

Chapter 3

Configuring Virtual Routers

This chapter describes how to configure virtual routers and contains the following sections:

- Overview on page 39
- References on page 40
- Configuration Tasks on page 40
- Creating Virtual Routers on page 40
- Configuring Virtual Routers on page 42
- Creating Management Access on page 58
- Creating IP Static Routes on page 61

Overview

The E-series 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)*. Each virtual router has its own separate set of IP interfaces, forwarding table, and instances of routing protocols.

Applications for virtual routers include the creation of individual routers dedicated to wholesale customers, corporate virtual private network (VPN) users, or a specific traffic type. An E-series 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 other routers, the default virtual router gets its IP addresses when interfaces are configured on it.

References

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

- *Associating Customer Profiles with IP Interfaces* in *NMC-RX User Guide, Vol. 1, Chapter 8, Configuring Customer Accounts*
- *Creating IP Interfaces* on page 88—Information about associating IP interfaces with virtual routers
- *Creating User Domain Maps* on page 115—Information about creating user domain map entries on top of virtual routers
- *Creating Local IP Address Pools* on page 118—Information about creating local IP address pools on top of virtual routers
- *Creating Authentication and Accounting Servers* on page 116
- *Creating DHCP Relay Servers* on page 117

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* on page 118.
6. (Optional) Create a user domain map entry. See *Creating User Domain Maps* on page 115.
7. (Optional) Configure trap destinations and global trap parameters. See also *Chapter 1, Configuring SNMP Traps*.

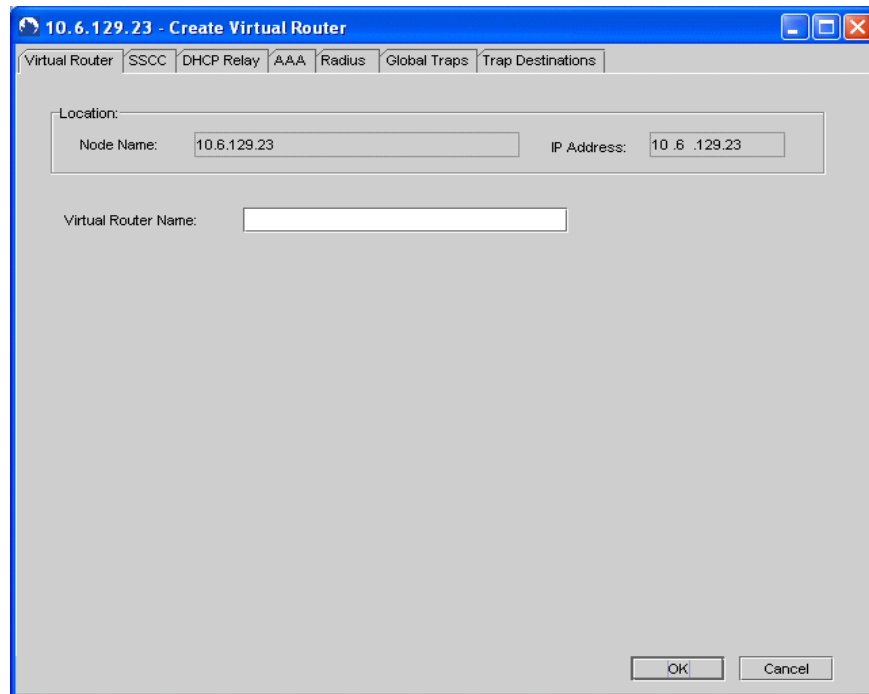
Creating Virtual Routers

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. Depending on which SNMP version of the software you are using, slightly different dialog boxes appear.

SNMPv2c dialog box:

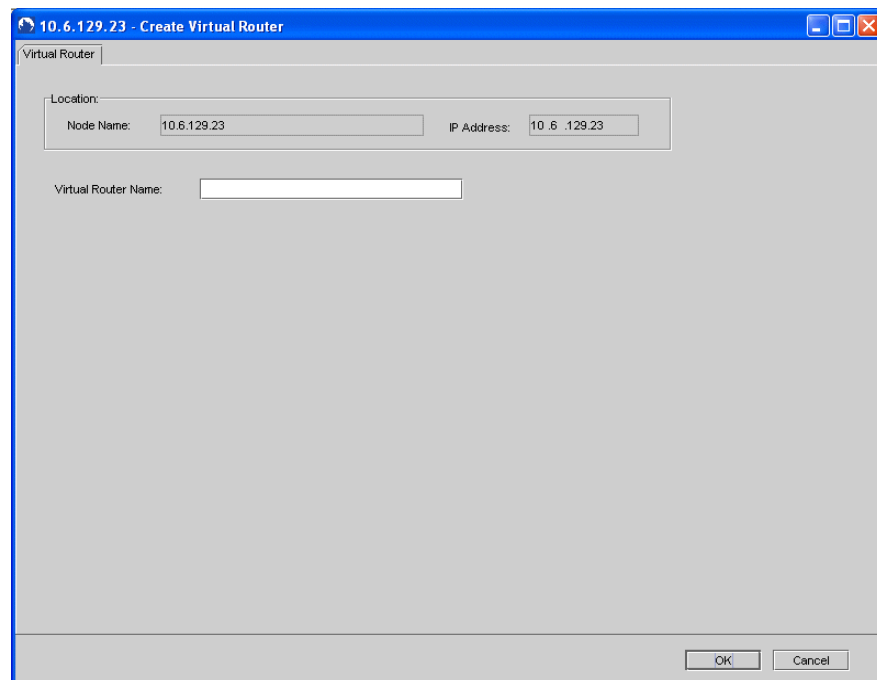


The screenshot shows a dialog box titled "10.6.129.23 - Create Virtual Router". It has a tabbed interface with the following tabs: "Virtual Router", "SSCC", "DHCP Relay", "AAA", "Radius", "Global Traps", and "Trap Destinations". The "Virtual Router" tab is selected. The dialog contains the following fields:

- Location:**
 - Node Name:** 10.6.129.23
 - IP Address:** 10.6.129.23
- Virtual Router Name:** (empty text box)

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

SNMPv3 dialog box:



The screenshot shows the same dialog box as above, but with the "Virtual Router" tab selected. The fields are:

- Location:**
 - Node Name:** 10.6.129.23
 - IP Address:** 10.6.129.23
- Virtual Router Name:** (empty text box)

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

3. Type a name for the virtual router in the Virtual Router Name text box. The name can be up to 15 characters long.

4. *(SNMPv2c version only)* Set the parameters for each tab. See *Configuring Virtual Routers*.
5. Click OK. The virtual router is created.
6. *(SNMPv3 version only)* Using the CLI, configure SNMPv3 users on the newly created virtual router. You will be unable to successfully configure the virtual router using the NMC-RX application until you complete this step.

Configuring Virtual Routers

There are seven general sets of parameters that you can configure on a virtual router. Each set is represented on a tab in the work area:

- 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



NOTE: *(SNMPv3 version only)* Before the NMC-RX application can begin to communicate with the router, SNMPv3 parameters must be set on the router by using the CLI. Use the NMC-RX application's remote login feature to access the CLI.

To configure a virtual router:

1. In the Device-wide Explorer, click Virtual Routers.
2. Right-click and click List All.

All virtual routers are displayed in the list area.

3. In the list area, select the virtual router you want to configure, right-click, and click Configure.

The virtual router appears in the work area.

4. Set the parameters for each tab in the work area. See the following sections for information.

- When you have finished setting the parameters, click Save to save the new settings.

Configuring the SDX Client

The E-series device has an embedded client that interacts with the Service Deployment System (SDX). 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. You can also identify SNMP community strings, which permits a communication exchange between the SDX and NMC-RX applications.

To configure the SDX client parameters:

- Click the SSCC tab.

The screenshot shows the 'ERX-700 - Create Virtual Router' window with the 'SSCC' tab selected. The 'SSCC Client Enabled' checkbox is unchecked. The 'Primary Address' field is set to '0.0.0.0', 'Secondary Address' is '0.0.0.0', and 'Tertiary Address' is '0.0.0.0'. The 'Primary Port', 'Secondary Port', and 'Tertiary Port' fields are all set to '0'. The 'Switchover Timeout (sec.)' field is set to '5'. The 'SNMP Community Strings' section has two empty text boxes for 'Read Only' and 'Read Write'. The 'OK' and 'Cancel' buttons are at the bottom right.

- Set the parameters (Table 18).

