Monitoring, Troubleshooting and Recommendations

Monitoring, Troubleshooting and Recommendations

Monitoring and troubleshooting the SGSN are not unrelated tasks that use many of the same procedures. This chapter provides information and instructions for using the system command line interface (CLI), primarily the **show** command, to monitor service status and performance and to troubleshoot operations.

The **show** commands used for monitoring and troubleshooting include keywords (parameters) that can fine-tune the output to produce information on all aspects of the system, ranging from current software configuration through call activity and status. The keywords, used in the procedures documented in this chapter, are intended to provide the most useful and in-depth information for monitoring the system. To learn about all of the keywords possible, refer to the *Command Line Interface Reference*. To learn about the details for the information in the **show** command outputs, refer to the *Statistics and Counters Reference*.

In addition to the CLI documented in this chapter, the system supports other monitoring and troubleshooting tools:

- SNMP (Simple Network Management Protocol) traps that indicate status and alarm conditions. Refer to the *SNMP MIB Reference* for a detailed listing of these traps.
- bulk statistics (performance data) which can be accessed in various manners. For a complete list of SGSN supported statistics, refer to the *Statistics and Counters Reference*. For information about configuring the formats for static collection, refer to the *Command Line Interface Reference*.
- threshold crossing alerts for conditions that are typically temporary, such as high CPU or port utilization, but can indicate potentially severe conditions. For information on threshold crossing alert configuration, refer to the *Thresholding Configuration Guide*.

The monitoring and troubleshooting procedures are organized on a task-basis with details for:

- Monitoring (information required regularly)
  - Daily Standard Health Check
  - Monthly System Maintenance

    - Semi-Annual Check
- Troubleshooting (information required intermittently)
    - Overview of Possible Fault Types
    - Single and Mass Problem Scenarios
    - Reference Materials (information required infrequently)

Monitoring

This section contains commands used to monitor system performance and the status of tasks, managers, applications, and various other software components. Most of the procedure commands are useful for both maintenance and diagnostics.

There is no limit to the frequency that any of the individual commands or procedures can be implemented, however, the organization of tasks into three unique sets of procedures suggests a recommendation for minimal implementation:

- Daily Standard Health Check
- Monthly System Maintenance
- Semi-Annual Check

Daily - Standard Health Check

The standard health check is divided into three independent procedures:

- Health Check - Hardware & Physical Layer
- Health Check - System & Performance
- Health Check - SGSN-Specific Status & Performance

Health Check - Hardware & Physical Layer

The first set of commands are useful for monitoring the hardware status for the entire system. The second set of commands check the status of hardware elements within the chassis and provide some verification of the physical layer status. The operational parameters for the hardware are included in the *Hardware Installation and Administration Guide*. Note that all hardware elements generate alarms in the case of failure.

Table 1: Hardware Status Checks

To Do This:	Enter This Command:
All hardware problems generate alarms, the following checks can be replaced by reviewing the trap history.	**show snmp trap history**
Check the status of the PFUs. Output indicates the power level for the cards in the chassis. All active cards should be in an "ON" state.	**show power chassis**
Check the power status of an individual chassis.	**show power all**
View the status of the fan trays. In case of a fan problem, refer to your support contract to contact the appropriate service or sales representative.	**show fans**

To Do This:	Enter This Command:
View the LED status for all installed cards. All LEDs for active cards should be green.	**show leds all**
Checking the temperatures confirms that all cards and fan trays are operating within safe ranges to ensure hardware efficiency.	**show temperature**

Table 2: Physical Layer Status Check

To Do This:	Enter This Command:
View mapping of the line cards-to-controlling application cards.	**show card mappings**
View a listing of all installed application cards in a chassis. Determine if all required cards are in active or standby state and not offline. Displays include slot numbers, card type, operational state, and attach information.	**show card table** **show card table all**
Display a listing of installed line cards with card type, state, and attach information. Run this command to ensure that all required cards are in Active/Standby state. No card should be in OFFLINE state.	**show linecard table**
View the number and status of physical ports on each line card. Output indicates Link and Operation state for all interfaces -- UP or down.	**show port table all**
Verify CPU usage and memory.	**show cpu table** **show cpu information**

Health Check - System & Performance

Most of these commands are useful for both maintenance and diagnotics, and if the system supports a "combo" (a co-located SGSN and GGSN), then these commands can be used for either service.

