



System Monitoring

This chapter describes how to use the command line interface (CLI) **show** commands to monitor system status and performance. These commands allow an operator to obtain information on all aspects of the system, from current software configuration to call activity and status.

The selection of commands described in this chapter provides useful and in-depth information for monitoring the hardware. For additional information on these and other **show** command keywords, refer to the CLI on-line Help and the *Command Line Interface Reference*.

This chapter includes the following sections:

- [Monitoring, page 1](#)
- [Counters and Bulkstats, page 5](#)
- [Summary of Maintenance Tasks, page 5](#)

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.



Important

All of the commands listed below can be run from the Exec mode prompt of the Command Line Interface (CLI).

Daily - Standard Health Check

The standard health check is divided into independent procedures:

- Hardware Status
- Physical Layer Status
- System Status and Performance

Table 1: Health Checks

To do this:	Enter this command:
Hardware	
All hardware problems generate alarms that generate SNMP traps. Review the trap history.	show snmp trap history
Check the status of the PFUs, the command 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.	show fans
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
Physical Layer	
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 info
System Status and Performance	
Check a summary of CPU state and load, memory and CPU usage.	show cpu table
Check NPU utilization within the chassis.	show npu table
Check availability of resources for sessions.	show resources utilization table

To do this:	Enter this command:
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
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
If enabled, view statistics associated with Inter-Chassis Session Recovery (ICSR).	show srp info show srp monitor all show srp checkpoint statistics

Periodic Status Checks

Depending upon system usage and performance, you may want to perform these tasks more frequently than recommended.

Table 2: Periodic Status Checks

To do this:	Enter this command:
Monthly	
Check for unused or unneeded file on the CompactFlash.	dir /flash
Delete unused or unneeded files to conserve space using the delete command. You should also perform the next action in list. See Note below.	delete /flash/<filename>
Synchronize the contents of the CompactFlash on both SMCs to ensure consistency between the two (Exec mode command).	filesystem synchronize all
Generate a crash list (and other show command information) and save the output as a tar file.	show support details <to location and filename>
	Flash: [file:] { /flash /pcmcia1 /hd } [/directory] /file_name
	TFTP: tftp:// { host [:port#] } [/directory] /file_name
	SFTP: [ftp: sftp:] // [username [:password] @] { host } [:port#] [/directory] /file_name NOTE: In release 20.0 and higher Trusted StarOS builds, FTP is not supported.
NOTE: If there is an issue with space, you can remove alarm and crash information from the system; however, this practice is not recommended. Support and engineering personnel use these records for troubleshooting if a problem should develop. You should request assigned support personnel to remove these files after storing the information for possible future use.	
Every 6 Months	
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
You should replace the particulate air filter installed directly above the lower fan tray in the chassis. Refer to the <i>Replacing the Chassis Air Filter</i> section of this guide for detailed instructions.	

Counters and Bulkstats

The ASR 5000 maintains many counters for gathering statistics and troubleshooting. In general you should not regularly clear the counters, just let them increment over time. Counters track events since the chassis booted (unless cleared), unlike **show** commands that give the current state (for example, the current number of calls). See the on-line help for a list of choices. A partial list of counters to choose from are:

- **show port datalink counters**
- **show port npu counters**
- **show radius counters all**
- **show l2tp full statistics**
- **show session disconnect reasons**
- **show session counters historical all** (This is an excellent command to see the call volume history for past three days.)

You may clear the counters via CLI **clear** commands.

A bulk statistics feature allows you to push a very large array of statistical data to a remote server. Bulkstats provide detailed information about the chassis' condition, particularly over extended periods of time.

See *Configuring Bulk Statistics* section in the *System Administration Guide* for more information.

Summary of Maintenance Tasks

This section contains a quick reference for when to perform various maintenance operations on the ASR 5000 chassis. These operations include, but are not limited to:

- Load on the chassis
- The number of operators regularly accessing it
- The placement of the chassis within your network
- Available staff to perform maintenance tasks
- Support level agreements within your organization
- The specifics of your chassis configuration
- Your organization's experience with the types of issues, such as subscriber or network, that you encounter over time

Constant Attention

- Watch SNMP traps for alarms/thresholds and take appropriate action. The traps inform you of serious problems that can occur on the system, including those that do not involve the ASR 5000.
- If you have an Element Management System (EMS) server that relies on bulkstats and other data, pay attention to alarms and call load.

Daily

- Analyze system logs for any unusual entries.
- Look at call volume and throughput for consistency and expected patterns.

Weekly

- Check the system clock if NTP is not enabled.

Monthly

- Clear the /flash filesystem of files that are not needed.

6 Months

- Change the air filter.

No Specific Time Frame

- If you make a config change that you want to be permanent, synchronize filesystems between SMCs and save the configuration to /flash.
- For an expired password, re-enable the operator as soon as possible.
- If the boot system priority is approaching a low value, reset it to a higher priority.
- When you finish troubleshooting with runtime logging, remove the logging commands from the config.
- Maintain your SNMP trap server.
- Maintain your syslog server.