

Configuring Virtual Routers

3

Your ERX device allows you to create multiple virtual routers in a single system. Each virtual router has its own separate set of IP interfaces, forwarding table, and instances of routing protocols.

Topic	Page
Overview	3-1
References	3-2
Configuration Tasks	3-2
Creating Virtual Routers	3-3
Creating Management Access	3-21
Creating IP Static Routes	3-24

Overview

The ERX device supports multiple distinct routers within a single system. This support allows service providers to configure multiple separate and secure routers within a single chassis. These routers are identified as virtual routers (VRs). Applications for this function include the creation of individual routers dedicated to wholesale customers, corporate virtual private network (VPN) users, or a specific traffic type. An ERX device supports up to 1000 VRs.

Default Virtual Router

When you first boot your system, it creates a default virtual router. The only difference between the default virtual router and any other virtual router is that you cannot create or delete it. Just like any other router, the

default virtual router gets its IP addresses when you configure interfaces on it.

References

For more information related to virtual routers, see the following resources:

- *Associating a Customer with an IP Interface* in *NMC-RX User Guide, Vol. 1, Chapter 7, Configuring Customers*
- *Creating IP Interfaces* in *Chapter 6, Configuring IP* – information on associating IP interfaces with virtual routers
- *Creating User Domain Maps* in *Chapter 8, Configuring Remote Access* – information on creating user domain map entries on top of virtual routers
- *Creating Local IP Address Pools* in *Chapter 8, Configuring Remote Access* – information on creating local IP address pools on top of virtual routers
- *Creating Authentication and Accounting Servers* in *Chapter 8, Configuring Remote Access*
- *Creating DHCP Relay Servers* in *Chapter 8, Configuring Remote Access*

Configuration Tasks

To configure a virtual router:

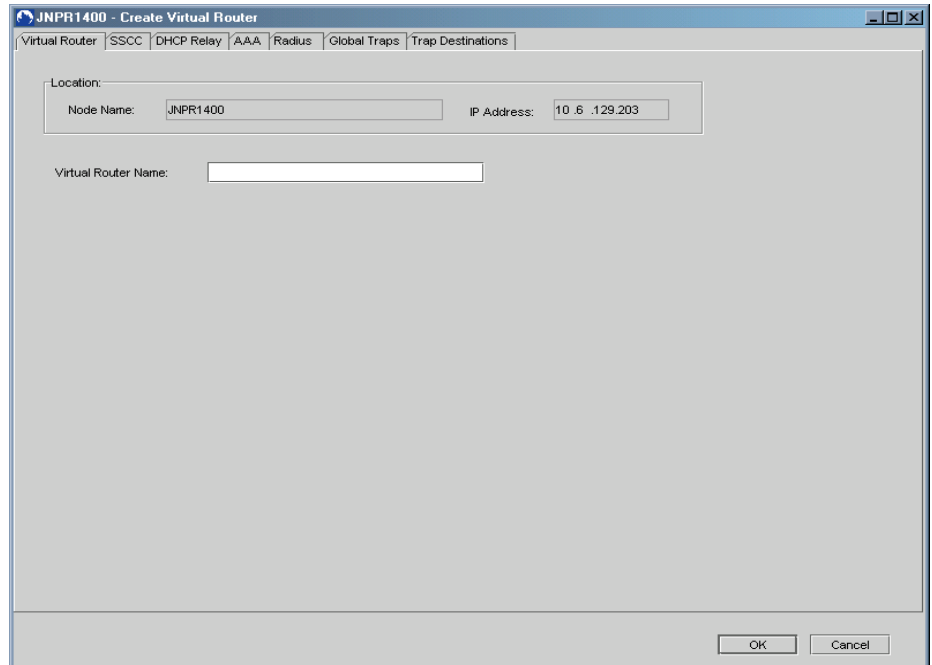
- 1 Create a virtual router.
- 2 Create one or more management access entries.
- 3 Create one or more access list entries.
- 4 (Optional) Create one or more IP static routes.
- 5 (Optional) Create an IP address pool. See *Creating Local IP Address Pools* in *Chapter 8, Configuring Remote Access*.
- 6 (Optional) Create a user domain map entry. See *Creating User Domain Maps* in *Chapter 8, Configuring Remote Access*.
- 7 (Optional) Configure trap destinations and global traps parameters. See also *Chapter 1, Configuring SNMP Traps*.

Creating Virtual Routers

In the NMC-RX application, you must use the Device-wide Explorer in the Device Workshop to create a virtual router:

- 1 In the Device-wide Explorer, click Virtual Routers.
- 2 Right-click, select Create, and click Virtual Router.

The Create Virtual Router dialog box appears.



This dialog box has the following tabs for ERX devices:

- Virtual Router – Allows you to name the virtual router
- SSCC – Allows you to set the parameters for the SDX client (formerly SSCC)
- DHCP Relay – Allows you to enable the DHCP relay agent and to associate DHCP relay servers with the virtual router
- AAA – Allows you to set the attributes related to authentication, accounting, and address resolution
- Radius – Allows you to set the parameters for RADIUS protocols and to associate authentication and accounting servers with the virtual router