Table 3: System & Performance Checks

To Do This:	Enter This Command:
Check a summary of CPU state and load, memory and CPU usage.	**show cpu table**
Check availability of resources for sessions.	**show resources session**
Review session statistics, such as connects, rejects, hand-offs, collected in 15-minute intervals.	**show session counters historical**
View duration, statistics, and state for active call sessions.	**show session duration** **show session progress**

To Do This:	Enter This Command:
Display statistics for the Session Manager.	**show session subsystem facility sessmgr all**
Check the amount of time that the system has been operational since the last downtime (maintenance or other). This confirms that the system has not rebooted recently.	**show system uptime**
Verify the status of the configured NTP servers. Node time should match the correct peer time with minimum jitter.	**show ntp status**
Check the current time of a chassis to compare network-wide times for synchronisation or logging purposes. Ensure network accounting and/or event records appear to have consistent timestamps.	**show clock universal**
View both active and inactive system event logs.	**show logs**
Check SNMP trap information. The trap history displays up to 400 time-stamped trap records that are stored in a buffer. Through the output, you can observe any outstanding alarms on the node and contact the relevant team for troubleshooting or proceed with SGSN troubleshooting guidelines.	**show snmp trap history**
Check the crash log. Use this command to determine if any software tasks have restarted on the system.	**show crash list**
Check current alarms to verify system status.	**show alarm outstanding all** **show alarm all**
View system alarm statistics to gain an overall picture of the system's alarm history.	**show alarm statistics**

Daily - Health Check- SGSN-Specific Status and Performance

These commands are useful for both maintenance and diagnotics.

Table 4: SGSN-Specific Status and Performance Checks

To Do This:	Enter This Command:
Check the status and configuration for the Iu-PS services. In the display, ensure the "state" is "STARTED" for the Iu interface.	**show iups-service all**
Check the configuration for theMAP services features and some of the HLR and EIR configuration. In the display, ensure the "state" is "STARTED" for the Gr interface.	**show map-service all**
Check the configuration for the SGSN services in the current context. In the display, ensure the "state" is "STARTED" for the SGSN.	**show sgsn-service all**

To Do This:	Enter This Command:
Check the SS7 Signalling Connection Control Part (SCCP) network configuration and status information, for example, check the state of the SIGTRAN. The display should show all links to all RNC/subsystem are available, as well as those toward the HLR.	**show sccp-network all status all**
Check the configuration and IDs for SS7 routing domains	**show ss7-routing-domain all**
Check the connection status on SS7 routes.	**show ss7-routing-domain <> routes**
Snapshot subscriber activity and summary of PDP context statistics.	**show subscribers sgsn-only**
Check the configured services and features for a specific subscriber.	**show subscribers sgsn-only full msid** *<msid_number>*

Monthly System Maintenance

Depending upon system usage and performance, you may want to perform these tasks more often than once-per-month.

Table 5: Irregular System Maintenance

To Do This:	Enter This Command:
Check for unused or unneeded file on the CompactFlash.	**dir /flash**
Delete unused or unneeded files to conserve space using the delete command. Recommend you perform next action in list	**delete /flash/***<filename>*
Synchronise the contents of the CompactFlash on both SMCs to ensure consistency between the two.	**card smc synchronize filesystem**
Generate crash list (and other "show" command information) and save the output as a tar file.	show support details <to location and filename> • [file:]{ /flash | /pcmcia1 | /hd }[/directory]/file_name • tftp://{ host[:port] }[/directory]/file_name • [ftp: | sftp:]//[username[:password]] { host }[:port][/directory]/file_name

If there is an issue with space, it is possible to remove alarm and crash information from the system - however, it is not recommended. Support and Engineering personnel use these records for troubleshooting if a problem should develop. We recommend that you request assigned Support personnel to remove these files so that they can store the information for possible future use.

