

4

Element and Network Management

This chapter explains the Juniper Networks element and network management features for ERX edge routers.

Topic	Page
Network Management Overview	4-1
Managing the ERX System	4-2
SNMP Features	4-4
Command Line Interface	4-9
Collecting Bulk Statistics	4-13
Security Features	4-13
Juniper Networks Management Products Overview	4-14

Network Management Overview

Management of the edge network is a key and critical function for a profitable, competitive network. The ERX system offers service providers both element-specific and network-wide management control.

Element-specific control allows a service provider to manage a single ERX system. Network-wide control allows the service provider to manage a set of ERX edge routers and other edge elements to create and apply global policies.

At its foundation, the ERX system supports standard-based methods of management access, including SNMP and CLI. All management functional areas are supported, including configuration, fault handling, monitoring, and statistics gathering. Multiple types of management access are supported to ensure that service providers can integrate the system into their operations support system (OSS) environments. Value-added

management services, such as customer network management, are also supported. The strength of the system's management capabilities makes it easy to configure, deploy, and maintain new IP edge services.

Managing the ERX System

There are a number of ways to manage ERX systems so that service providers can control the element in the best manner for their operational environment. Figure 4-1 shows a number of applications and access methods for the system.

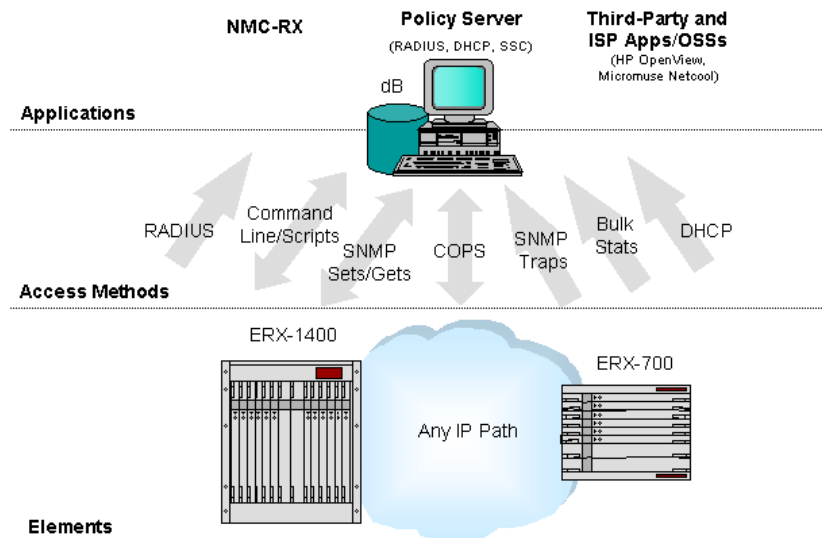


Figure 4-1 Management of ERX edge routers

Starting at the bottom of Figure 4-1 with the ERX edge router itself, the ERX system can be managed in several ways:

- Via standard SNMP MIB variables. This is the method by which the NMC-RX network management application communicates with the ERX system. SNMP traps and SNMP statistics are also issued by the ERX system and can be sent to multiple host destinations.
- Via a Cisco-like command line interface (CLI). Operators who are familiar with the Cisco CLI can configure and manage the ERX system immediately with no additional training. In addition, scripts developed for Cisco routers can be used with the next-generation ERX edge router.

- Via a Common Open Policy Server (COPS). This interface allows the system to be controlled by other applications with a reliable delivery mechanism for real-time configuration changes. The Service Deployment System (SDX) uses COPS to communicate with the ERX system.
- Via Bulkstats. The ERX system has the ability to collect and store statistics in an ASCII file that can be retrieved from the system via FTP. This allows for efficient gathering of statistical information, eliminating the polling overhead of SNMP statistics retrieval. You can FTP the file to a server as often as every five minutes or only once per day.

A number of applications can control the ERX system:

- NMC-RX application – A network management application that delivers a graphical way to manage and control a network of ERX systems. It can dramatically reduce provisioning times for service provider operators who prefer GUI-based interfaces. It also delivers advanced management control, allowing service provider operators to manage ERX systems logically, by customer and service, in addition to managing by the standard physical level.
- Policy servers – Servers such as RADIUS or the SDX product can dynamically configure the ERX system in response to customer input. These types of servers are especially valuable in B-RAS applications, where subscriber configurations need to involve minimal operator assistance. Interaction with these servers allows an ERX system to provision individual subscribers dynamically, with “zero touch” by the operators after the initial system configuration.
- OSSs – The NMC-RX application has an open architecture that allows it to interface with existing OSSs. Its Java Remote Method Invocation (RMI) interfaces allow information to pass to higher-level applications seamlessly.
- HP OpenView – The ERX system can be managed via integration with HP OpenView Network Node Manager, which allows for icon display and coloring, and fault management. In addition, the NMC-RX application can be integrated into the OpenView application for a single management interface to the element.
- Micromuse Netcool – This fault management tool can be used to manage the ERX system.
- Other third-party applications – The ERX system can be managed by any standards-based third-party application, such as provisioning and monitoring. There are specific applications for which the ERX system

is already integrated, alleviating this work from the service provider. These include: Quallaby PROVISIO network performance monitoring and service assurance software for performance management, including generation of reports, and Orchestream Service Activator software for MPLS VPN management.

