

Chapter 8

Configuring Remote Access

This chapter describes how to configure remote access to your E-series devices.

Topic	Page
Overview	109
References	110
Before You Begin	111
Configuration Tasks	111
Configuring a B-RAS License	112
Creating User Domain Maps	113
Creating Authentication and Accounting Servers	114
Creating DHCP Relay Servers	115
Creating Local IP Address Pools	116

Overview

The NMC-RX application allows you to configure Broadband Remote Access Server (B-RAS) on your E-series device. The B-RAS application:

- Aggregates the output from digital subscriber line access multiplexers (DSLAMs)
- Provides user PPP sessions
- Provides PPP session termination
- Enforces quality of service (QoS) policies
- Routes traffic into an ISP's backbone network

A DSLAM collects data traffic from multiple subscribers into a centralized point so that it can be uploaded to your E-series device over an ATM connection via a DS3, an OC3, an E3, or an OC12 link.

The E-series device provides the logical termination for PPP sessions, as well as the interface to authentication and accounting systems.

B-RAS Protocol Support

Your E-series device supports the following protocols for B-RAS services for remote PPP clients:

- PPP
- PPP over Ethernet PPPoE
- Bridged Ethernet
- L2TP (LAC and LNS)
- L2F

B-RAS Data Flow

The E-series device performs several tasks for a digital subscriber line (DSL) PPP user to establish a PPP connection:

- Authenticates the subscriber through RADIUS authentication
- Assigns an IP address to the PPP/IP session via RADIUS, local address pools, or DHCP
- Terminates the PPP encapsulation
- Provides user accounting via RADIUS

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that protects networks against unauthorized access. RADIUS clients running on an E-series device send authentication requests to a central RADIUS server. This server contains all the required user authentication and network access information.

You can configure RADIUS authentication and accounting services via the NMC-RX application. The authentication service determines that a user is allowed to access a specific service or resource. The accounting service tracks service use by subscribers.

DHCP

Dynamic Host Configuration Protocol (DHCP) provides a mechanism through which computers using TCP/IP can obtain protocol configuration parameters automatically from a DHCP server on the network.

References

For more information about RADIUS, see *E-series Broadband Access Configuration Guide, Chapter 1, Configuring Remote Access*.

Before You Begin

Before you can configure B-RAS, you must:

Get a B-RAS license from Juniper Networks.

Create at least one group.

Create at least one E-series device.

Additionally, you must determine the following for the RADIUS authentication and accounting servers:

IP addresses

UDP port numbers

Secret keys

For information on associating servers with a virtual router and on setting the B-RAS parameters on a virtual router, see *Chapter 3, Configuring Virtual Routers*.

Configuration Tasks

Complete the B-RAS tasks in this order:

1. Configure a B-RAS license.
2. Create a user domain map entry.
3. Create authentication and accounting servers.
4. Create DHCP relay servers.
5. Associate the servers with virtual routers.
6. Create a local IP address pool.
7. (Optional) Create a bridged IP interface. See *NMC-RX User Guide, Vol. 1, Chapter 19, Configuring Bridged IP*.
8. Create a PPP over ATM or a PPP over Ethernet over ATM interface. See *NMC-RX User Guide, Vol. 1, Chapter 26, Configuring PPP* and *Chapter 27, Configuring PPP over Ethernet*.

Configuring a B-RAS License

Your B-RAS license is a string of alphanumeric characters provided by your Juniper Networks sales representative or by Juniper Networks customer service. Depending on the license purchased, you can activate 4000, 8000, 16000, or 32000 authenticated PPP sessions at any one time. The license key limits the number of active subscribers.



NOTE: To use a B-RAS license for 16,000 or more interfaces, your SRP module(s) must have 512 MB of memory.

To configure a B-RAS license:

1. In the Device-wide Explorer, under System folder, click Licensing, right-click, and click Configure.

The Licensing tab appears in the work area.

2. Enter the License String. See Table 39.

Table 39: Licensing parameters

Parameter	Description
License String	License string can contain up to 15 alphanumeric characters.
Number of PPP Sessions	Number of PPP sessions allowed by the given license string. The number of PPP sessions available is automatically filled in when you save a valid license string. If the string is invalid, an error message is displayed.

3. Click the Save button.

A dialog box appears asking if you want to save your changes.

4. Click Yes.

Creating User Domain Maps

You can configure RADIUS authentication, RADIUS accounting, DHCP servers, and local address pools for a specific virtual router, and then map a user domain to that virtual router.

The E-series device uses the name appearing to the right of the @ character in a username as the domain name. For example, juniper.net is the domain of xsmith@juniper.net. Your E-series device keeps track of the domain-name-to-virtual-router mapping.