Every 6 Months

We recommend that you replace the particulate air filter installed directly above the lower fan tray in the chassis. Refer to the *Replacing the Chassis' Air Filter* section of the *Hardware Installation and Administration Guide* for information and instruction to performing this task.

Table 6: Verify the Hardware Inventory

To Do This:	Enter This Command:
View a listing of all cards installed in the chassis with hardware revision, part, serial, assembly, and fabrication numbers.	**show hardware card** **show hardware inventory** **show hardware system**
View all cards installed in the chassis with hardware revision, and the firmware version of the on-board Field Programmable Gate Array (FPGAs).	**show hardware version board**

Troubleshooting

Troubleshooting is tricky unless you are very familiar with the system and the configuration of the system and the various network components. The issue is divided into three groups intended to assist you with diagnosing problems and determining courses of action.

Problems and Issues

Table 7: Possible Problems

Problem	Analysis
Users cannot Attach to the SGSN - Attach Failure	Typically, the root cause is either a fundamental configuration error or a connection problem either on the system (the SGSN) or the network. Configuration changes may have been made incorrectly on either the SGSN or on the signalling network or access network equipment.
Users can Attach to the SGSN but cannot Activate a PDP Context.	In most cases, this type of problem is related either to an issue with the LAN connectivity between the SGSN and the DNS server or a general connectivity problem between the SGSN and a GGSN.
Users can Attach to the SGSN, they can Activate a PDP Context but data transfer isn't happening.	The problem could be between the GGSN and an external server. The PDP Context indicates that the tunnel between the SGSN and the GGSN is intact, but the lack of data transfer suggests that external servers can not be reached.

Problem	Analysis
Users can Attach to the SGSN, they can Activate a PDP Context but they encounter other problems.	Problems, such as slow data transfer or a session disconnect for an already established session, can be caused by congestion during high traffic periods, external network problems, or handover problems.

Troubleshooting More Serious Problems

You will see that the commands from the Daily Health Check section are also used for troubleshooting to diagnose problems and possibly discover solutions. And of course, your Support Team is always available to help.

Causes for Attach Reject

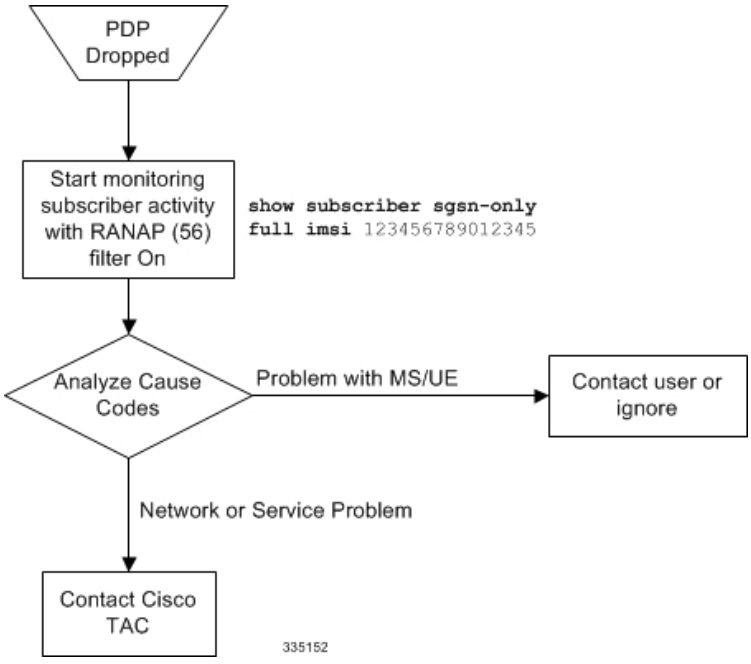
If an SGSN receives Attach Request messages but responds with Attach Rejects, then the reason might be found in one of the cause codes. These codes are included as attributes in the Reject messages and can be seen during monitoring with the following command:

```
monitor subscriber IMSI
```

Single Attach and Single Activate Failures

To troubleshoot an Attach or Activate problem for a single subscriber, you will need to begin with the subscriber's MS-ISDN number. The attached flow chart suggests commands that should assist with determining the root of the problem:

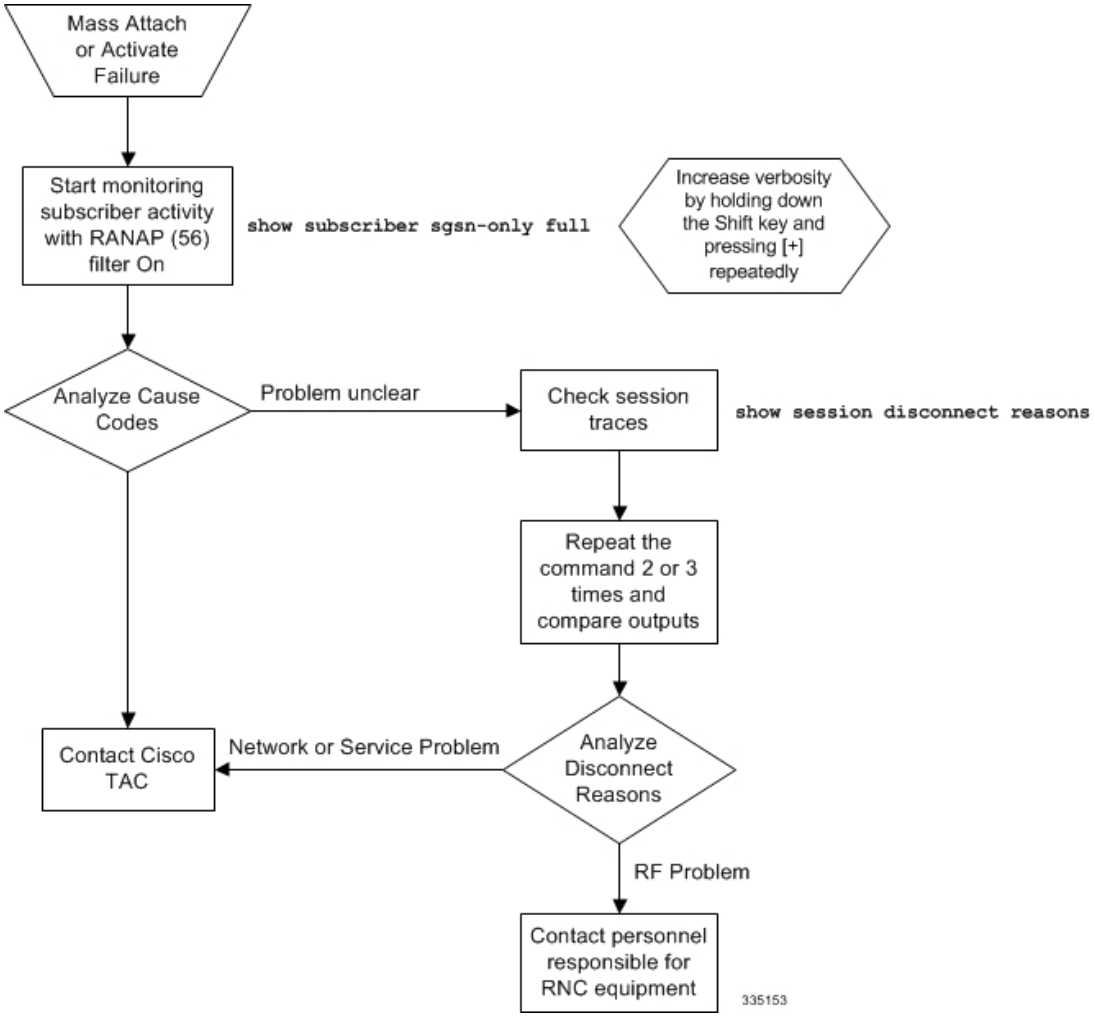
Figure 1: Troubleshooting Single Attach/Activate Failures



Mass Attach and Activate Problems

The following flow chart is intended to help you diagnose the problem and determine an appropriate response:

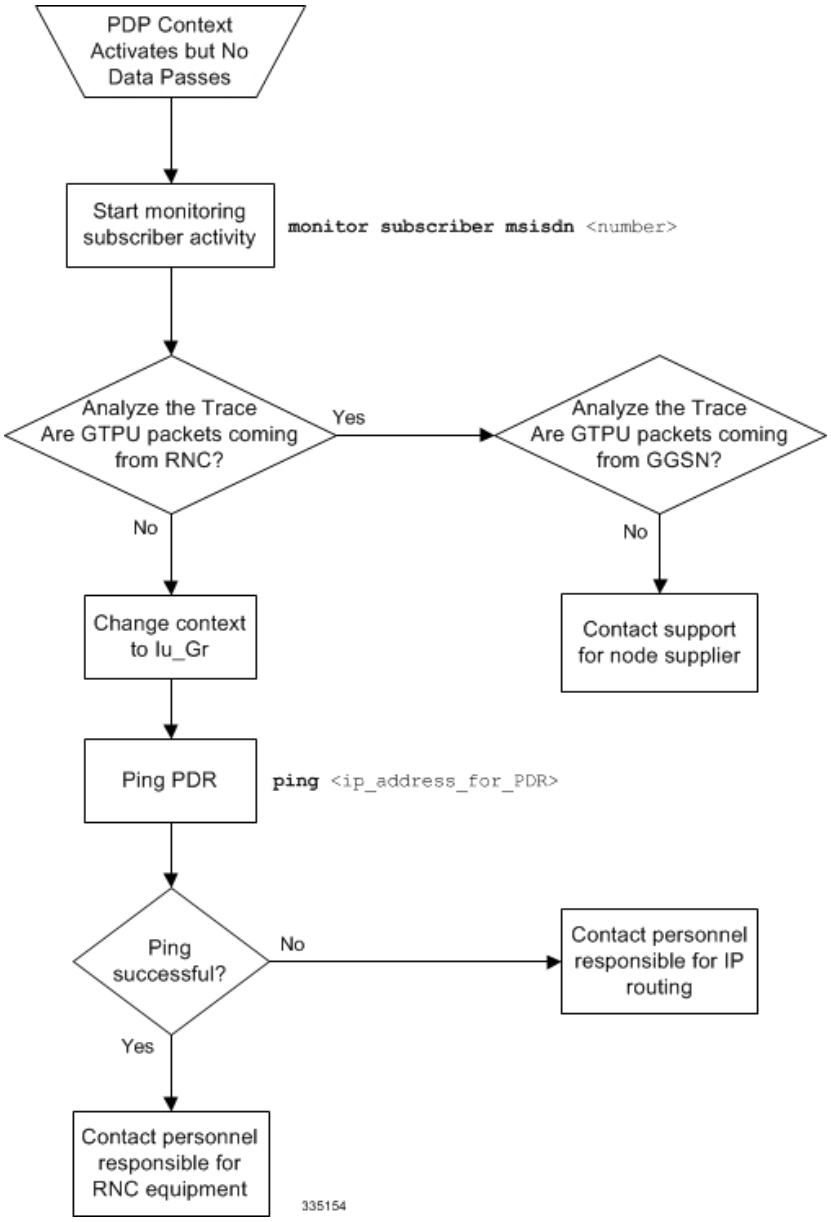
Figure 2: Troubleshooting Multiple Attach/Activate Failures



Single PDP Context Activation without Data

In a situation where the subscriber has PDP Context Activation but data is going through, the following procedure will facilitate problem analysis. To begin, you must first obtain the subscriber's MS-ISDN number.