SNMP Features

Each ERX system has its own SNMP agent. The agent is located on the system's active SRP module. UDP/IP is used for the transport.

The following SNMP features are supported:

- Support for SNMP Version 1 (v1), Version 2 Community-based (v2c), and Version 3 (v3)
- SNMP control of the system with GET and SET support
- SNMP access control
- SNMP trap management and filtering
- SNMP error statistics
- PDU size support from 484 – 8192 bytes
- 32-bit and 64-bit octet statistical SNMP counter support to handle high-speed interfaces (such as Gigabit Ethernet and OC12/STM4)
- All SNMP control parameters can be configured through the CLI

RFCs Supported

The following RFCs are supported:

- RFC 1155 – Structure and Identification of Management Information for TCP/IP-based Internets (May 1990)
- RFC 1157 – A Simple Network Management Protocol (SNMP) (May 1990)
- RFC 1212 – Concise MIB Definitions (March 1991)
- RFC 1215 – A Convention for Defining Traps for use with the SNMP (March 1991)
- RFC 1901 – Introduction to Community-based SNMPv2 (January 1996)
- RFC 1905 – Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2) (January 1996)

- RFC 1906 – Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2) (January 1996)
- RFC 1907 – Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2) (January 1996)
- RFC 2576 – Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework (March 2000)
- RFC 2578 – Structure of Management Information Version 2 (SMIPv2) (April 1999)
- RFC 2579 – Textual Conventions for SMIPv2 (April 1999)
- RFC 2580 – Conformance Statements for SMIPv2 (April 1999)

See *Security Features* later in this chapter for information on management access to the individual ERX devices.

Each virtual router instance can have a unique SNMP proxy agent to maintain secure management access between virtual routers.

SNMP Traps

The system fully supports SNMP traps. Traps are generated for the following categories:

- Standard SNMP traps (for example, coldstart, authentication, link up, link down)
- ERX system-level traps (for example, board insert, board removal, temperature change)
- Routing protocol traps (for example, BGP-4-specific traps)

Traps issued by the system can be sent to up to eight different IP hosts simultaneously. Several parameters can be controlled, including the:

- IP address of the host
- Community name to send in the trap message
- SNMP format (v1, v2c, or v3) of the trap
- Categories of traps to be sent (for example, SNMP, system-level, routing protocol)
- Severity level of traps to be sent

These features allow a service provider to assign varied classes of traps to different service provider network operators, such as all system-level traps to network operator #1 and all routing-level traps to network

operator #2. Individual traps can also be enabled or disabled for each ERX system and for each IP host destination. This feature reduces the number of SNMP traps issued by the system.

SNMP Support

Juniper Networks supports the standard MIBs in the following list on the ERX system. In addition to standard MIBs, Juniper Networks supports a wide array of proprietary MIBs for your system.

ATM MIBs

- RFC 2515 – Definitions of Managed Objects for ATM Management (February 1999)
 - > ATM Interface Configuration group
 - > ATM VCC Termination group (read-only support)
 - > ATM AAL5 VCC group
 - > ATM Interface TC Sublayer group
- ATM Forum SNMP-M4-MIB – AF-NM-0095.001
 - > ATM Cell Layer Interface Loopback Location Code object
 - > ATM VCL Termination Point Configuration Extensions group
 - > ATM VP Termination Point Test group
 - > ATM VC Termination Point Test group

BGP-4 MIB

- RFC 1657 – Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIV2 (July 1997)

Ethernet MIB

- RFC 2665 – Definitions of Managed Objects for the Ethernet-like Interface Types (August 1998)

Frame Relay MIBs

- RFC 2115 – Management Information Base for Frame Relay DTEs Using SMIV2 (September 1997)
- RFC 2863 – The Interfaces Group MIB (June 2000)

Interface MIBs

- RFC 2495 – Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types (January 1999)
- RFC 2496 – Definitions of Managed Objects for the DS3/E3 Interface Types (January 1999)
- RFC 2863 – The Interfaces Group MIB (June 2000) – linkUp/Down SNMP trap support

IP MIBs

- RFC 1213 – Management Information Base for Network Management of TCP/IP-based Internets: MIB-II (March 1991)
- RFC 2011 – SNMPv2 Management Information Base for the Internet Protocol using SMIV2 (November 1996)
- RFC 2012 – SNMPv2 Management Information Base for the Transmission Control Protocol using SMIV2 (November 1996)
- RFC 2013 – SNMPv2 Management Information Base for the User Datagram Protocol using SMIV2 (November 1996)
- RFC 2096 – IP Forwarding Table MIB (January 1997)
- RFC 2667 – IP Tunnel MIB (August 1999)

OSPF MIB

- RFC 1850 – OSPF Version 2 Management Information Base (November 1995)

PPP MIBs

- RFC 1471 – The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol (June 1993)
- RFC 1473 – The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol (June 1993)
- RFC 2863 – The Interfaces Group MIB (June 2000)

