

Statistics, Accounting, and Diagnostics

This chapter describes the ERX system's statistics, accounting, and diagnostics features.

| Topic | Page |
|----------------------------|------|
| Statistics and Accounting | 5-1 |
| Monitoring and Diagnostics | 5-2 |
| Product Upgrades | 5-7 |

Statistics and Accounting

A critical necessity for service providers is the ability to measure traffic in the network. This information is used for a variety of purposes, including subscriber billing, traffic planning, and network load assessment. The most scalable place to measure subscriber traffic is at the edge of the network.

The ERX system is capable of gathering statistics for each interface, for each policy, and for each service class without affecting system performance. This is possible because each of the system's line modules has sophisticated hardware support for statistics. Specific intervals for the collection of statistics can be set. Once gathered, the statistics can be offloaded to a service provider OSS or relational database for further processing.

The ERX system provides bulk statistics collection and file transfer to support the download of statistics on a scheduled interval. This method gives service providers an option to retrieve statistical information beyond SNMP polling.

The ERX system gathers statistics at three levels: layer 2, network interface, and traffic. Statistics gathered include:

Per layer 2 interface

- Bytes/cells/frames – ingress and egress
- Bytes/cells/frames discarded – ingress and egress
- Ingress errored cells/frames
- Packet discard reason counters – ingress and egress

Per network interface

- Bytes/packets – ingress and egress
- Ingress bytes/packets forwarded (total across all egresses)
- Ingress errored packets
- Bytes/packets discarded – ingress and egress

Per flow

- Ingress packets marked in/out
- Ingress bytes/packets per DS class after stamping step (DS can be any QoS class)
- Ingress bytes/packets per DS class forwarded (total across all egresses)
- Ingress/egress bytes per DS class discarded (total across all egresses)

Monitoring and Diagnostics

The ERX system supports a number of monitoring and diagnostic functions to help operators and Juniper Networks Customer Service troubleshoot the system. Some of these functions are described in the following sections.

Module Identifier

Each line module and I/O module has its own EEPROM to store and make key information on the module accessible to management. The information is coded onto the module during the in-circuit test phase of the manufacturing process. This identifier allows the service provider to accurately identify and track the ERX systems and modules after they are installed.

Information for identifying the module includes:

- ID to identify the board type

- Storage of the module's MAC address(es), if required by the board
- Serial number that indicates manufacture date
- Part number and revision level
- Return and repair counts

Event Logging

The ERX system provides comprehensive information that can be stored in event logs. This information enables service providers to troubleshoot system-level and interface-level problems. A number of features are supported, including filtering capabilities and destination options.

Information stored in event logs can be filtered in different ways to help isolate the cause of the problem. Filter options include:

- Severity level – emergency, alert, critical, error, warning, notice, information, and debug
- Instance – instances vary by event category
- Verbosity level – high, medium, low

Event logs can be directed to up to four destinations and the severity level can be designated per destination. For example, you could specify that all severity *emergency* events be sent to the syslog. Event log destinations include:

- NVS on the SRP
- Console serial port on the SRP
- Syslog daemon
- Buffer on the SRP, which can be viewed with the CLI

Diagnostic Support

The ERX system implements a comprehensive suite of diagnostic tests to help operators identify and troubleshoot product problems. You can access the diagnostic tests through a local or modem connection to the DB-9 management port on the SRP I/O module.

When a test is run, it returns results that indicate if it was successful. Unsuccessful test results include information that indicate the condition expected and the actual condition that caused the failure.

The following features are supported:

- Context-sensitive help menus and prompts

- Power-on self-test (POST) that runs on chassis power-up and module hot insertion
- Standby diagnostics that run while a system is operational: active and standby (run on redundant boards). Tests do not disrupt network traffic.
- Event logs that record hardware failures associated with a board as well as other significant events, such as a reset and a log that contains entries for system failures such as fan failures. Logs are stored in NVS and are timestamped by the system clock.

Protocol Diagnostics

Diagnostic tests can be run to isolate network or system anomalies for each line module and each protocol. The ERX system supports a verbose mode to capture the PPP frames of any single link, including a timestamp that enables a user to troubleshoot the PPP link if LCP and/or IPCP cannot successfully establish a connection. A trace function and event log allow retrieval of this information for use beyond the local console. The system also supports Frame Relay and ATM diagnostic tools such as LMI and OAM F5 to isolate problems with these protocols.

Loopback Tests

The system supports a number of loopback tests for the CT3 module. See Table 5-1.