Table 18: SDX Client Parameters

Parameter	Description
SSCC Client Enabled	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)

Table 18: SDX Client Parameters (continued)

Parameter	Description
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.
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

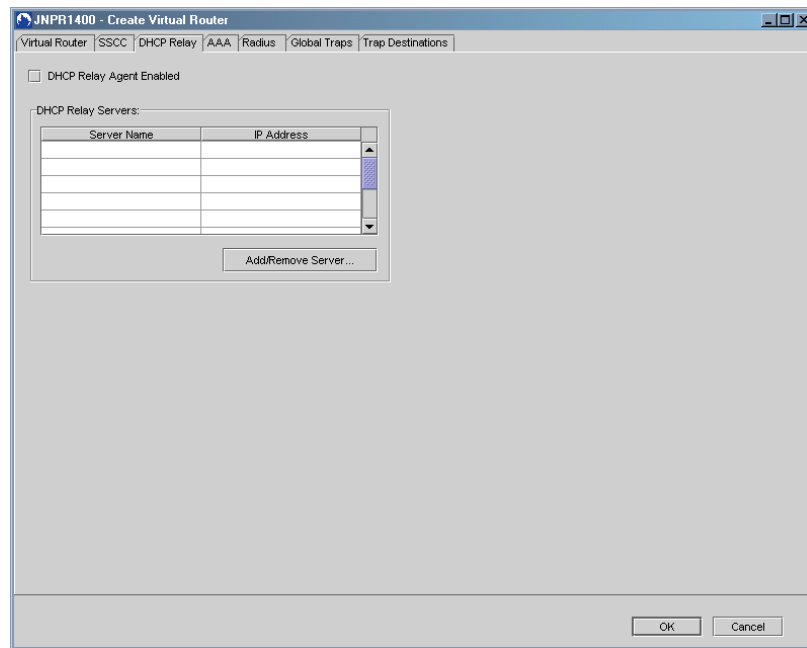
3. If you have finished configuring the virtual router, click Save. Otherwise, continue to the next tab.

Associating DHCP Relay Servers

The DHCP Relay tab allows you to associate DHCP relay servers with the virtual router you are creating on an E-series 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.

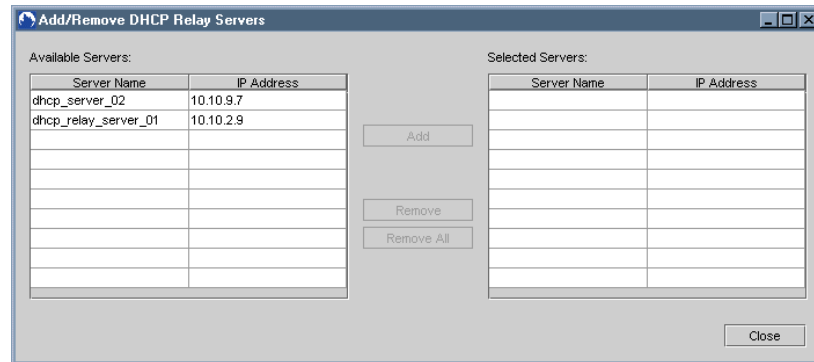


2. To enable the DHCP Relay Agent, select the check box.

When you enable the agent, the E-series 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 configuring the virtual router, click Save. Otherwise, continue to the next tab.

Configuring AAA

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

To configure AAA:


1. Set the parameters for authentication and accounting (Table 19).

The screenshot shows the 'JNPR1400 - Create Virtual Router' dialog box with the 'AAA' tab selected. The 'Authentication' section has 'Protocol' set to 'Radius'. The 'User Session' section has 'Idle Timeout (sec)' and 'Session Timeout (sec)' both set to '0'. The 'Accounting' section has 'Protocol' set to 'Radius', 'Interval(min)' set to '0', and 'Duplication' set to '-- None --'. The 'Stop On Failure' checkbox is checked, and 'Stop On Access Deny' is unchecked. The 'Address Resolution' section has 'Addressing Scheme' set to 'Local' and 'Duplicate Address Check' checked. The 'Name Servers' section has four empty input fields for Primary DNS, Secondary DNS, Primary WINS, and Secondary WINS. 'OK' and 'Cancel' buttons are at the bottom right.

Table 19: 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 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 0.
Accounting	
Protocol	Currently, the only protocol option available for accounting is RADIUS. Option is set automatically.

Table 19: Authentication and Accounting Parameters (continued)

Parameter	Description
Interval(min)	Specifies the number of minutes between accounting updates. Range 10–1080; default 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: 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: 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 (Table 20).