RIP MIB

- RFC 1724 – RIP Version 2 MIB Extension (November 1994)

SNMP MIBs

- RFC 1213 – Management Information Base for Network Management of TCP/IP-based Internets: MIB-II (March 1991)
- RFC 1907 – Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2) (January 1996)

SNMP v3 MIBs

- RFC 2571 – An Architecture for Describing SNMP Management Frameworks (April 1999)
- RFC 2572 – Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) (April 1999)
- RFC 2573 – SNMPv3 Applications (April 1999)
- RFC 2574 – User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) (April 1999)
- RFC 2575 – View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) (April 1999)
- SNMP Notification – SNMP-NOTIFICATION-MIB

SONET MIBs

- RFC 2558 – Definitions of Managed Objects for the SONET/SDH Interface Type (March 1999)
- sonetMediumTable
- sonetSectionCurrentTable
- sonetSectionIntervalTable
- sonetLineCurrentTable
- sonetLineIntervalTable
- sonetPathCurrentTable
- sonetPathIntervalTable

UDP MIB

- RFC 2013 – SNMPv2 Management Information Base for the User Datagram Protocol using SMIV2 (November 1996)

Juniper Networks ERX Enterprise MIB

- Boot and dump configuration parameters, diagnostics results for each slot, software revision, SNMP control, control for interface creation and deletion (such as the FT1, T1, PPP, Frame Relay, Frame Relay subinterfaces, ATM AAL5, and ATM subinterfaces), and virtual router configuration.

Command Line Interface

The ERX system supports a complete CLI to support system configuration, monitoring, and troubleshooting. The CLI has an industry *de facto* standard look and feel, and requires little, if any, operator retraining for operators familiar with routing interfaces.

Operator access to the CLI is covered in *Security Features* later in this chapter.

Following is a set of sample configuration commands that could be used to configure an ATM uplink. (See *ERX Physical and Link Layers Configuration Guide, Chapter 10, Configuring ATM*, for the exact command syntax when configuring the system.)

- 1 Configure a physical interface.

```
host1(config)#interface atm 0/1
```

- 2 Configure the subinterface.

```
host1(config-if)#interface atm 0/1.20
```

- 3 Configure a PVC by specifying the VCD, VCI, VPI, and the encapsulation type.

```
host1(config-if)#atm pvc 10 22 100 aal5snap
```

- 4 Assign an IP address and subnet mask to the PVC.

```
host1(config-subif)#ip address 192.32.10.20 255.255.255.0
```

The system also supports **show** commands. The example below shows the result displayed for a **show atm interface** command. (See the *Command Reference Guide* for exact syntax for **show** commands.)

```
host1#show atm interface atm 3/0
ATM Interface 3/0 is down, line protocol is disabled

AAL5 operational status:          lowerLayerDown
    time since last status change: 11 days, 23 hours
ATM operational status:          lowerLayerDown
    time since last status change: 11 days, 23 hours
```

```
SONET path operational status: lowerLayerDown
    time since last status change: 12 days, 1 hours
SONET operational status:      down
    time since last status change: 12 days, 1 hours
```

```
UNI version: Auto-config, Maximum VCs: 4096
E164 Address:
ATM E164 Address Configured: NO
ATM E164 Auto Conversion: disabled
ATM E164 Gateway: disabled
ATM E164 Translation: disabled
Current VCs: 1
Max VCI per VPI: 32768
signalling VPI/VCI: 5/5, VCD 1
QSAAL status: disconnected
Network prefix:
CAC admin state: disabled
SNMP trap link-status: disabled
OAM cell receive status: enabled
atm oam loopback-location 0xFFFFFFFF
```

```
PHY Type: oc3, Framing: sonet, TX clocking: line
Loopback: none, Receive FIFO Overruns: 0
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
InPackets:      0
InBytes:        0
InCells:        0
OutPackets:     0
OutBytes:       6213840
OutCells:       517820
InErrors:       0
OutErrors:      0
InPacketDiscards: 0
InByteDiscards: 0
InCellErrors:   0
```

```
qos-mode-port disabled
```

Script Capability

The ability to automate device configuration is critical to large service providers. Automation reduces configuration time and errors by implementing a consistent process for the operator. The ERX system

offers two scripting functions: the ability to load external CLI scripts and an innovative, versatile macro language.

External CLI Scripts

External scripts can be referenced by the ERX system to allow administrators to create and perfect a set of commands and then consistently use them in standard configurations. These scripts are ASCII files that contain any number of CLI commands.

Scripts can also be generated from the existing system configuration with a **show config** command. This ability allows the service provider to capture the existing configuration within the system for duplication on other systems or for archival storage.

Scripts are executed by the operator using a CLI command and can be stored in NVS on the SRP module or on a network-resident host. The circumstances under which a particular script or configuration file is used for rebooting are configurable.

The ERX system's script function can interpret scripts developed for Cisco routers to configure the system. This function allows service providers to use existing scripts developed for a Cisco router with their new ERX edge router.