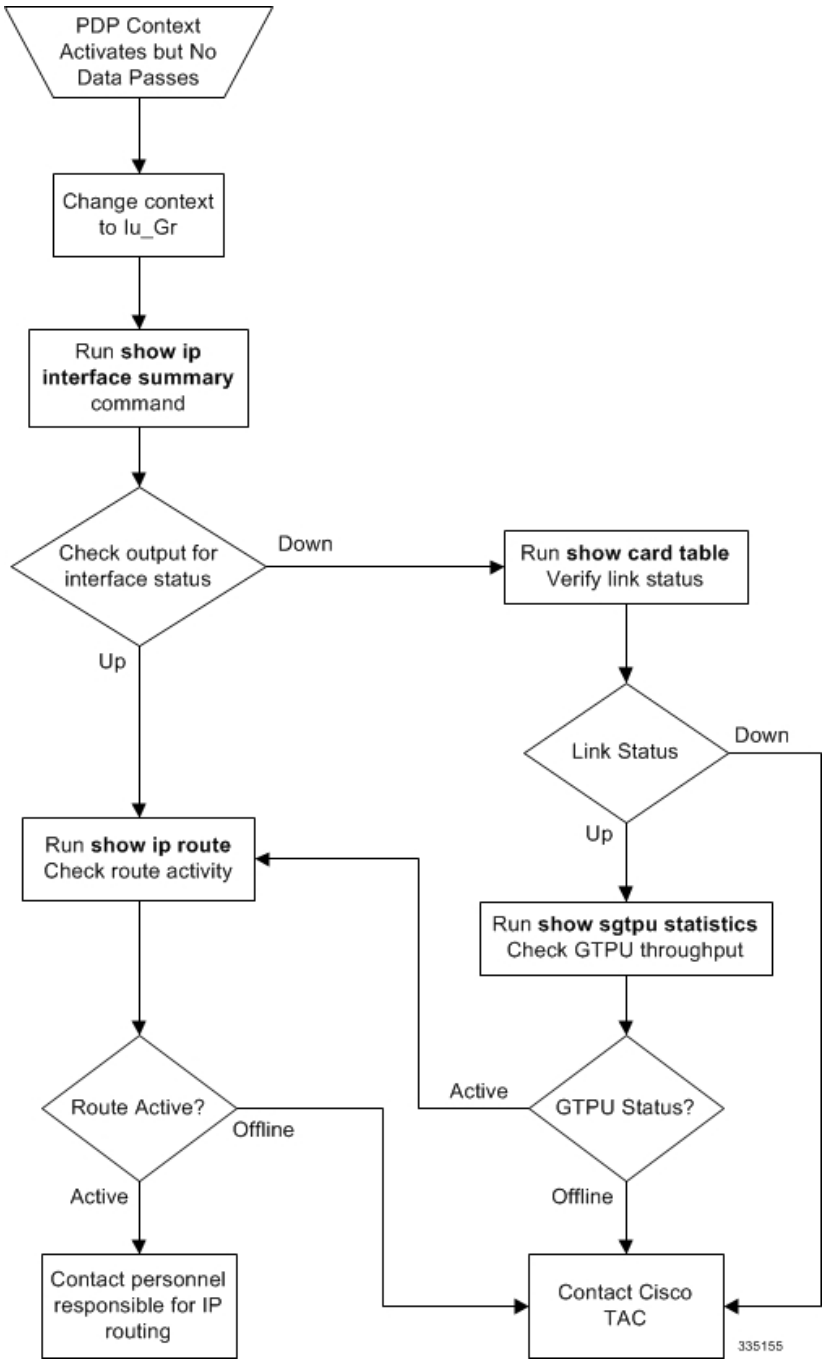
Figure 3: Troubleshooting Missing Data for Single PDP Context Activation



Mass PDP Context Activation but No Data

In many cases, this type of problem is due to a change in the configuration: hardware, interface, routing. The following will suggest commands to help run down the problem:

Figure 4: Troubleshooting Missing Data for Multiple PDP Context Activation



Recommendations

This section describes some recommendations and guidelines to ensure proper functioning of the system. Generic platform and system rules or limits can be found in the "Engineering Rules" appendix in the *System Administration Guide* and/or contact your Cisco account representative.

- The **task facility linkmgr** command is used to configure the maximum number of Link Managers for an SGSN. It is recommended to restrict the number of Link Managers for PSC2/PSC3 to a maximum of "4" due memory and hardware limitations. If the Link Managers are overloaded, then the number of Link Managers can be increased based on the number of cards available and associated ASP links needs to be updated. For more information on this command see *Command Line Interface Reference* document.

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