When the E-series device is configured to require authentication of a PPP user, it checks for the appropriate user-domain-name-to-virtual-router mapping. If it finds a match, the E-series device sends a RADIUS authentication request to the RADIUS server configured for the specific virtual router.



NOTE: You cannot reconfigure a domain map entry. To change the virtual router assignment, you must first delete the domain map entry and then recreate it, selecting a different virtual router.

To create a user domain map entry:

1. In the Device-wide Explorer, select Virtual Routers, right-click, and click List All.

The names of all currently configured virtual routers on the device, including a default virtual router, appear in the list area.

Virtual Router Name	Type
default	DEFAULT
vrOne	User Created
VR-Yi_Test2	User Created
hgfhg	User Created

2. Select a virtual router in the list, right-click, select Create, and click User Domain Map Entry.

The Create User Domain Map Entry dialog box appears.

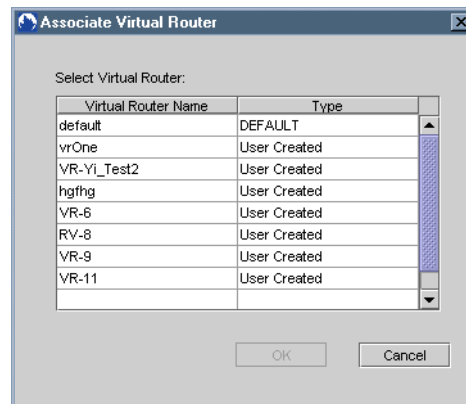
3. Set the parameters. See Table 40.

Table 40: User domain map parameters

Parameter	Description
Domain Name	Domain name you want to map (for example, juniper.net); maximum of 32 characters.
Virtual Router	Currently selected virtual router

- To change the virtual router name, click  to the right of the Virtual Router text box.

The Associate Virtual Router dialog box appears.



- Select a virtual router from the list, and click OK.

The virtual router you selected now appears in the Virtual Router text box of the Create User Domain Map Entry dialog box.

- Click OK.

Creating Authentication and Accounting Servers

You can create and configure up to ten authentication and ten accounting servers as part of the RADIUS services. Authentication service determines whether or not a user is allowed access to a specific service or resource. The accounting service tracks service use by subscribers.

If you do not configure a primary authentication or accounting server, all authentication and accounting requests will fail. You can configure other servers as backup in the event that the primary server cannot be reached.



NOTE: You can configure B-RAS with RADIUS accounting without RADIUS authentication. In this configuration, the username and password on the remote end are not authenticated and can be set to any value.

The authentication and accounting servers have the same parameters.

The following procedure can be performed from both the Network Workshop and the Device Workshop.

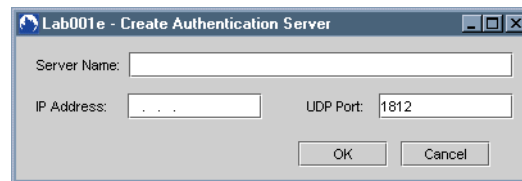


NOTE: Because the procedure for creating authentication and accounting servers is the same, only authentication servers are used in this example.

To create an authentication server:

1. On the Configuration menu, select Create, and click Authentication Server.

The Create Authentication Server dialog box appears.



2. Set the server's parameters. See Table 41.

Setting the parameters allows you to identify an authentication server as a network resource. When you associate a server with a virtual router, you can set parameters that can be specific to that particular virtual router. See *Chapter 3, Configuring Virtual Routers*.

Table 41: Authentication server parameters

Parameter	Description
Server Name	Name associated with this server; up to 32 alphanumeric characters
IP Address	Valid IP address for the server
UDP Port	Port where the RADIUS server can be contacted; range 0–65536

3. Click OK.

Creating DHCP Relay Servers

The Dynamic Host Configuration Protocol (DHCP) provides a mechanism through which computers using TCP/IP can obtain protocol configuration parameters automatically from a DHCP server on the network.

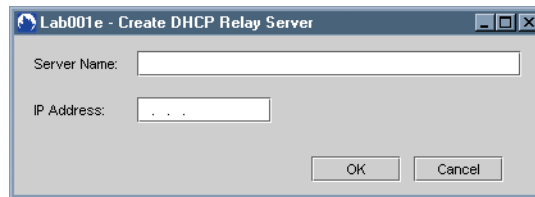
The DHCP server is typically centrally located and operated by the network administrator. An IP client contacts a DHCP server for configuration parameters. Because the server is run by a network administrator, DHCP clients can be reliably and dynamically configured with parameters appropriate to the current network architecture.

For PPP users, the E-series device acts as a DHCP client to obtain an address for the PPP user. This is referred to as DHCP proxy.

DHCP proxy client support enables the device to obtain an IP address from a DHCP server for a remote PPP client. Each virtual router (acting as a DHCP proxy client) can query up to five DHCP servers.