Scripting Language

The system supports a powerful internal scripting language that allows the operator to automate repetitious tasks and create miniprograms to configure the system. Macros are loaded into the system by the operator through the CLI and can be run on an ERX system during operation.

Example The following is an example of the system's scripting capability:

```
<# atmIf #>
<# slotPort:=env.getline("slot/port?") #>

<# while (vcType != 1 && vcType != 2);
  vcTypeStr :=env.getline("VC type (1 = AAL5MUX IP, 2 =
  AAL5SNAP)?");
  vcType := env.atoi(vcTypeStr);
endwhile #>
<# if vcType = 1; vcTypeStr := "aal5mux ip"; else; vcTypeStr
:= aal5snap; endif #>

<# encapRouted:=1; encapBridged:=2; encapPPP:=3 #>
<# while (encapType < encapRouted || encapType > encapPPP );
  encapTypeStr :=env.getline("encapsulation (1 = routed, 2
= bridged, 3 = ppp)?");
```

```

        encapType := env.atoi(encapTypeStr);
    endwhile #>
<# if encapType = encapPPP #>
    <# authNone:=1; authPap:=2; authChap:=3; authPapChap:=4;
    authChapPap:=5 #>
    <# while (authType < authNone || authType > authChapPap );
    authTypeStr :=env.getline("authentication (1 = None, 2 =
    PAP, 3 = CHAP, 4 = PAP/CHAP; 5 = CHAP/PAP)?");
    authType    := env.atoi(authTypeStr);
    endwhile #>
    <# endif #>

<# vpStartStr := env.getline("Starting VP number?");
    vpStart:=env.atoi(vpStartStr)#>
<# vpEndStr    := env.getline("Ending   VP number?"); vpEnd
:=env.atoi(vpEndStr)#>
<# vcStartStr := env.getline("Starting VC number?");
    vcStart:=env.atoi(vcStartStr)#>
<# vcEndStr    := env.getline("Ending   VC number?"); vcEnd
:=env.atoi(vcEndStr)#>

<# loopbackStr := env.getline("Loopback interface number or
<cr>?") #>

<# vp := vpStart; while vp <= vpEnd, ++vp #>
    <# vc := vcStart; while vc <= vcEnd, ++vc #>
    interface atm <#slotPort $ '.' $ ++i;\n'#>
    atm pvc <# i; ' '; vp; ' '; vc; ' '; vcTypeStr;\n'#>
    <# if encapType = encapPpp #>
    encap ppp
    <# if authType = authPap#>
    ppp authentication pap
    <# elseif authType = authPapChap#>
    ppp authentication pap chap
    <# elseif authType = authChapPap#>
    ppp authentication chap pap
    <# elseif authType = authChap#>
    ppp authentication chap
    <# endif #>
    <# elseif encapType = encapBridged #>
    encap bridged1483
    <# endif #>
    <# if loopbackStr != "" #>
    ip unnumbered loopback <# loopbackStr;"\n" #>
    <# endif #>
!
    <# endwhile #>
!

```

```
<# endwhile #>  
<# endtmpl #>
```

Collecting Bulk Statistics

The ERX system offers an efficient data collection and transfer facility for accounting and performance-monitoring applications. The Juniper Networks ERX SNMP MIBs extend the accounting data collection mechanism defined in RFC 2513 to include support for connectionless networks.

Service providers need reasonably accurate data about customers' use of networks. This data is used for billing customers and must be available at a customer's request. Accounting applications based on SNMP polling models consume significant network bandwidth because they poll large volumes of data frequently.

Unfortunately, SNMP is not well suited for gathering large volumes of data, especially over short intervals. The bulk statistics (bulkstats) feature provides the capability for doing this by avoiding the need for continuous polling of SNMP statistics. It uses applications known as *collectors* to retrieve data. The ERX system then sends collected statistics via FTP to assigned hosts, known as *receivers*.

The data is stored in an ASCII file on the system and can be sent to servers periodically via FTP. The data can then be used by any third-party application.

Security Features

Operator access to the ERX system is protected by the network management architecture. Of course, the service provider should implement other security means, such as physical security or logical security via firewalls between the outside world and the operations centers.

All ERX management access methods, such as CLI, SNMP, and NMC-RX, implement authorization checks before enabling operator access.

CLI

The CLI supports access-level security that permits up to 16 unique levels of operator access. Each level can be configured for read and read-write access, as well as for restrictions on individual commands or command sets. To be permitted to an access level, the operator must log in with the

correct password. This supports different levels of operators who may need access to the system. Optionally, RADIUS-based operator authentication provides security at the individual operator level.

SNMP

Access lists are used to control operator access to the SNMP agent on the system. Both the source IP address of the NMS and the SNMP community name can be used to create the access list. This feature means that an incoming SNMP request is checked against the IP address/community name access filter list before it is fulfilled. Unauthorized users are not allowed access. This approach allows the service provider to control which SNMP operators or applications access the MIBs.

SSH

The ERX system supports the Secure Shell (SSH) Server protocol version 2 as a secure alternative to Telnet for ERX system administration. SSH supports secure remote login and other secure network services. It allows operators to manage remotely over a secure connection.