Table 5-1 Loopback tests for a CT3 module

| Loopback Mode | Description |
|---------------------------|--|
| DS3/DS1 Internal Loopback | The transmit DS3 or DS1 stream is looped back to the receiver before the DS3/DS1 framer, blocking any external incoming traffic. The test is run using a copy of the transmit data stream. |
| DS3/DS1 Line Loopback | The receive DS3 or DS1 data stream is looped back to the transmitter before the DS1 framer, blocking any internal transmit traffic. |
| DS3/DS1 Payload Loopback | The receive DS3 or DS1 data stream is looped back to the transmitter after the DS3/DS1 framer. |
| Per DS1/DS0 Loopback | Similar to payload loopback, any DS1/DS0 receive stream can be individually looped back to the transmitter. This test allows loopback down to the individual DS0. |

Test Patterns

To help service providers troubleshoot line problems, the system provides powerful test pattern generation and bit error rate test (BERT) capabilities. All of the standard test patterns ($2^{23}+1$, $2^{15}+1$, QRSS, 511, etc.) are supported. Pseudorandom patterns and user-programmable patterns are also supported. The patterns can be generated and tested over any DS0 or group of DS0s. Both $n \times 56K$ and $n \times 64K$ are supported.

Dump Capability

To help identify system problems, the system supports a crash dump capability that allows the operational software to save the stack trace, the reason for failure, and the CPU registers. Information can be gathered from both the line modules and the SRP module. The crash dump information is stored in NVS on the SRP module and can be copied from the system to a designated host.

show Commands

A number of **show** commands are available to examine information about the system. The following list is a sampling:

- **show aaa** – displays information on accounting intervals, mapping between user domains and virtual routers, IP address of DNS and WINS name servers, and the name of the virtual router for which duplicate accounting records are saved
- **show atm** – displays information and statistics about ATM interfaces
- **show boot** – displays configuration, system, image, and diagnostic images used at startup
- **show bulkstats** – displays information statistics, traps, and counters
- **show clns** – displays information about Connectionless Network Service (CLNS) interfaces, neighbors, routing processes, and traffic
- **show config** – lists all commands required to duplicate the existing operational configuration
- **show controllers** – displays information about T1, T3, E1, E3, CT1, and CE1 controller interfaces
- **show dhcp relay** – displays IP address of the configured DHCP server
- **show environment** – displays the temperature and voltage information
- **show frame-relay** – displays information and statistics about Frame Relay interfaces

- **show hosts** – lists all configured hosts
- **show interfaces** – displays current state of the FastEthernet or serial interfaces
- **show interfaces pos** – displays packet over SONET information
- **show ip** – displays information about IP configurations, including templates, traffic, routing tables, routes, statistics, route distribution policy, and access lists
- **show ip multicast routing** – displays information about the status of multicast routing
- **show l2tp** – displays information about the L2TP configuration on the system
- **show last-reset** – displays the reason for reloading specified by the user and detailed information in the event of system failure
- **show log** – displays the system log and log configuration settings
- **show mpls** – displays status and configuration information about MPLS
- **show pppoe subinterface** – displays PPP over Ethernet subinterface information
- **show radius** – displays information about the RADIUS authentication and accounting servers
- **show reload** – shows the reload status
- **show route-map** – displays the route maps
- **show secrets** – displays system passwords and secrets
- **show snmp** – displays information on the state of communication between the SNMP agent and the SNMP manager, communities, and traps
- **show subscribers** – displays authenticated PPP users
- **show terminal** – displays information about the terminal configuration of the current terminal line
- **show version** – displays the operational status, the software version, and the armed release version for each module
- **show virtual-router** – displays the virtual routers configured

Product Upgrades

The system is designed for ease of maintenance, including upgrades to hardware and software. The system supports dynamic configuration changes to the system software and hardware modules without disrupting other system operations.

For example, all firmware can be upgraded in the background during normal service delivery; then individual software objects, such as routing protocols and line interface modules, can be restarted to reduce service disruption. The system can save previous files and images for each of these objects and revert to those images if problems are discovered in the new software. The older image can be enabled in two ways:

- If the system is rebooting with an abnormal rate (as defined by the configuration), the system automatically reverts to the previous system image.
- If the system successfully boots, the administrator can still manually choose to revert to the previous image at any time.

All startup, boot, diagnostic, and operational software can be remotely upgraded through out-of-band management ports and in-band IP interfaces to further ease upgrade operations.

System Startup

The ERX system receives the operational software image from the SRP module. This image is then downloaded to each line module as appropriate. The SRP module can receive the operational image from the NVS card or through a network download.

Configuration Storage

The ERX system supports system configuration storage in an NVS software component located on the SRP module. A configuration image is downloaded to each line module. This functionality supports the following features:

- Configuration information storage between powercycles
- Fast system startup achieved by storage data in a compact binary form
- Configuration synchronization among redundant modules, regardless of the current state of the standby module(s)

