service configuration.

Check the RDR Settings in the SCAtE, make any necessary corrections, and apply the service configuration again. Use the NME-APA CLI `show running-config-application` to see whether the service configuration is applied.

Note It may take some some time for the RDRs to be generated for certain traffic. For example, some RDRs for the UDP flows are generated at the close of the flow, which may take several minutes after the last packet of the traffic is sent.

Step 2 Check that the correct CAP file is being used.

If necessary, replace the cap file.

Step 3 Check the setup for traffic generate tools such as kiwi.

Make sure that kiwi is set up correctly.

Step 4 Load a debug SML image to capture traces for the Protocol Library.

Contact the DE team to see if you need to load an SML debug image and to find out which debug flags need to be turned on for this particular protocol or application.

RDRs are received with incorrect values for some parameters

Step 1 Check that the traffic contains the expected packets.

Capture the packets and then examine them.

Step 2 Compare the signature, protocol, and service ID values of the RDRs with the values in the table.

Stop as many applications in the network as possible, in order to debug and see if any application generates conflicting traffic that causes the error. Record traffic and check the CAP files.

Step 3 Load a debug SML image to capture traces for the Protocol Library.

Contact the DE team to see if you need to load an SML debug image and to find out which debug flags need to be turned on for this particular protocol or application.

Step 4 Load an SML debug image and turn on debug flags.

If necessary, contact the DE team.

Step 5 Look through the traces on the NME-APA to find the cause of the errors.

RDR File Troubleshooting

No RDRs are received by the external entity

Step 1 Make sure that the configuration of the RDR-Formatter is correct (for instance, the IP address and the port number).

Use the NME-APA CLI `show RDR-Formatter` to see whether the connection between the NME-APA and the external entity is up. If the connection is down, the RDRs are queued. Check the connection between NME-APA and the external entity. (Note that this is for debugging purposes only. The RDRs should be written to files in the normal case.)

The same command will also show the number of RDRs being queued. If no RDRs are queued, refer to Traffic Classification Troubleshooting, page 2-13 to see why no RDRs are generated.

No RDR files are generated

Step 1 Check if an IP address is configured for the RDR-Formatter.

If no IP address is configured, the RDRs are queued in the buffers and will never be written to a file even if the connection is up.

Step 2 Confirm that RDRs are being generated.

Use the NME-APA CLI `show RDR-Formatter` to see whether the RDRs are queued. If no RDRs are queued, refer to Traffic Classification Troubleshooting, page 2-13 to see why no RDRs are generated.

Step 3 Use the ShellConn command, **rdrShowSts**, to see how much longer it has to wait before the RDRs are written to a file.

By default, these RDRs are written to a file every 30 minutes.

Step 4 After this time has elapsed, use the ShellConn command **rdrShowAllFiles** to see whether the file has been created.

The ShellConn command, **rdrHelp**, provides a list of commands for debugging RDRs.

The RDR files are not retrieved

Step 1 Make sure that the ftp server is enabled.

Use the NME-APA CLI `show ip ftp-server` to see whether the server is enabled.

SNMP Troubleshooting

Cannot get MIB values

Step 1 Make sure that SNMP Agent is enabled.

Use the NME-APA CLI `show snmp` to see whether SNMP Agent is enabled. If not, use the CLI `snmp enable` under configuration mode to enable it.

Step 2 Check that the console displays `SNMP Server started`.

If not, enter the ShellConn command `debugScripts 1` from the console, and then disable and enable SNMP Agent again.

Step 3 Capture the communication between Agent and AgentX.

Enter the ShellConn command `SNMP_Agentx_logging 0`. The logs are stored in the file `/root/tffs0/system/p3hidden/net-snmp/agentxDebug.log`. Send this file to DEs for analysis.

Step 4 The ShellConn commands **SNMP_AGENTX_Help** and **SNMP_AGENT_Help** provide a list of commands for SNMP debugging.

SNMP Troubleshooting on APADC

SNMP agent is running but no MIB values are displayed on the Device Statistics pages

Step 1 Use command line utilities like snmpget, snmpwalk, or a third party MIB browser to connect to the NME-APA and verify if you are able to view the MIB-II system group.

Step 2 If you are not able to see the system group values, this indicates that the SNMP agent is not functioning properly.

Step 3 If you are able to view the MIB-II system group as well as some tables such as user counters and package counters, the most likely problem is incorrect community strings.

Step 4 If you are able to view MIB-II system group and snmp counters but not NME-APA counters such as user counters, package, and rdr counters, the problem lies with the subagent implementing the enterprise specific objects. Contact Cisco systems technical support with the relevant information.