RADIUS

RADIUS is a distributed client/server system that protects networks against unauthorized access. Operators can be authenticated via RADIUS before access to the system is permitted.

NMC-RX

The NMC-RX application supports detailed security control. All operators must supply a username and password before they are allowed access to the ERX system. Administrators can create operator profiles. The administrator can set profile options for read and read-write access, as well as restricting users to individual ERX devices. This capability allows the service provider to divide up the network securely, with different operators managing different systems.

Juniper Networks Management Products Overview

Juniper Networks management products enable service providers to profit from highly differentiated content, multimedia, voice, and data services that attract and retain subscribers and partners. These standards-based management products enable service providers to take advantage of emerging standards and technologies—while extending existing networks

and applications—and to deliver value-added services across diverse network architectures. All the managements products are designed to extend the functionality of an existing OSS infrastructure.

The management products include:

- NMC-RX application
- SDX application with UMC MetaDirectory option
- Integration packs for management applications

NMC-RX Application

The NMC-RX application is a stand-alone network management application that is capable of provisioning and controlling an entire network of ERX systems. This application comprises a set of tools that enables service providers to quickly and easily provision an ERX system and its physical interfaces, protocols, and services. In addition, it delivers a key advantage over other applications by allowing operators to view and manage the ERX network elements in terms of customers and services.

The Java-based NMC-RX application provides a graphical user interface (GUI) to augment traditional CLI and SNMP-based methods of configuring the ERX system. With a GUI-based application, operators are freed from learning arcane commands and have a more intuitive window into the network operation. The NMC-RX application also stores all configuration information in a relational database, giving operators new levels of ability in terms of organizing element data, synchronizing element configurations, and speeding element configuration. In addition, the NMC-RX application is a cost-effective client/services platform, easily able to support all operators who need access to the software.

NMC-RX Architecture

The NMC-RX application is optimized for GUI-based provisioning control of the ERX system. The NMC-RX application runs on both Windows (95/98/NT) and Sun Solaris UNIX (Version 2.7). The Windows version delivers a cost-effective program that allows operators to install the NMC-RX client application on laptops and home systems.

The NMC-RX architecture comprises several key elements:

- ODBC relational database
- Java client application installed on each management station
- Polling Service
- ConfigSync Service

These elements are individual applications and can be run as separate processes over multiple host machines if desired to scale performance.

Relational Database The NMC-RX architecture is based on an SQL-compliant ODBC (Open Database Connectivity) relational database system (RDBS). This standards-based approach allows the NMC-RX client applications to communicate with a single centralized host. It also allows the NMC-RX architecture to be independent of vendor databases, capable of supporting any SQL-compliant database including Sybase, Microsoft SQL, and Oracle. The current version of the product ships with Sybase SQL.

This NMC-RX database architecture enforces a tight security policy, with all function calls entered and checked by the database before they are issued to the element. This policy provides a secure buffer between operators and subscribers.

Java Technology The NMC-RX uses a Sun Microsystems Java-based architecture. The Java programming language allows all applications to be platform independent and capable of running on multiple different operating systems. This capability allows Juniper Networks to draw from a wide base of experienced programmers to quickly add new features and reports for our service provider customers and their subscribers.

Java Application The Java application downloads to run on one or more client management machines and then executes locally on the client machine. Java software provides platform independence for the application, allowing it to be run on Windows, NT, or UNIX machines.

Polling Service The Polling Service is a separate application that allows the service provider to obtain information about the health of ERX elements. The Polling Service operates by contacting each of the designated elements and polling them for status information. It returns the state of the element and its interfaces and displays the information graphically. Service provider operators can use this function as an early

warning detection of element problems or to monitor problem interfaces. The Polling Service is also architected to support advanced, targeted polling of elements or interfaces so that the service provider can more accurately pinpoint element interfaces for monitoring.

ConfigSync Service The ConfigSync Service provides device discovery services. When you create a new device through the NMC-RX application, the ConfigSync Service discovers the device on its network and obtains information about it.

Streamlined Provisioning

One of the most critical functions for service providers is the ability to quickly provision new elements and new services. Performing this function cost effectively becomes critical when mass market B-RAS services are offered to subscribers. The ERX system offers a number of ways to automate provisioning, which can be viewed in two stages:

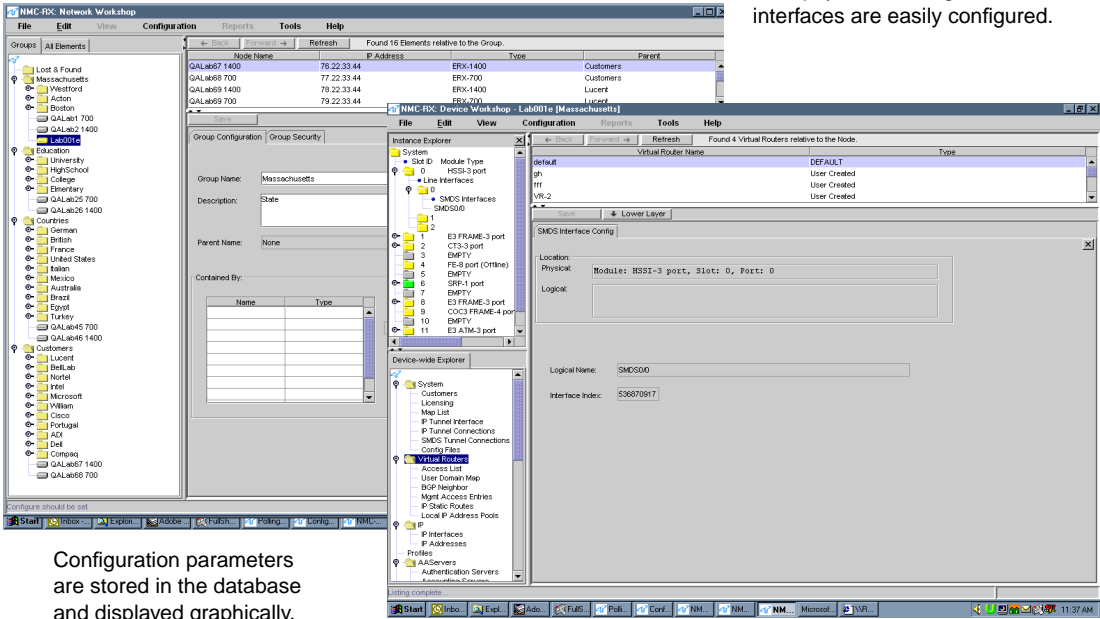
- **Initial provisioning** – This stage encompasses such tasks as configuration of the hardware, physical interfaces, and protocols. This stage also includes mapping customers to configurations in order to implement customer-based management. The NMC-RX application provides a number of time-saving tools to help streamline this process while also eliminating configuration mistakes.
- **Subscriber-level provisioning** – This stage is for mass market applications, such as xDSL termination and service delivery. The ERX system automates provisioning to drive cost-effective network rollout. Both RADIUS and the SDX application can be used to auto-provision subscribers as they enter the network by assigning different levels or types of service with no intervention by the network operator.

Intuitive Workshop Approach

There are two main work areas in the NMC-RX application: the network-level workshop and the device-level workshop. These work spaces allow the operator to manage both network-wide configurations and also specific elements (devices).

Network Workshop

Both physical and logical interfaces are easily configured.



Configuration parameters are stored in the database and displayed graphically.

Device Workshop

Figure 4-2 Network-level and device-level workshops

Network Workshop At the Network Workshop level, an operator can perform the following functions:

- Create and configure new groups
- View or reconfigure existing groups
- Organize groups into a hierarchy
- Create new devices
- Create new customers
- Create new users (if you are an administrator)
- Access the Device Workshop
- Create server sets to ease the provisioning of RADIUS, accounting, and authentication servers

The power of the network level is that operators can group elements together in meaningful ways, which allows the operator to manage the network in a way that is logical.

Access to groups and elements is controlled by passwords and security privileges associated with groups. Only approved operators are allowed to configure an ERX system. This privilege is controlled by community lists and access lists of approved IP addresses, which allows for enforcement of an IP address match before the system can be configured.

Device Workshop At the device workshop level, an operator can perform the following functions:

- Configure a device's objects
- View configurations and statistics
- Delete devices
- List objects configured on the devices
- List customers associated with a device
- Create templates
- Run diagnostics

In addition, the NMC-RX application will autodiscover all installed components within a given ERX system, allowing operators to ensure installed configurations and easing initial provisioning tasks.

Streamlined Provisioning via Templates

The NMC-RX application offers a key feature to help operators speed network provisioning and also reduce the number of errors made during configuration. The NMC-RX template function allows the operator to create and store standard configurations and reuse those configurations when initializing a new element or interface. See Figure 4-3.

Powerful templates feature allows for “configure once, replicate many times” to speed provisioning of new users, new interfaces, or new ERX systems.

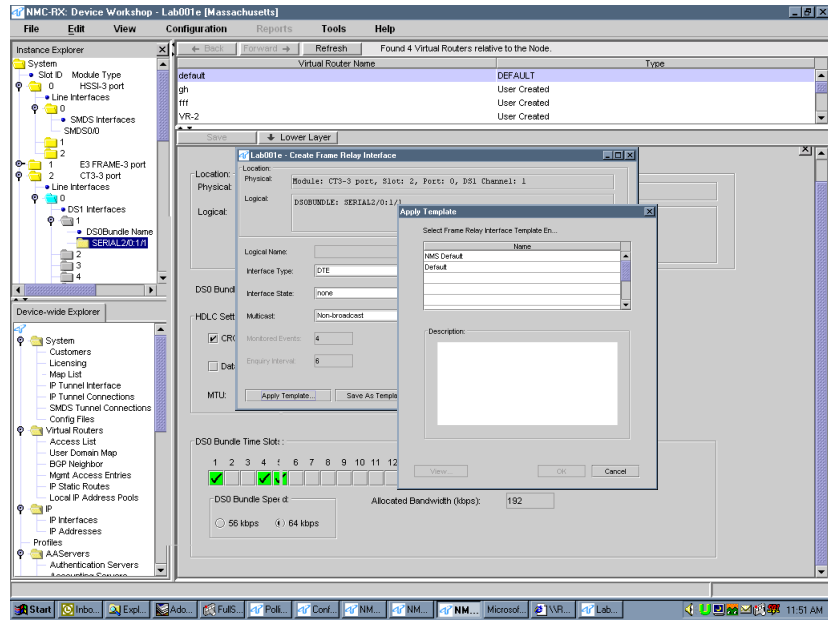


Figure 4-3 Templates feature

An advanced feature allows the service provider to bundle templates together to create service templates for a complete configuration. This allows the service provider to group together items that are configured to make a service – such as *gold* service or T1 internet access service.