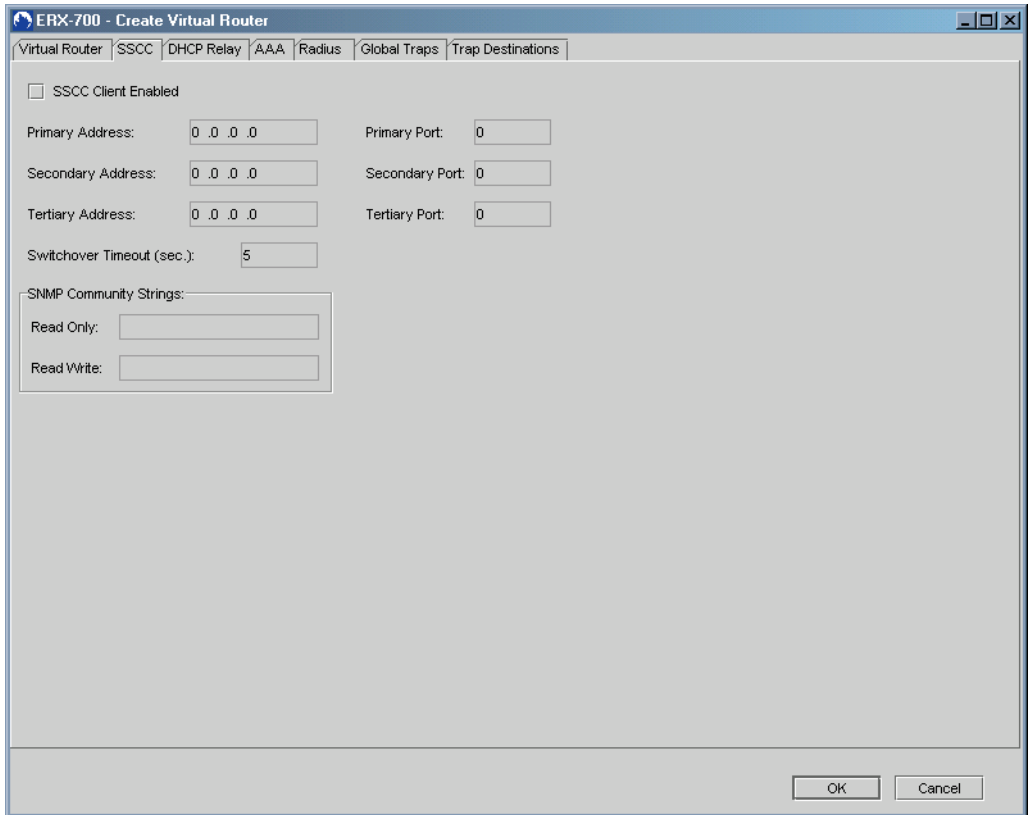
- Global Traps – Allows you to set global trap parameters for the specified virtual router
 - Trap Destinations – Allows you to set trap destination parameters for the specified virtual router
- 3 On the Virtual Router tab, type a name for the virtual router in the Virtual Router Name text box. The name can be up to 15 characters long.
 - 4 Set the parameters for each tab on the Create Virtual Router dialog box. See the following sections for information.
 - 5 When you have finished setting the parameters, click OK to save the new virtual router.

Configuring the SDX Client

The ERX device has an embedded client that interacts with the Service Deployment System (SDX; formerly SSC, Service Selection Center). To configure the SDX client, you specify the IP addresses of primary, secondary, and/or tertiary SDX servers. You can specify the port on which each SDX server listens for activity. Also, you can identify SNMP community strings, which permits a communication exchange between the SDX and NMC-RX applications.

To configure the SDX client parameters:

- 1 Click the SSCC tab.



- 2 Set the parameters. See Table 3-1.

Table 3-1 SDX client parameters

Parameter	Description
SSCC Client Enables	Enables the SDX client
Primary Address	IP address for the primary SDX server
Secondary Address	IP address for the secondary SDX server (optional)
Tertiary Address	IP address for the tertiary SDX server (optional)
Switchover Timeout (sec.)	Number in the range 5–300 seconds. The delay period during which the SDX client waits for a response from the SDX server. When the timer expires, the client attempts to reach the secondary server and, if that fails, the tertiary server, before trying the primary server again. The client waits for the delay period with each attempt.

Table 3-1 SDX client parameters (continued)

Parameter	Description
Primary Port	Port on which the primary SDX server listens for activity
Secondary Port	Port on which the secondary SDX server listens for activity (optional)
Tertiary Port	Port on which the tertiary SDX server listens for activity (optional)
SNMP Community Strings	
Read Only	SNMP Read Only community string used by SDX application when communicating with this virtual router; up to 32 alphanumeric characters
Read Write	SNMP Read/Write community string used by SDX application when communicating with this virtual router; up to 32 alphanumeric characters

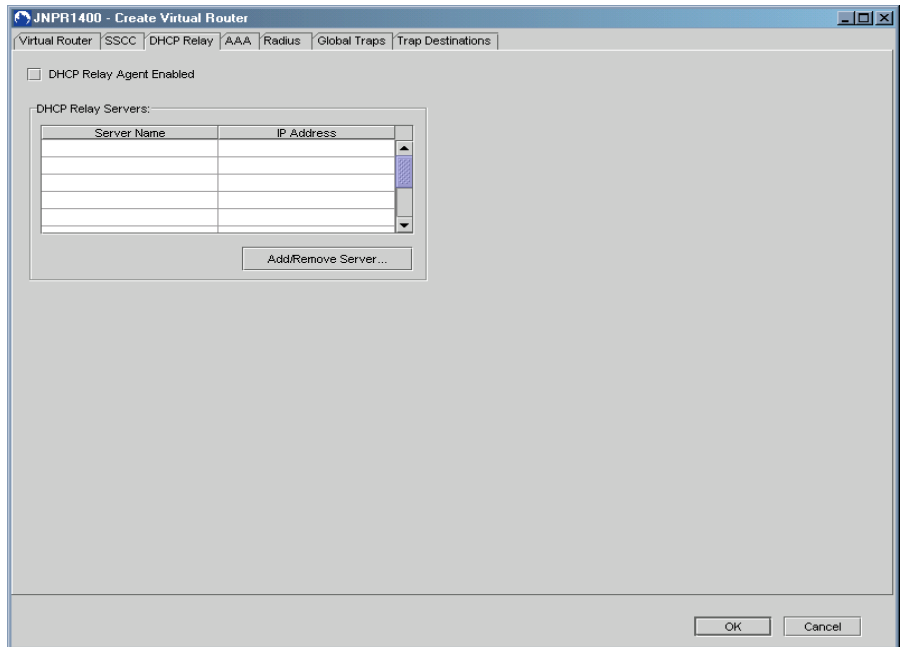
- 3 If you have finished creating the virtual router, click OK. Otherwise, continue to the next tab.

Associating DHCP Relay Servers

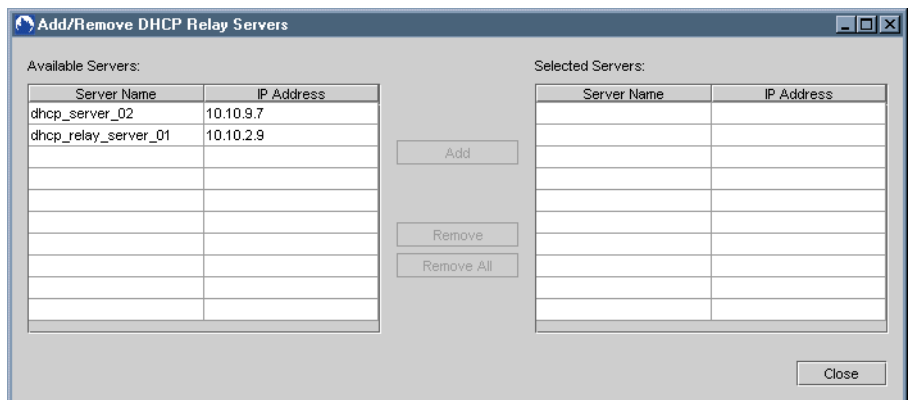
The DHCP Relay tab allows you to associate DHCP relay servers with the virtual router you are creating on an ERX device. The DHCP relay feature relays a request from a remote client to a DHCP server for an IP address. When the system receives a DHCP request from an IP client, it forwards the request to the DHCP server and passes the response back to the IP client.

To associate a DHCP Relay server with the virtual router:

- 1 Click the DHCP Relay tab.



- 2 To enable the DHCP Relay Agent, select the check box.
 When you enable the agent, the ERX device adds the DHCP relay agent information option to every packet it relays from a DHCP client to a DHCP server.
- 3 Click Add/Remove Server to associate servers with the virtual router.
 The Add/Remove DHCP Relay Servers dialog box appears.



- 4 To associate a server with the virtual router, select the server in the Available Servers list, and click Add.

The server's name appears in the Selected Servers list.



Note: You can associate a maximum of five DHCP relay servers with a single virtual router.

- 5 Click Close.

The application returns to the DHCP Relay tab with the selected servers added to the table.

- 6 If you have finished creating the virtual router, click OK. Otherwise, continue to the next tab.

Configuring AAA

The AAA tab provides access to the parameters for authentication, accounting, and address resolution on an ERX device.

To configure AAA:


- 1 Set the parameters for authentication and accounting. See Table 3-2.

The screenshot shows the 'JNPR1400 - Create Virtual Router' dialog box with the 'AAA' tab selected. The dialog has several sections for configuration:

- Authentication:** Protocol is set to 'Radius'.
- User Session:** Idle Timeout (sec) and Session Timeout (sec) are both set to '0'.
- Accounting:** Protocol is set to 'Radius'. 'Stop On Failure' is checked, and 'Stop On Access Deny' is unchecked. Interval (min) is set to '0'. Duplication is set to '-- None --'.
- Address Resolution:** Addressing Scheme is set to 'Local'. 'Duplicate Address Check' is checked.
- Name Servers:** Fields for Primary DNS, Secondary DNS, Primary WINS, and Secondary WINS are present, each with a placeholder of three dots.

At the bottom right, there are 'OK' and 'Cancel' buttons.

Table 3-2 Authentication and accounting parameters

Parameter	Description
Authentication	
Protocol	Currently, the only protocol option available for authentication is RADIUS, a distributed client/server system that protects networks against unauthorized access. Option is set automatically.
User Session	
Idle Timeout (sec)	Maximum number of seconds that a user session can be idle before the system disconnects the user. Range 0 or 300–7200; zero means no limit. Default is 0.
Session Timeout (sec)	Maximum number of seconds that a user session can be established before the system disconnects the user. Range 0 or 60–604800; zero means no limit. Default is 0.
Accounting	
Protocol	Currently, the only protocol option available for accounting is RADIUS. Option is set automatically.
Interval(min)	Specifies the number of minutes between accounting updates. Range is 10–1080. Default is 0. Zero (0) disables.
Stop on Failure	Enables/disables the accounting stop message sent to the accounting server when the authentication server access is denied. Default is disabled.
Stop on Access Deny	Enables/disables the accounting stop message sent to the accounting server when the authentication server grants access, but AAA denies access. Default is disabled.
Duplication	Specifies that duplicate accounting records are to be sent to the accounting server on another virtual router. Click  to select a virtual router from the Associate Virtual Routers dialog box.

2 Set the parameters for address resolution. See Table 3-3.

You can optionally assign IP addresses to Domain Name System (DNS) and Windows Internet Name Service (WINS) name servers.

Table 3-3 Address resolution parameters

Parameter	Description
Addressing Scheme	<ul style="list-style-type: none"> Local – enables the use of a local address pool for address allocations; the default DHCP – DHCP relay server supplies the IP addresses

Table 3-3 Address resolution parameters (continued)

Parameter	Description
Duplicate Address Check	Enables/disables the duplicate IP address checking, which causes the system to check the route table for the PPP user's dynamic IP address provided to PPP from AAA. Default is disabled.
Name Servers	
Primary DNS	IP address of the primary DNS name server
Secondary DNS	IP address of the secondary DNS name server
Primary WINS	IP address of the primary WINS name server
Secondary WINS	IP address of the secondary WINS name server

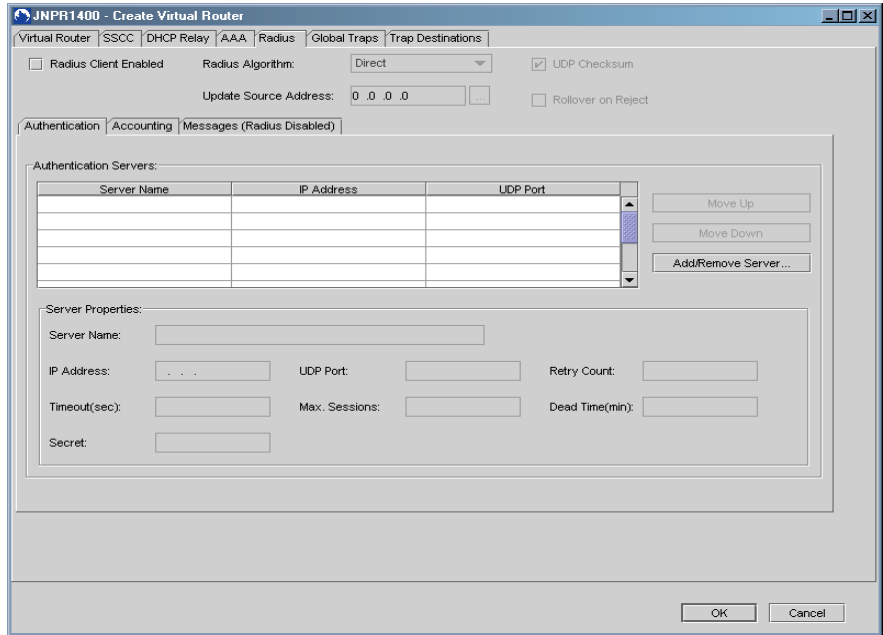
- 3 If you have finished creating the virtual router, click OK. Otherwise, continue to the next tab.

Configuring RADIUS Servers

The Radius tab allows you to set the parameters for RADIUS authentication and accounting servers. It also allows you to associate authentication and accounting servers with the virtual router you are creating.

To configure RADIUS servers:

- 1 Click the Radius tab.
- 2 Set authentication and accounting server parameters. See Table 3-4.



The authentication server determines whether or not a user is allowed access to a specific service or resource. The accounting server tracks service use by subscribers.

Table 3-4 RADIUS authentication and accounting server parameters

Parameter	Description
Radius Algorithm	<ul style="list-style-type: none"> Direct – The first authentication or accounting server that you configure is treated as the primary authentication or accounting server, the next server configured is the secondary, and so on. Round-robin – The first configured server is treated as a primary for the first request, the second configured server as primary for the second request, and so on. When the system reaches the end of the list of servers, it starts again at the top of the list.
Authentication/Accounting Servers	The Radius tab allows you to associate authentication and accounting servers with the virtual router you are creating. See <i>Associating RADIUS Servers with a Virtual Router</i> .
Server Properties	
Server Name	Name associated with this server; up to 32 alphanumeric characters
IP Address	Valid IP address for the server

Table 3-4 RADIUS authentication and accounting server parameters (continued)

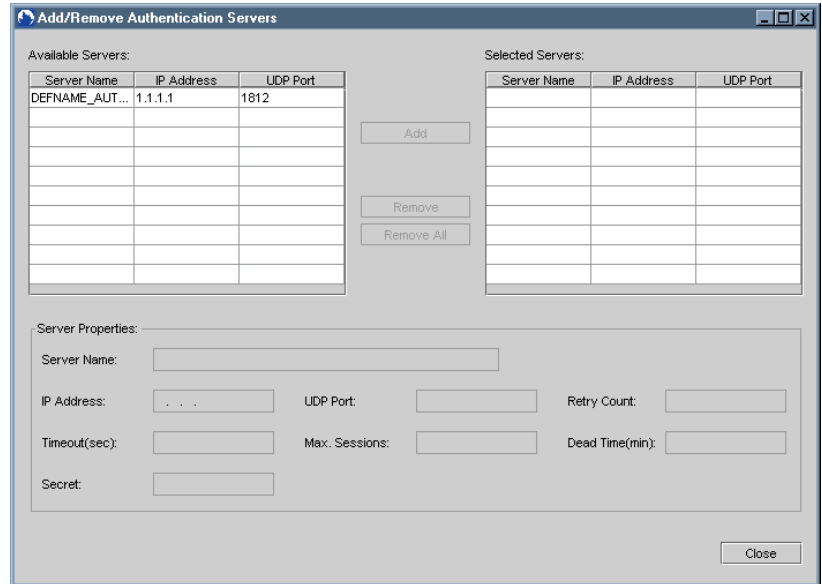
Parameter	Description
UDP Port	Number in the range 0–65536 representing the port where the RADIUS server resides
Retry Count	Number in the range 0–16 representing the number of times the ERX device will attempt to resend a request to the server before sending it to the next server in the list
Timeout (sec)	Number in the range of 3–30 seconds representing the amount of time that will elapse between retry attempts
Max. Sessions	Number in the range 10–4000 representing the outstanding requests that the server can have before it sends any new requests to the next server
Dead Time (min)	Number in minutes in the range 0–30. A server that fails to answer a request is marked unavailable. The dead time is the amount of time that will elapse before another attempt is made to reach that system again.
Secret	Used for encrypting communication between the client and the server. Up to 32 characters. Default is a blank field.

- 3 If you have finished creating the virtual router, click OK. Otherwise, continue to the next tab.

Associating RADIUS Servers with a Virtual Router

To associate an authentication or accounting server with the virtual router:

- 1 On the Authentication or Accounting tab, click Add/Remove Server.
The Add/Remove Authentication/Accounting Servers dialog box appears.



- 2 To associate a server with the virtual router, select the server in the Available Servers list, and click Add.

The server's name appears in the Selected Servers list.



Note: You can associate a maximum of ten authentication and ten accounting servers with a single virtual router.

- 3 In the Server Properties group box, modify the parameters for a specific server if necessary. See Table 3-4.
- 4 Select the server in the Available Servers list.
- 5 Edit the fields in the Server Properties group box.
- 6 When you finish associating the servers you want, click Close.
 The application returns to the Create Virtual Router dialog box.
- 7 If you have finished creating the virtual router, click OK. Otherwise, continue to the next tab.

Moving RADIUS Servers

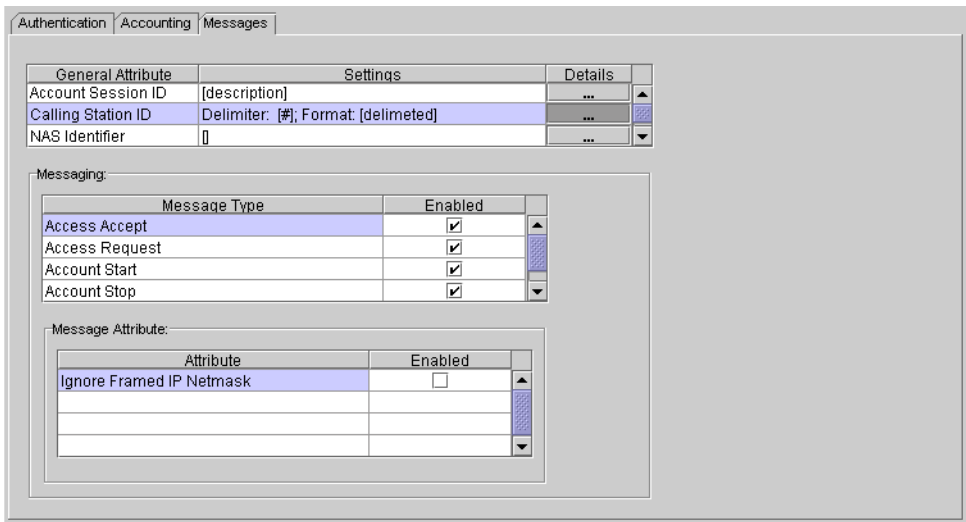
If you have more than one authentication or accounting server in a list, you can rearrange the order of the servers. The order of servers in a list dictates the order in which a virtual router uses the servers.

To move the servers in a list:

- 1 On the Authentication or Accounting server tab, select the server that you want to move.
- 2 Click Move Up or Move Down.
- 3 Click OK.

RADIUS Messages

The Messages tab displays RADIUS attributes that communicate information between the device and the RADIUS server.

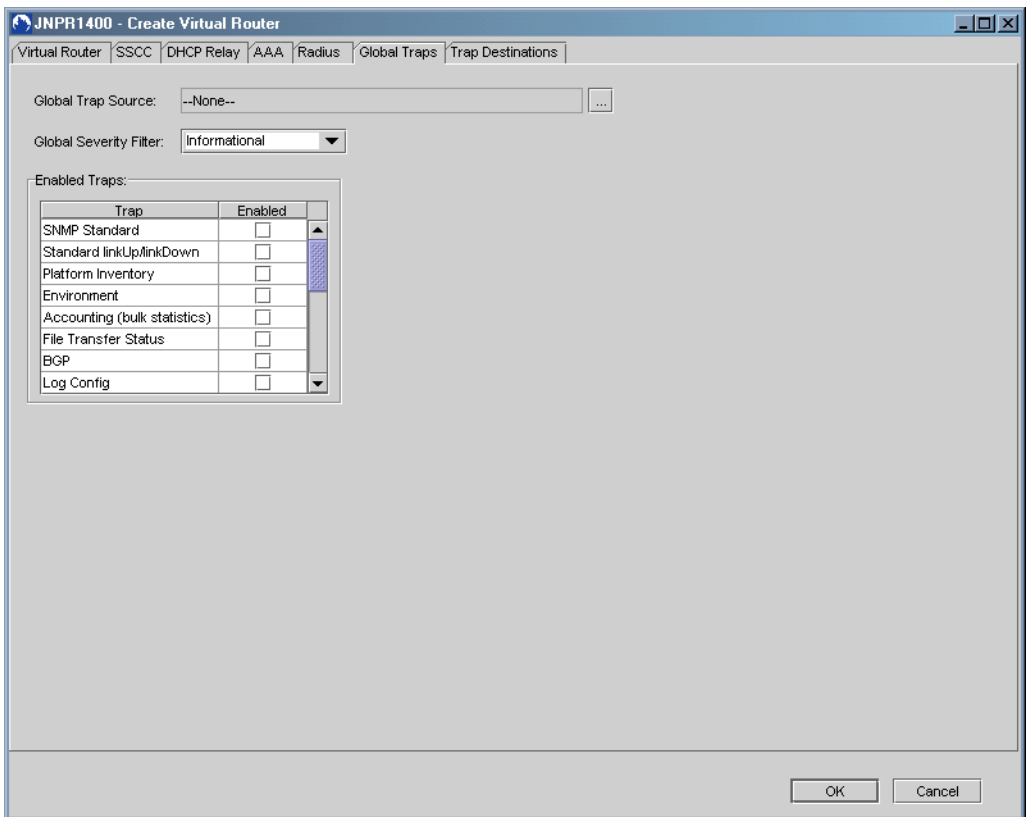


Configuring Global Traps

The Global Traps tab allows you to change parameters for this virtual router. From the Global Traps tab you access the Trap Source Selection dialog box. When an interface is selected, the Global Trap Source text field is populated with the location information for the selected interface. If no interface is selected, –None– is displayed.


To configure Global Traps:

- 1 Click the Global Traps tab.



- 2 Set the global traps parameters. See Table 3-5.

Table 3-5 Global trap parameters

Parameter	Description
Global Trap Source	Interface index of the interface whose IP address is used as the source IP address for outbound SNMP traps. Default is –None–. Click  to select a trap source from the Select Trap Source dialog box. See <i>Related Dialog Boxes</i> .
Global Severity Filter	Defines the global minimum severity level that a trap must have to be forwarded to host-level trap processing. A trap is discarded if its security level is less than the value of this filter. Levels include: <ul style="list-style-type: none"> • Emergency – system unusable • Alert – immediate action needed • Critical – critical conditions exist • Error – error conditions exist • Warning – warning conditions exist • Notice – normal but significant conditions exist • Informational – informational messages (default) • Debug – debug messages
Enabled Traps	Bit mask designating the specific trap types enabled for transmission to this trap destination. Up to 20 traps can be enabled. Default: all bits are selected.

- 3 If you have finished creating the virtual router, click OK. Otherwise, continue to the next tab.

Configuring Trap Destinations

The Trap Destinations tab allows you to associate a trap destination with any ERX device’s virtual router that does not yet have the maximum number of trap destinations associated with it. When you select the device row in the Associate Trap Destinations table, the Device Trap Parameters fields are populated with the values specific to the selected trap destination of this virtual router.

The Add/Remove Destination button launches the Add/Remove Trap Destination dialog box. From this dialog box, you make selections of available trap destinations that you want to associate with the virtual router.

To configure trap destinations:

- 1 Click the Trap Destinations tab. See Table 3-6.

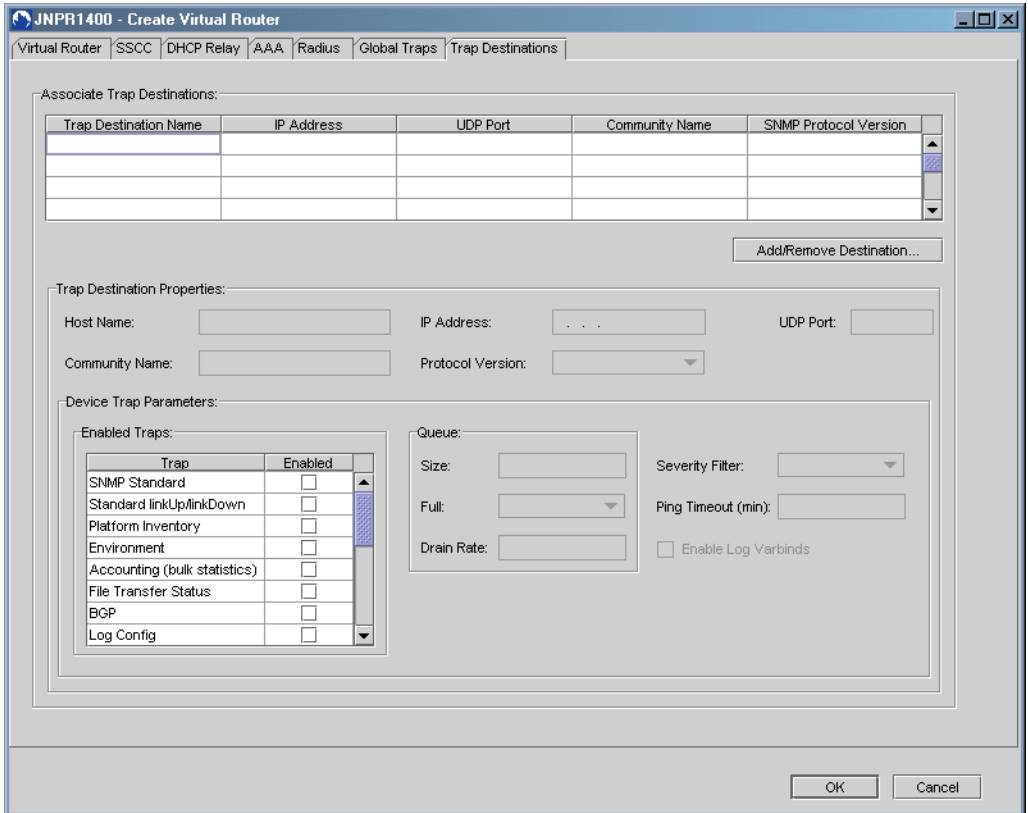


Table 3-6 Trap destination parameters

Field	Description
Associate Trap Destinations	
Trap Destination list	Lists associated trap destinations and associated information (IP Address, UDP Port, Community Name, SNMP Protocol Version)
Add/Remove Destination . . .	Click to access the Add/Remove Device dialog box. From this dialog box you can associate virtual routers with trap destinations. See <i>Related Dialog Boxes</i> .
Trap Destination Properties	
Host Name	Name of trap destination host; not editable
IP Address	IP address of the authorized SNMP trap recipient; not editable
UDP Port	UDP port to which traps will be sent; not editable

Table 3-6 Trap destination parameters (continued)

Field	Description
Community Name	SNMP community name to be used in traps sent to this destination; not editable
Protocol Version	Format of the SNMP trap PDU to be sent to this trap destination; not editable <ul style="list-style-type: none"> • v1 – default; SNMPv1 (defined in RFC 1157) • v2c – SNMPv2c (community-based SNMPv2, defined in RFC 1901 and RFC 1905) • v3 – SNMPv3 (compliant with RFCs 2570–2575)
Device Trap Parameters	
Enabled Traps	Bit mask designating the specific trap types enabled for transmission to this trap destination. Up to 19 traps can be enabled.
Queue	
Size	Maximum number of traps to be kept in the queue; range: 32–2147483647
Severity Filter	Minimum severity value that an SNMP trap must have to be forwarded to this host. A trap is discarded if its security level is less than the value of this filter. Levels include: <ul style="list-style-type: none"> • Emergency – system unusable • Alert – immediate action needed • Critical – critical conditions exist • Error – error conditions exist • Warning – warning conditions exist • Notice – normal but significant conditions exist • Informational – informational messages • Debug – debug messages
Full	Method for handling Queue-Full condition. Options: Drop Last In or Drop First In
Ping Timeout (min)	Number of minutes that this host is pinged repeatedly; range: 0–90
Drain Rate	Maximum number of traps per second to be sent to this host. Value of 0 indicates that there is no control over the drain rate; range: 0–2147483647
Enable Log Varbinds	(Optional) Configures the associated SNMP agent to include notification log name and the corresponding log index as part of the trap messages sent to this host. Options: Enable or Disable

2 Click the Add/Remove Destination button.


The Add/Remove Trap Destinations dialog box appears. See *Related Dialog Boxes* for information on adding or removing trap destinations.

- 3 Select a device from the Associate Trap Destinations list.
 The Trap Destinations Properties fields are populated with the parameters associated with the currently selected device from the table.
- 4 (Optional) Modify the Device Trap Parameters fields. See Table 3-6.
- 5 Click OK.

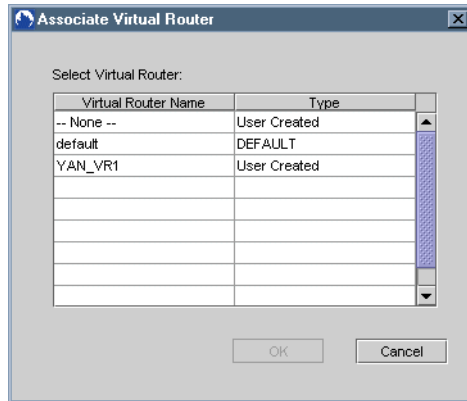
Related Dialog Boxes

Associate Virtual Router

To duplicate accounting records:

- 1 In the AAA tab in the Create Virtual Router dialog box, click  to the right of the Duplication text box.