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

Table 20: 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 ■ DHCP—DHCP relay server supplies the IP addresses
Duplicate Address Check	Enables/disables the duplicate IP address checking, which causes the system to check the routing table for the PPP user's dynamic IP address provided to PPP from AAA; default: 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

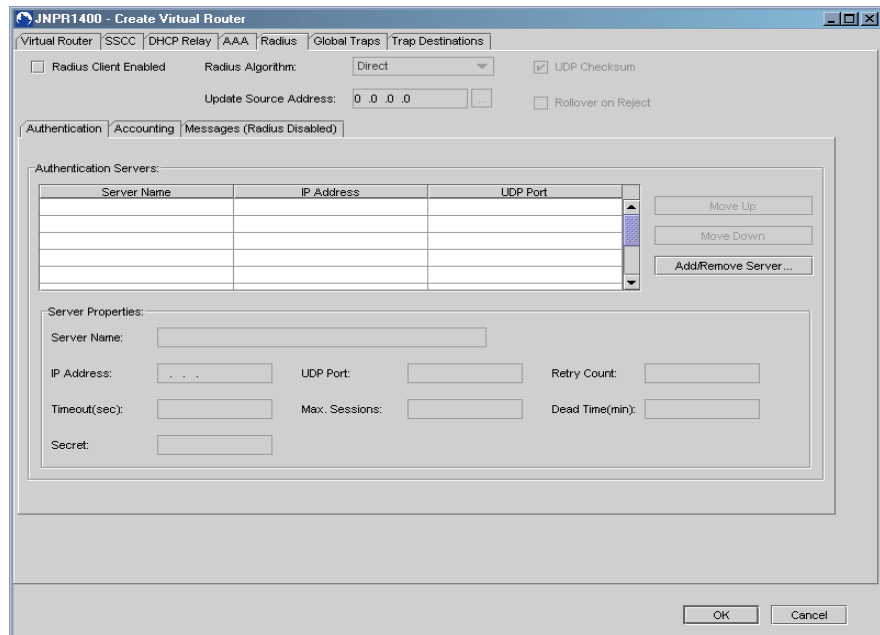
3. If you have finished configuring the virtual router, click Save. Otherwise, continue to the next tab.

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. 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.

To configure RADIUS servers:

1. Click the Radius tab.
2. Set authentication and accounting server parameters (Table 21).

**Table 21: 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> on page 50.
Server Properties	
Server Name	Name associated with this server; up to 32 alphanumeric characters
IP Address	Valid IP address for the server
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 E-series 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

Table 21: RADIUS Authentication and Accounting Server Parameters (continued)

Parameter	Description
Dead Time (min)	Amount of time that will elapse before another attempt is made to reach that system. A server that fails to answer a request is marked unavailable; range 0–30 minutes.
Secret	Used for encrypting communication between the client and the server. Up to 32 characters. Default: blank.

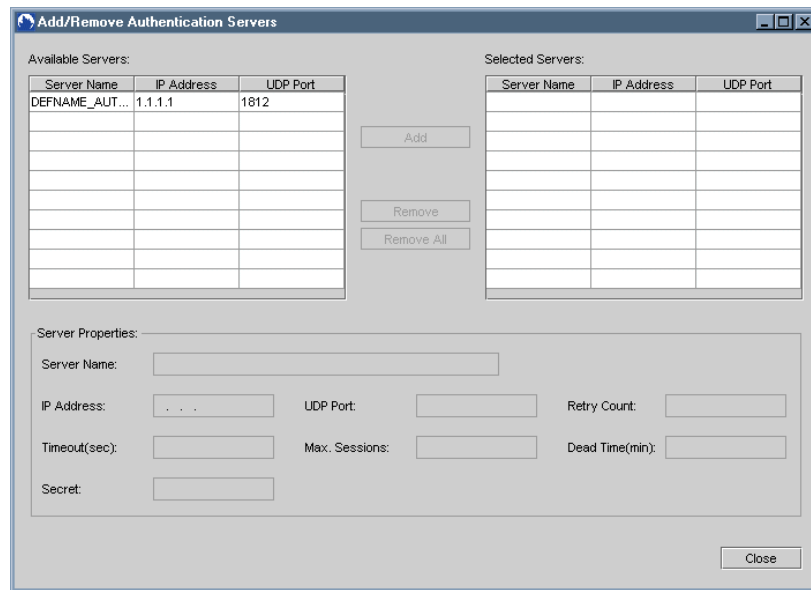
- If you have finished configuring the virtual router, click Save. Otherwise, continue to the next tab.