Statistics Display

As part of the configuration process, the NMC-RX application also gives the ability to display statistics on a given element. The service provider can then display real-time statistics that are provided by the Polling Service on an individual element.

Customer-Driven Management

As service providers strive to offer competitive service delivery, the network management paradigm is changing from one of *element and service management* to one based on *customer management*. The NMC-RX application offers advanced capabilities that allow the operator to associate customers and customer sites with the service-delivering elements and then manage the network according to the customer’s needs. See Figure 4-4.

You can list all customers on a specific device, circuit, or interface.

You can associate customers with interfaces, allowing for powerful tracking features.

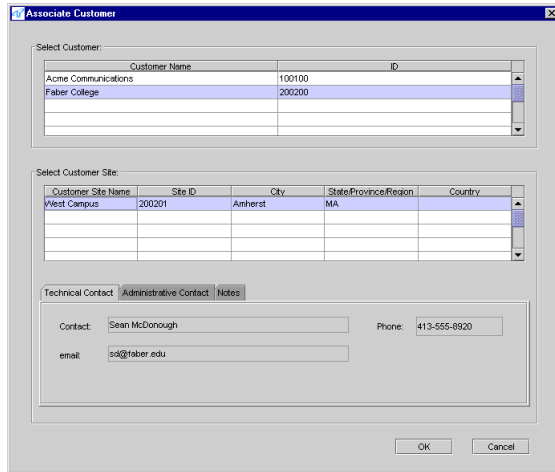


Figure 4-4 Associating customers and customer sites with services

Operators can use the powerful database of the NMC-RX application to create and store customer-to-element associations and then pull from this database to:

- Configure new customer sites according to a service profile
- Find all customers with traffic on a specific element to proactively warn when downtimes may happen
- Find all customers associated with a given element in case of a service-related fault to ensure that proper compensation is made to the right customers
- Easily find and modify the configuration settings of a particular customer when the customer upgrades or changes service requirements

OSS Integration

The NMC-RX open architecture makes it capable of easily integrating with existing OSSs already in place inside service provider networks. These might include HP OpenView NNM, Quallaby PROVISIO software and Orchestream Service Activator software, or custom-developed accounting and configuration applications. Northbound Common Object Request Broker Architecture (CORBA) and Java RMI-based interfaces allow for an open interface to all configuration capabilities in the NMC-RX application. In addition, the standards-based compliance of the

ERX system allows applications to communicate directly to the element via SNMP or CLI.

SDX Application

Designed to ease key steps in the service life-cycle process, the SDX application provides integrated service management, including service creation, subscriber management, service activation, and accounting capabilities. The SDX application enables service providers to rapidly create and deploy new services to hundreds of thousands of subscribers over a variety of broadband access technologies, such as DSL, cable, Ethernet, and fixed wireless. Working with the ERX edge router, the SDX application lets users activate service offerings as they need them and provisions the network to deliver those services; service activation becomes a fully automated, real-time process.

The SDX application includes three integral functionalities that address the critical phases of the service life cycle. These functionalities include:

- Intelligent Service Creation – builds innovative services
- Intelligent Service Activation – delivers services on demand to subscribers
- Intelligent Service Accounting – tracks, collates, and rates service usage to enable rich and creative tariff models

Intelligent Service Creation

The traditional approach to creating new services is to hard code services, such as firewalls or VPNs, into network elements. However, this approach limits service offerings and may result in performance sacrifices.

Providers can use the SDX application to easily configure different levels of service offerings and to provide services on demand.

Using service templates, providers can transform edge device features such as policy routing, filtering, rate limiting, traffic shaping, and multicasting into service building blocks. They can then combine those blocks with content servers to define a wide range of access, content, and bundled services. These service definitions are stored in a logically centralized directory, along with subscriber information. They can be activated at any time by a subscriber's mouse click on a Service Selection Portal (SSP) page.

In addition, creative tariff models may be defined in association with new services. Such tariff models may be based on a combination of flat fees, pay-per-time, pay-per-byte, discounts, and other criteria.

With the SDX application, providers can quickly define service parameters, efficiently create services, and economically deliver the services to subscribers. By delivering content and applications with the most appropriate bandwidth, latency, and quality of service, subscribers' service is optimized. The SDX application also provides the ability to use multiple differentiated tariff models, which helps to promote a steady service revenue stream and reduces demands on customer care resources.

Dynamic, On-Demand Service Activation

When a specific service is activated for a user, the SDX application retrieves policy and provisioning information from the directory for that service. The application then uses the information to quickly and automatically update the ERX system configuration and manages network resources to control QoS levels that provide an optimal experience for subscribers. It invokes the policy rules and parameters that characterize a service and ensures proper mapping to network elements. Modeled on the IETF policy framework, this carrier-grade, directory-driven service activation engine acts as the decision point for service requests coming from users and interfaces directly with network elements to enforce policies. In addition, collection of service and policy usage data is initiated to track service sessions.

Web-Based Customizable Portal

Reducing the cost of operations and building closer bonds with subscribers are essential for any service provider's success. Enabling subscribers to activate services instantaneously when they want to use them is key to achieving this goal.

The Intelligent Service Activation function of the SDX application includes a customizable Web-based portal, the SSP, which can be tailored to providers' presentation needs and customized to each individual subscriber. Dynamically generated from information stored in the subscriber profile, the SSP Web pages give subscribers instant access to personalized services without the need to interact with customer representatives. Proprietary client software is not required; the subscriber can use any Web browser.

Using the SDX application gives subscribers more control over their service choices and helps providers build closer bonds with subscribers and with retail partners, while letting providers retain control of their network.

Integration with OSS and Billing Applications

The Intelligent Service Accounting function of the SDX application tracks the service activity for each user and each service, collects usage information and rates it (enforcing the appropriate tariff model), and passes that information to the appropriate billing system.

Because service providers have made a significant investment in back office systems, it is important to note that the SDX application supports open interfaces and mediation mechanisms to facilitate system integration with diverse OSS applications, including customer care, order entry, provisioning, billing, security, and sales support systems.

UMC MetaDirectory Option

The UMC MetaDirectory option provides the scalability required by large or rapidly growing subscriber bases. This general purpose, highly scalable repository complies with X.500-93, X.509, and Lightweight Directory Access Protocol (LDAP) standards. Based on Siemens' award-winning DirX MetaDirectory application, its data management features include the ability to exchange information from external repositories, such as databases, and synchronize them bidirectionally. Such synchronization capability is key to allowing fast integration with existing OSSs.

The UMC MetaDirectory option houses infrequently changing information such as user profiles, service definition parameters, RADIUS authentication and authorization information, service policies, and service portal configurations, while providing a single point of administration.

HP OpenView Integration Pack

Using HP OpenView Integration Pack software, you can manage the ERX system with the HP OpenView manager-of-managers network management solution. HP OpenView provides in-depth views of networks, automatically discovers network devices, and provides an intuitive GUI representing the network topology. A multilevel map indicates which devices and network segments are healthy and which areas need attention.

When a flood of events resulting from a major device failure appears in its Alarm Browser, HP OpenView correlates the events and presents a summarized view of the failure, as well as offering trend analysis, thresholding, and data warehousing features that empower proactive network management. The HP OpenView Integration Pack also includes the capability to automatically launch the NMC-RX Element Management System directly from the HP OpenView GUI in a

context-sensitive manner, allowing operators to rapidly access the necessary tools for configuration and diagnostics.

IP OSS Alliance Program

Juniper Networks created the IP OSS Alliance Program to enable service providers to develop management strategies for their next-generation networks. This program features a number of market-leading and technically superior management solution vendors whose products complement the Juniper Networks management products. The goal of the program is to create a suite of compatible management products that provide an overall OSS architecture.

In addition, the program is designed to ensure that service providers can best use the complete set of features available from our devices to define services that best meet their own customers' needs. This approach gives service providers the advantage of tested and supported applications that perform all necessary management functions and the ability to purchase from vendors who are each experts in their respective areas.

The IP OSS Alliance Program includes vendors who are market and technical leaders in their fields, as well as promising new companies in each relevant area of specialization. This strategy allows service providers to use a new set of focused applications that effectively manage their multivendor environments and to free their technical staff to focus on next-generation network design. IP OSS Alliance partners are selected according to stringent criteria, including their product development goals, the strength and experience of their engineering core, their business focus and account presence, and their geographic location.

As we develop relationships with these companies, those that fulfill the promise of the program most effectively will be able to progress through a multitiered partner program that begins with relatively loose affiliation and continues towards true software concurrency and beta participation. This multitiered approach means that a broad variety of solutions are possible, from relatively simple single-point solutions to comprehensive OSS outsourcing.

In addition to the partnership with HP in the creation of the HP OpenView Integration Pack, Juniper Networks also has partners in a number of key areas. Enhanced fault management is possible through integration with Micromuse Netcool/OMNIBus, a market-leading solution that provides comprehensive real-time fault notification, correlation and management. In the performance management area, Juniper partners with:

- Performance management by Quallaby and Infovista, who both provide complete data collection, processing, and reporting

applications that allow service providers to make the best use of their network resources

- Integration with the award-winning Steel-Belted RADIUS authentication server from Funk Software
- VPN management by Orchestream Holdings plc, a leading provider of IP service activation and performance management software, for VPN management

As the IP Alliance Program evolves, we will add significantly to the list of partners who provide tightly integrated solutions that ensure rapid time-to-market for new networks and revenue-generating services.