The Associate Virtual Router dialog box appears.



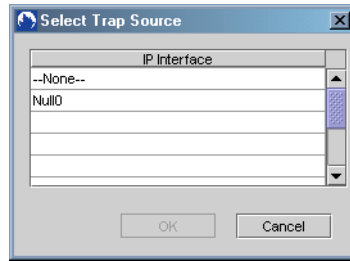
- 2 Select the virtual router you want to receive duplicate accounting records.
- 3 Click OK.

Select Trap Source

To select a trap source:

- 1 In the Global Traps tab, click  to the right of the Global Trap Source text box.

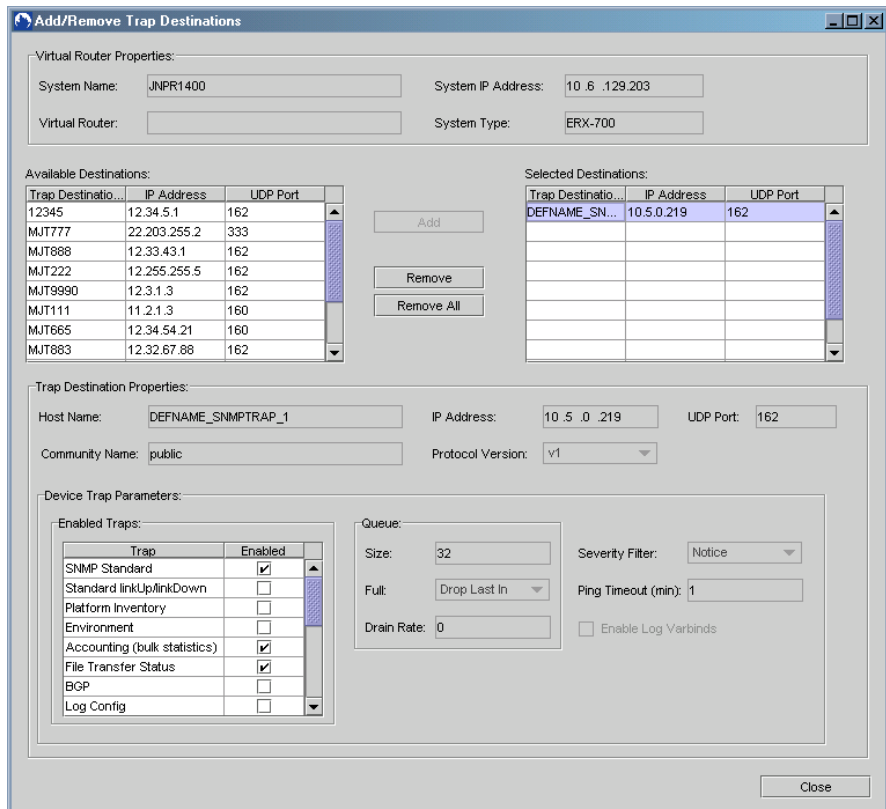
The Select Trap Source dialog box appears.



- 2 Select the IP interface you want to use as the global trap source.
- 3 Click OK.

**Add/Remove
Trap
Destinations**

The Add/Remove Trap Destinations dialog box appears when you select the Add/Remove Destination button on the Trap Destinations tab of the Create Virtual Router dialog box. Use this dialog box to add or remove a trap destination.



To add a trap destination:

- 1 From the Available Destinations table, click an item in the list.
When you select an item in the Selected Destinations table, the values are populated in the Trap Destination Properties fields.
- 2 (Optional) Edit the Device Trap Parameters fields for the trap destination.
- 3 Click Add.
The item is added to the Selected Destinations table.
- 4 Repeat steps 1–3 for each available destination that you want to add.
- 5 Click Close.

To remove a trap destination:

- 1 From the Selected Destinations table, click an item in the list.
- 2 Click Remove.
The destination is removed from the Selected Destinations list.
- 3 Repeat steps 1 and 2 for each destination that you want to remove.
- 4 Click Close.

To remove all destinations:

- 1 Click Remove All.
All destinations are deleted from the Selected Destinations table.
- 2 Click Close.

Creating Management Access

Usually, a system administrator or network specialist determines who is permitted or denied access to certain network management functions. The NMC-RX application uses SNMP to provide security features for the purpose of safeguarding critical network information.

A proprietary SNMP Community Table governs access to an SNMP server by an SNMP client. This table identifies those communities that have different permission levels to the SNMP MIB stored on a particular server. When an SNMP server receives a request, the server extracts the client's IP address and the community name. The SNMP server's

Community Table is searched for a matching community. The server's access list is then used to validate the IP address. Access is determined based on validation of these criteria.

Creating Management Access Entries

After you create a management access entry, you can create access list entries and associate them with the newly created management access entry. The NMC-RX application propagates the access list entry number from the management access entry to the access list. One or more access list entries can be associated with a single management access entry.

To create a management access entry:

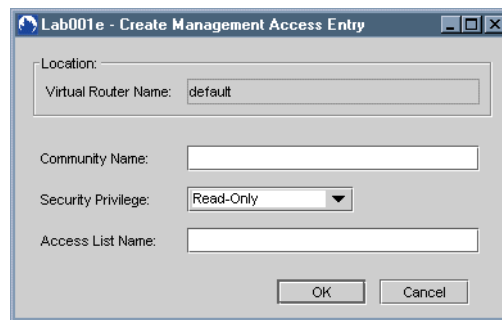
- 1 From the Device-wide Explorer, click Virtual Routers, right-click, and click List All.

The names of all the virtual routers created for this device appear in the list area. This list always includes a default virtual router preconfigured on your ERX device. It also includes any additional virtual routers that you have created.

Virtual Router Name	Type
default	DEFAULT
YAN_VR1	User Created

- 2 Click a virtual router in the list, right-click, select Create, and click Mgmt Access Entry.

The Create Management Access Entry dialog box appears.



- 3 Set the management access entry parameters. See Table 3-7.

Table 3-7 Management access entry parameters

Parameter	Description
Virtual Router Name	Name of the virtual router for which you are creating the management access entry. Name is automatically propagated by the system from the name you previously selected.
Community Name	Name of the SNMP community. A text string of 1–31 characters. Community name acts as a password and is used to authenticate messages sent between an SNMP client and a router containing an SNMP server. Every packet between the client and the server contains the community string.
Security Privilege	Access level assigned to the community name: <ul style="list-style-type: none"> • Read-Only – allows read-only access to the entire MIB except for SNMP configuration objects • Read-Write – allows read-write access to the entire MIB except for SNMP configuration objects • Admin – allows read-write access to the entire MIB
Access List Name	Name identifies the list. The IP access list identifies those IP addresses of SNMP clients permitted to use a given SNMP community.

- 4 Click OK.

The system saves the management access entry.

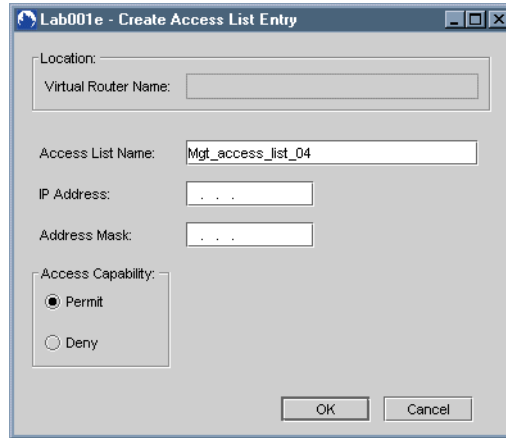
Creating Access List Entries

Before you can create access list entries from the management access entry, you must list the available management access entries. When you create an access list entry for a management access entry, you establish an association.

To create an access list entry:

- 1 From the Device-wide Explorer, open the Virtual Routers folder.
- 2 Click Mgmt Access Entries, right-click, and click List All.
- 3 In the list area, select the management access entry for which you want to create an access list, right-click, select Create, and click Access List Entry.

The Create Access List Entry dialog box appears.



4 Set the access list entry parameters. See Table 3-8.

Table 3-8 Access list entry parameters

Parameter	Description
Access List Name	Name identifies the list. The IP access list identifies those IP addresses of SNMP clients permitted to use a given SNMP community.
IP Address	IP address of the management station communicating through SNMP to a device
Address Mask	IP mask of the management station communicating through SNMP to a device
Access Capability	Access permission: <ul style="list-style-type: none">• Permit – access is allowed• Deny – access is not allowed

5 Click OK.

The new access list entry is created.

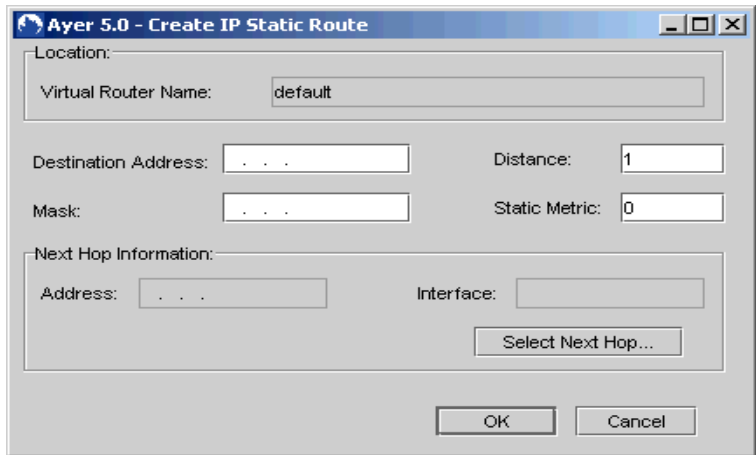
Creating IP Static Routes

You can create IP static routes for your virtual routers. An IP static route allows you to receive and send traffic by assigning a fixed route through the network.

To create an IP static route on a virtual router:

- 1 In the Device-wide Explorer, right-click Virtual Routers, and click List All.
- 2 From the list of virtual routers in the list area, click the router for which you want to configure an IP static route.
- 3 Right-click, select Create, and click IP Static Route.

The Create IP Static Route dialog box appears.



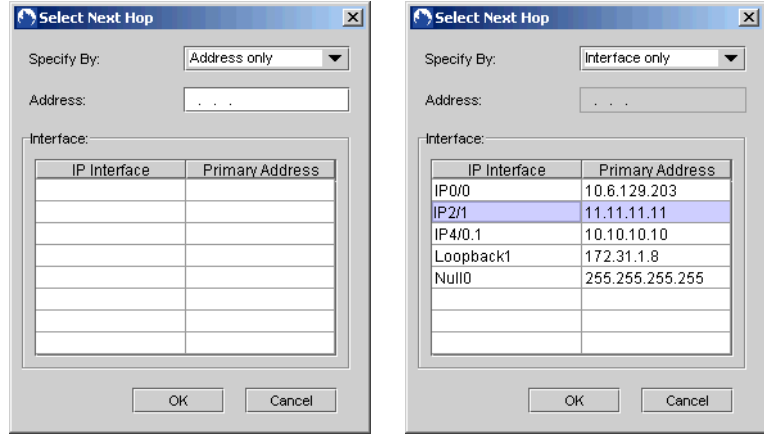
- 4 Set the first four parameters. See Table 3-9.

Table 3-9 IP static route parameters

Parameter	Description
Destination Address	IP address for the device at the other end of the connection from the virtual router
Mask	IP address mask for the destination address
Distance	Administrative distance or weight assigned to the route
Static Metric	Hop count
Next Hop Information	
Address	IP address of the next hop
Interface	Interface of the next hop

- 5 Click Select Next Hop.

The Select Next Hop dialog box appears.



- 6 From the Specify By drop-down list, select how you want to specify the next hop:
 - Address only – Enables the Address field.
 - Interface only – Dims the Address field and displays all IP interfaces defined on the same virtual router as the IP static route.
 - Address and Interface – Enables the Address field and lists unnumbered IP interfaces defined on the same virtual router as the IP static route.
- 7 Depending on your selection, enter an address, select an interface, or do both, and click OK.

Your selections are entered in the corresponding fields in the Create IP Static Route dialog box. If an address does not exist on the virtual router, “Unresolved” appears in the Interface field.
- 8 Click OK to save the settings.