Associating RADIUS Servers with a Virtual Router

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

- On the Authentication or Accounting tab, click Add/Remove Server.

The Add/Remove Authentication or Accounting Servers dialog box appears.



- 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.

- In the Server Properties group box, modify the parameters for a specific server if necessary (Table 21).

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 configuring the virtual router, click Save. 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

On the Create Virtual Routers tab, the Messages tab displays RADIUS attributes that communicate information between the device and the RADIUS server.

The screenshot shows the 'Messages' tab of a configuration window. It features three tabs: 'Authentication', 'Accounting', and 'Messages'. The 'Messages' tab is selected. The window contains the following sections:

General Attribute	Settings	Details
Account Session ID	[description]	...
Calling Station ID	Delimiter: [#]; Format: [delimited]	...
NAS Identifier	[]	...

Messaging:

Message Type	Enabled
Access Accept	<input checked="" type="checkbox"/>
Access Request	<input checked="" type="checkbox"/>
Account Start	<input checked="" type="checkbox"/>
Account Stop	<input checked="" type="checkbox"/>

Message Attribute:

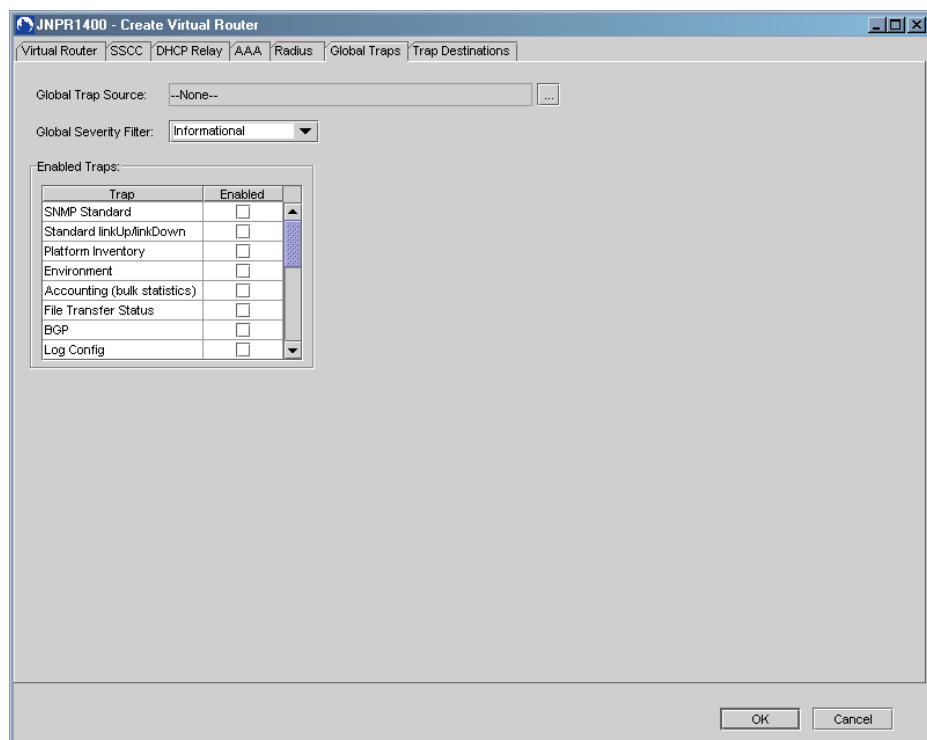
Attribute	Enabled
Ignore Framed IP Netmask	<input type="checkbox"/>

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 (Table 22).

Table 22: 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> on page 56.

Table 22: Global Trap Parameters (continued)

Parameter	Description
Global Severity Filter	<p>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.</p> <p>Levels include:</p> <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	<p>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.</p>

3. If you have finished configuring the virtual router, click Save. Otherwise, continue to the next tab.

Configuring Trap Destinations

The Trap Destinations tab allows you to associate a trap destination with any E-series 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 starts 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.
2. Set the Trap Destinations parameters (Table 23).

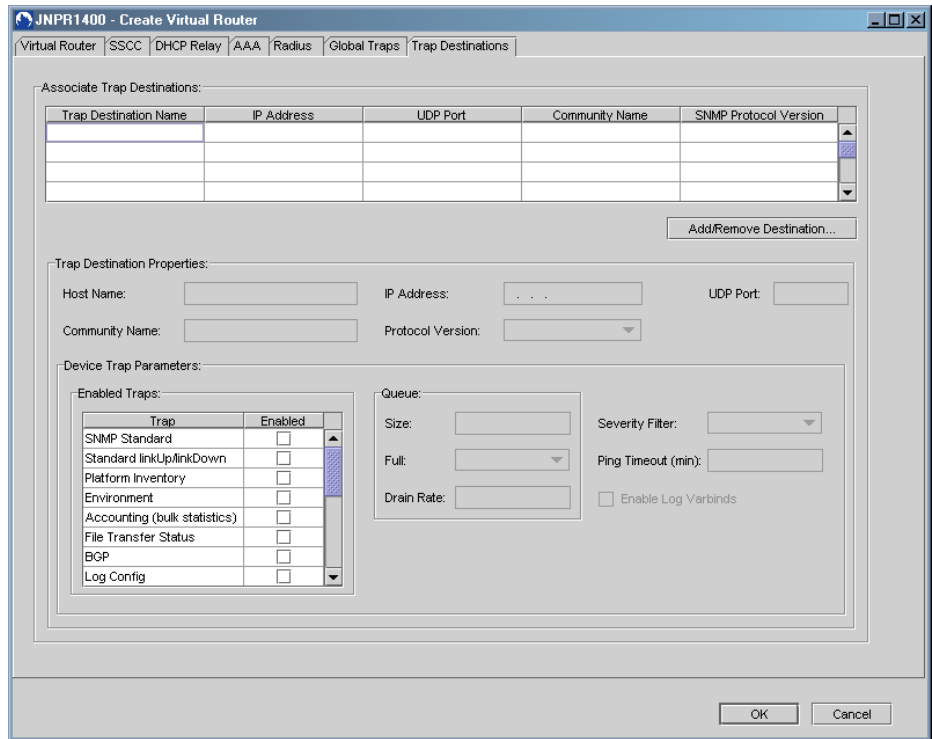


Table 23: Trap Destination Parameters (Create Virtual Router)

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> on page 56.
Trap Destination Properties	
Host Name	Name of trap destination host; cannot edit
IP Address	IP address of the authorized SNMP trap recipient; cannot edit
UDP Port	UDP port to which traps will be sent; cannot edit
Community Name	SNMP community name to be used in traps sent to this destination; cannot edit
Protocol Version	Format of the SNMP trap PDU to be sent to this trap destination; cannot edit <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)

Table 23: Trap Destination Parameters (Create Virtual Router) (continued)

Field	Description
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 ■ Information—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

3. Click the Add/Remove Destination button.

The Add/Remove Trap Destinations dialog box appears. See *Related Dialog Boxes* on page 56 for information about adding or removing trap destinations.


4. 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.

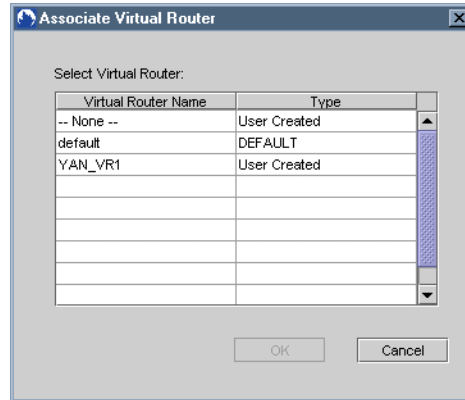
5. (Optional) Modify the Device Trap Parameters fields. (See Table 23.)
6. Click OK.

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.

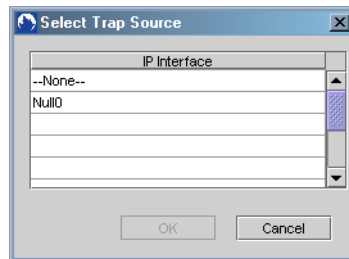


2. Select the virtual router that you want to receive duplicate accounting records.
3. Click OK.

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.

Virtual Router Properties:

System Name: JNPR1400 System IP Address: 10.6.129.203
 Virtual Router: System Type: ERX-700

Available Destinations:

Trap Destination	IP Address	UDP Port
12345	12.34.5.1	162
MJT777	22.203.255.2	333
MJT888	12.33.43.1	162
MJT222	12.255.255.5	162
MJT9990	12.3.1.3	162
MJT111	11.2.1.3	160
MJT665	12.34.54.21	160
MJT883	12.32.67.88	162

Selected Destinations:

Trap Destination	IP Address	UDP Port
DEFNAME_SN...	10.5.0.219	162

Trap Destination Properties:

Host Name: DEFNAME_SNMPTRAP_1 IP Address: 10.5.0.219 UDP Port: 162
 Community Name: public Protocol Version: v1

Device Trap Parameters:

Enabled Traps:

Trap	Enabled
SNMP Standard	<input checked="" type="checkbox"/>
Standard linkUp/linkDown	<input type="checkbox"/>
Platform Inventory	<input type="checkbox"/>
Environment	<input type="checkbox"/>
Accounting (bulk statistics)	<input checked="" type="checkbox"/>
File Transfer Status	<input checked="" type="checkbox"/>
BGP	<input type="checkbox"/>
Log Config	<input type="checkbox"/>

Queue:
 Size: 32 Severity Filter: Notice
 Full: Drop Last In Ping Timeout (min): 1
 Drain Rate: 0 Enable Log Varbinds

Buttons: Add, Remove, Remove All, Close

To add a trap destination:

1. From the Available Destinations table, click an item in the list.
2. (Optional) Edit the Device Trap Parameters fields for the trap destination. See Table 23.
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.

When you select an item in the Selected Destinations table, the values are populated in the Trap Destination Properties fields.

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 by 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:

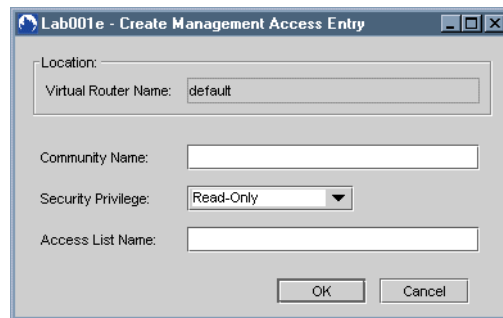
1. From the Device-wide Explorer, click Virtual Routers, right-click, and click List All.

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 E-series device. It also includes any additional virtual routers that you have created.

Virtual Router Name	Type
default	DEFAULT
YAN_VR1	User Created

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

The Create Management Access Entry dialog box appears.



- Set the management access entry parameters (Table 24).

Table 24: 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.

- 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 (Table 25).

Table 25: 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.

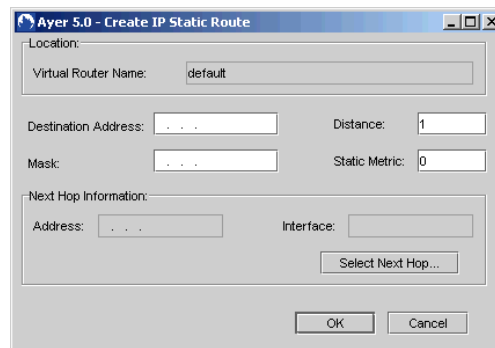
Creating IP Static Routes

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.



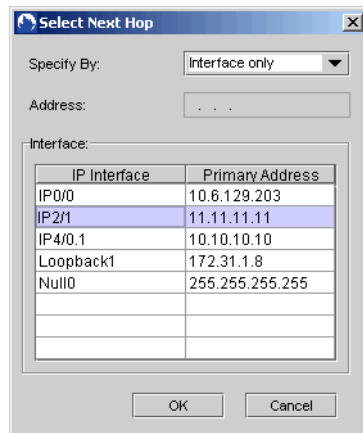
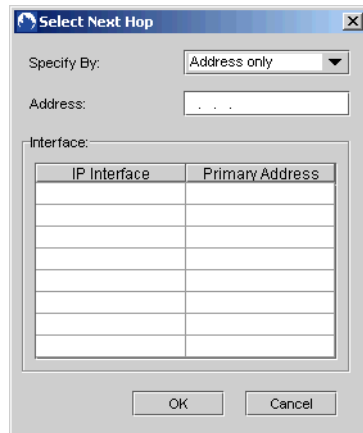
4. Set the first four parameters (Table 26).

Table 26: 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.