To create a DHCP relay server:

1. From the Configuration menu, select Create, and click DHCP Relay Server. The Create DHCP Relay Server dialog box appears.



2. Set the DHCP relay server parameters. See Table 42.

Setting the parameters allows you to identify a DHCP server as a network resource. When you associate a server with a virtual router, you can set parameters that can be specific to that particular virtual router. See *Chapter 3, Configuring Virtual Routers*.

Table 42: DHCP relay server parameters

Parameter	Description
Server Name	Name associated with this server; must not be more than 32 alphanumeric characters
IP Address	Valid IP address for the server

3. Click OK.

Creating Local IP Address Pools

IP address pools are configured for virtual routers. To make the E-series router use the address pools specified on the virtual router, the virtual router must have the addressing scheme set to *Local*.

You can configure the E-series device to provide an IP address during the authentication process. These IP addresses must be configured in a local IP address pool. Each address pool must be associated with a virtual router before it can be used.

Each local address pool is named and contains ranges of sequentially ordered IP addresses. These addresses are allocated when the AAA server makes a request for an IP address.

If a local address pool range is exhausted, the next range of addresses is used. If all pool ranges are exhausted, a new range can be configured to extend or supplement the existing range of addresses, or a new pool can be created. The newly created pool range is then used for future address allocation. If addresses allocated from the first pool range are released, then subsequent requests for addresses are taken from the first pool range.

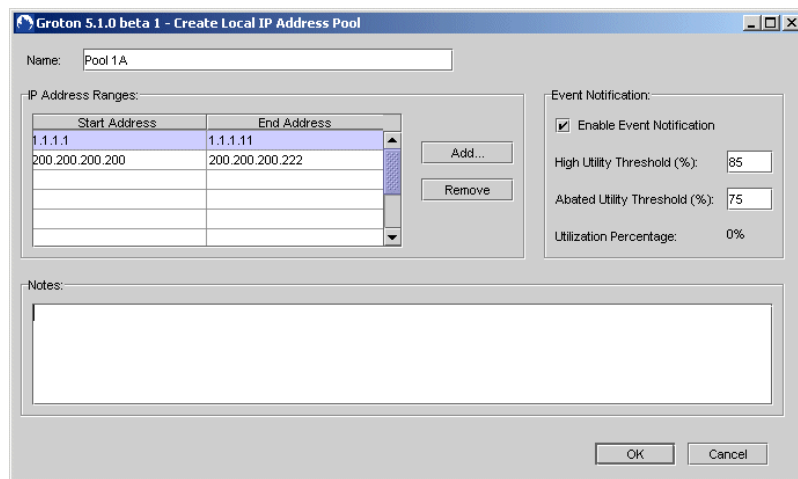
To create a local IP address pool:

1. From the Device-wide Explorer, select Virtual Routers, right-click, and click List All.

A listing of all available virtual routers appears in the list area.

2. Select a virtual router in the list, right-click, select Create, and click Local IP Address Pools.

The Create Local IP Address Pool dialog box appears.



3. Set the local IP address pool parameters. See Table 43.

Table 43: Local IP address pool parameters

Parameter	Description
Name	Name associated with this address pool; up to 32 characters
IP Address Ranges	
Add	Click to enter an IP address range. The Add Local IP Address Pool Range dialog box appears. After entering a start and end address, click OK. The range is added to the list. Start Address – First valid IP address available in the address pool End Address – Last valid IP address available in the address pool
Remove	Click to delete the selected IP address range. The range is removed from the list.
Event Notification	
Enable Event Notification	Enables utility threshold event notification through SNMP traps
High Utility Threshold (%)	Percentage of usage that triggers a high utility event notification; range 1-100; default: 85

Table 43: Local IP address pool parameters (continued)

Parameter	Description
Abated Utility Threshold (%)	Percentage of usage that triggers an abated utility event notification; range 1-100; default: 75
Utilization Percentage	Displays the percentage of IP addressees currently in use; range 0-100
Notes	Stores descriptive or contextual information of up to 256 alphanumeric characters

4. Click OK.

Configuring and Viewing IP Address Pools

You can configure IP address pools in two ways: list all address pools on a device or list address pools associated with a particular virtual router.

You can view the number of addresses per range, the number in use per range, and the percentage of address utilization by listing all address pools, right-clicking, and then clicking View. The results are displayed in the work area on the Local IP Address Pool tab.

Save Lower Layer

Local IP Address Pool

Name: abc

IP Address Ranges:

Start Address	End Address	Addresses	In Use
1.1.1.1	1.1.1.2	2	0

Add... Remove

Event Notification:

Enable Event Notification

High Utility Threshold (%): 85

Abated Utility Threshold (%): 75

Utilization Percentage: 0%

Notes:

