

Chapter 12

Using Device Utilities

You can open a remote login session, execute a ping command, and initiate a traceroute on a selected E-series device by using the NMC-RX device utilities. Each utility is available in the Tools menu or on the pop-up menu of a selected device.

| Topic | Page |
|---|------|
| Overview | 187 |
| Using Remote Login | 188 |
| Using Ping | 190 |
| Using Traceroute | 196 |
| Using the Config Save and Restore Utilities | 200 |

Overview

The NMC-RX device utilities are a group of common utilities that include:

Config Save and Restore – Enables you to save, restore, and delete configuration files on a device.

Remote Login – Enables you to log in to a remote system and use resources as if they were connected to your local system. Either Telnet or SSH can be used for remote terminal connections. Telnet is a standard terminal emulation protocol in the TCP/IP protocol stack. Secure Shell Server (SSH) protocol version 2 is supported as a secure alternative to Telnet.

Ping – Enables you to send an Internet Control Message Protocol (ICMP) echo request packet to an IP address that you specify.

Traceroute – Traces the path a packet takes to a destination. A list of hosts that receive probe packets as they travel to the destination host is displayed in the order that the receiving hosts receive the packets. Traceroute is mostly used to debug routing problems between hosts.

Both ping and traceroute commands can originate in two ways:

From the NMC-RX host platform to a specified device address (default setting)

From a specified device to an IP address

Table 59: NMC-RX device utilities

| Used to Determine | Remote Login | Ping | Traceroute |
|---|--------------|------|------------|
| Network connectivity (whether an address is considered valid) | x | x | x |
| Operational status of a destination host | x | x | x |
| Network loading and speed (how long it takes the replies to return) | | x | x |
| Network errors (percentage of packets that are lost) | | x | x |
| Path a packet takes to a destination | | x | x |

Using Remote Login

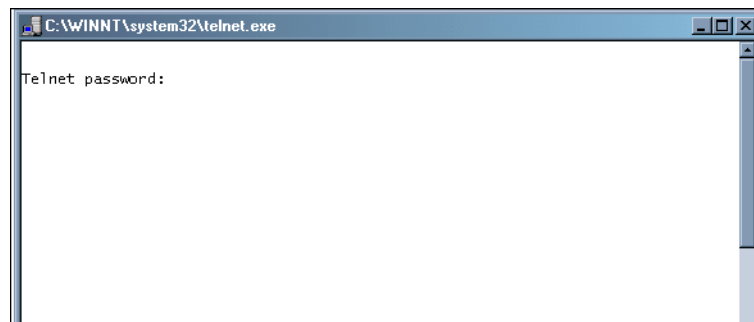
The NMC-RX administrator can configure the remote login to be Telnet or SSH, which is described in *NMC-RX User Guide, Vol. 1, Chapter 8, NMC-RX Security*. Once the remote login is configured, you can start Telnet or SSH either from the Network Workshop or Device Workshop.

To automatically connect to a device:

From the Network Workshop – Select the device, right-click, and select Remote Login.

From the Device Workshop – Select the System folder, right-click, and select Remote Login.

The remote login window appears, and you are connected to the selected device. An example of a Telnet session is shown.



To connect to a device from the Tools menu from either the Network or Device Workshop:

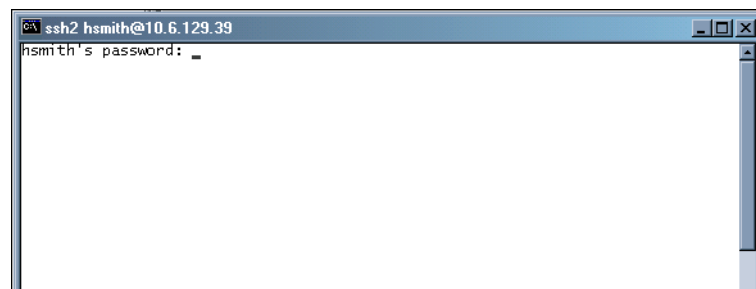
- SSH Login Example**
1. From the Tools menu, select Device Utilities, and click Remote Login.

The SSH Session dialog box appears.



2. Type the IP address of the device to which you want to connect.
3. Click OK.

The SSH login window appears.

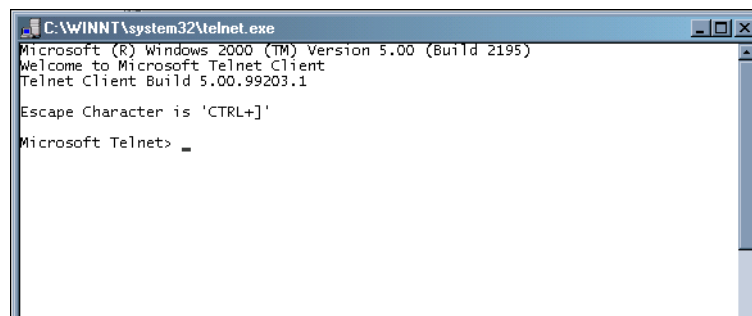


4. Enter your password.

You are logged into the system.

- Telnet Login Example**
1. From the Tools menu, select Device Utilities, and click Remote Login.

The Telnet login window appears.



2. Type the word "open" and the IP address of the device to which you want to connect. For example:

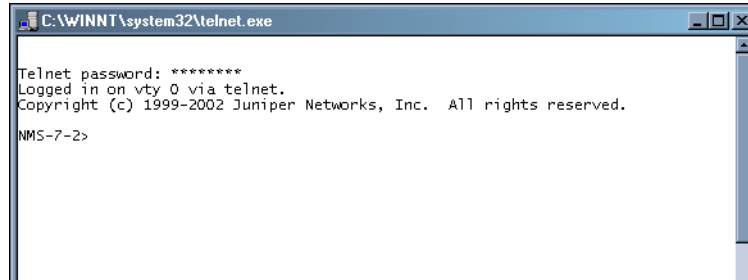
open 10.6.129.39



NOTE: Step 2 may be slightly different depending on the version of Windows you are running.

3. Press < Enter> .

You are prompted for your Telnet password.



4. Type your Telnet password and press < Enter> .

You are logged into the system.

Using Ping

Ping can be used to test the connection status between two devices. You can ping using the basic default settings, or you can set advanced settings to provide more detailed information.

There are three ways to launch the Ping utility:

From the Tools menu – Select Device Utilities, and click Ping. You must then manually enter the IP address.

From the Network Workshop – Select the device, right-click, and click Ping. The IP address of the selected device is automatically entered in the Address field.

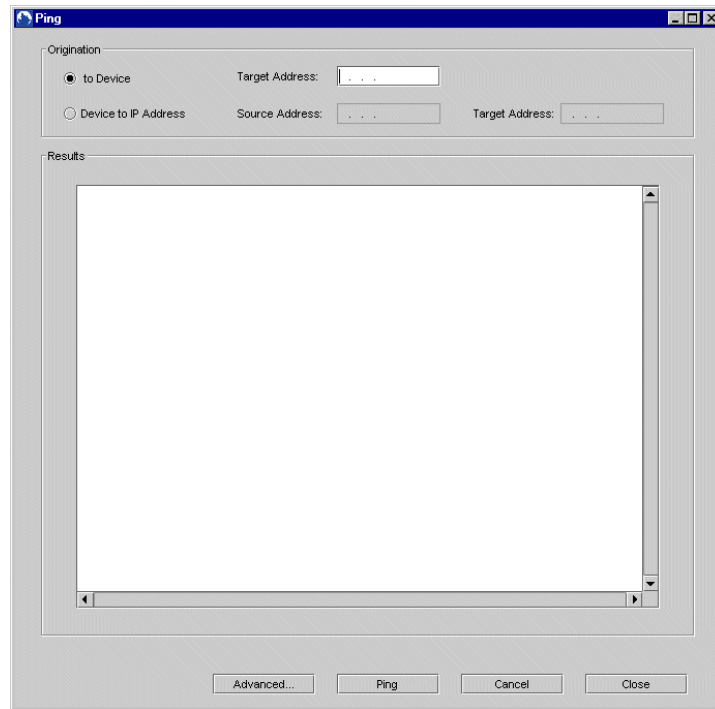
From the Device Workshop – Select the System folder, right-click, and click Ping. The IP address of the selected device is automatically entered in the Address field.

Using Basic Ping Settings

To ping an IP address using basic settings:

1. Launch the Ping utility by using one of the methods described above.

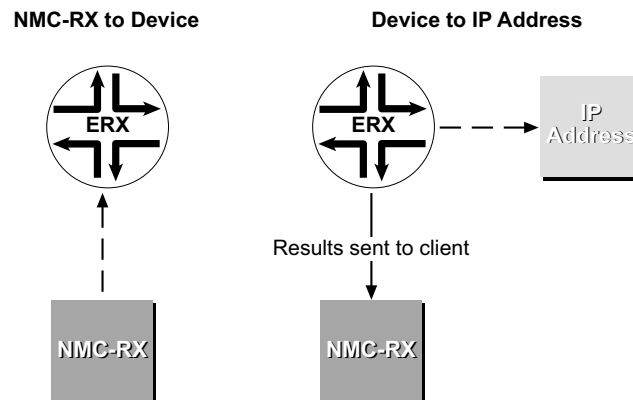
The Ping dialog box appears.



2. Select the Origination point:

To Device – Initiates ping from the computer containing the NMC-RX software you are using to a device. Similar to using the ping command in a DOS window.

Device to IP Address – Initiates ping from an E-series router to another IP address.



3. Enter the target address and source address (if applicable).
4. Click Ping.

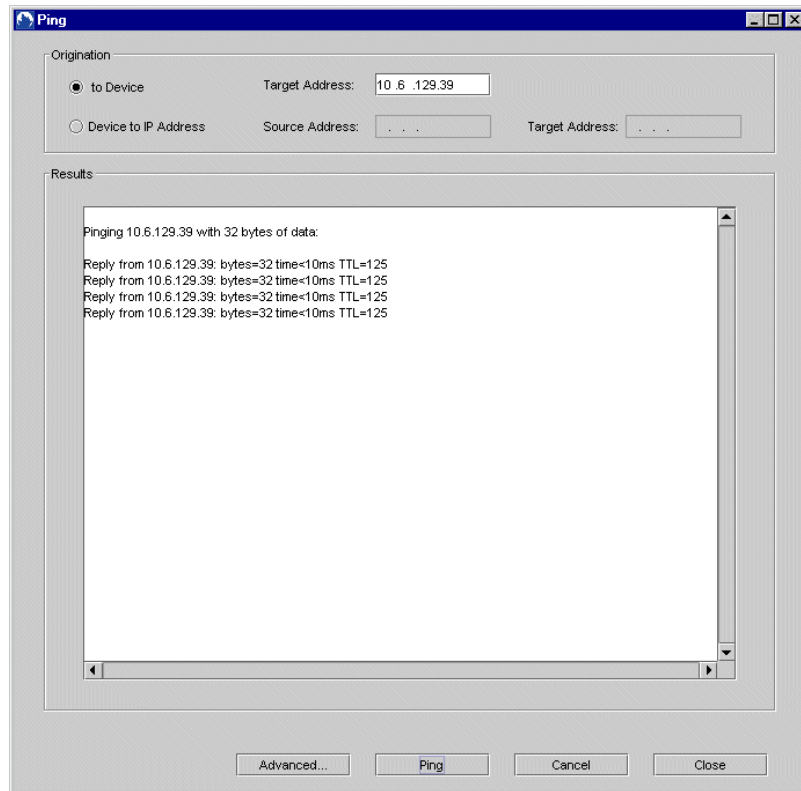
The results appear in the dialog box.



NOTE: Depending on the origin selected, different results appear.



NOTE: Clicking Ping again clears the previous results, executes the command, and displays the new results.



Using Advanced Ping Settings

To ping an IP address using advanced settings:

1. Perform steps 1–3 in the previous section.
2. Click Advanced.

Depending on the Origination type selected, one of the following Advanced Ping Options dialog boxes appears.

Figure 4: NMC-RX to device advanced ping options (Windows)

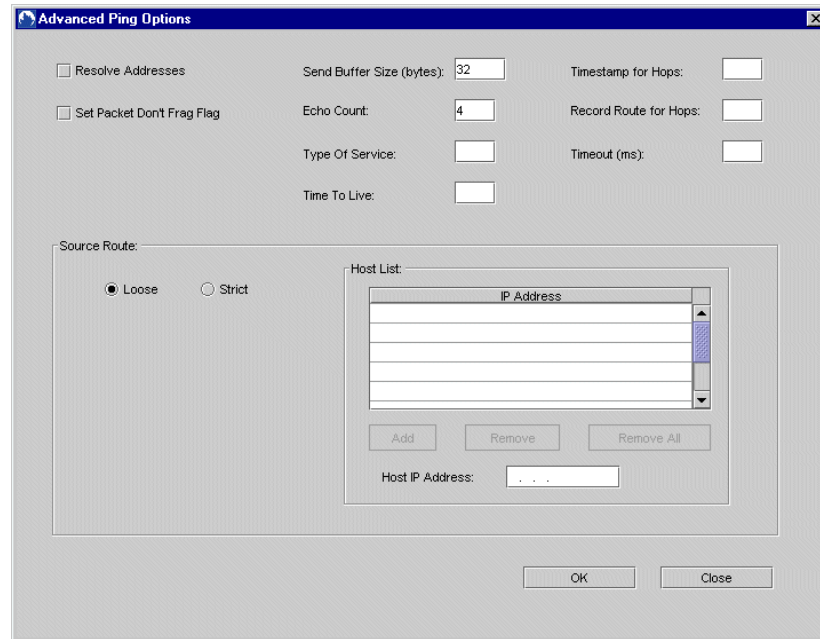
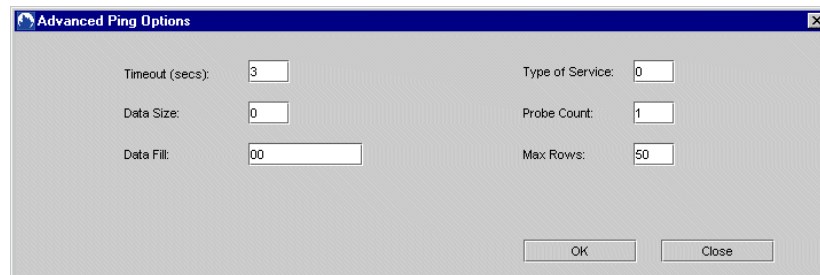


Figure 5: Device to IP address advanced ping options (Windows)



3. Set the Advanced Ping options. See Table 60 or Table 61.

NMC-RX to Device Options

Table 60: NMC-RX to device advanced ping parameters

| Parameters | Description |
|----------------------------|---|
| Resolve Addresses | Select to resolve addresses to host names. |
| Set Packet Don't Frag Flag | Select to send a Do Not Fragment flag in the packet. The packet will not be fragmented by gateways on the route. Use in conjunction with Send Buffer Size option. |
| Send Buffer Size (bytes) | Used to increase or decrease the size of the ICMP packets sent in the ping request Minimum: 0 Maximum: 65500 |

Table 60: NMC-RX to device advanced ping parameters (continued)

| Parameters | Description |
|------------------------|--|
| Echo Count | Sends Echo packets specified by count. For example, if the Echo Count is four, four pings will be sent. Default: 4 |
| Type of Service | Sets the ToS value in the ICMP packet for routers that are set up to treat packets with certain types of service differently than others. ToS is not used very often, and most routers ignore it. |
| Time to Live | Sets the number of hops (routers) that the ping request can traverse before it is discarded. The TTL field in the packet is decremented by one each time it passes through a router. When the number reaches zero, the router discards the packet and sends a TTL Expired ICMP message back. |
| Timestamp for Hops | Specifies the timestamp for the number of hops Minimum: 1 Maximum: 4 |
| Record Route for Hops | Records the route of the outgoing packet and the returning packet in the record route field Minimum: 1 Maximum: 9 |
| Timeout (ms) | Time ping waits for each reply. NMC-RX to Device uses milliseconds (ms) Device to IP Address uses seconds (sec) |
| Source Route Loose | Identifies certain milestone routers that must be used in route to the destination address. However, any path can be used to get to these milestone routers. When selected, routes packets via the hosts specified in the host list Consecutive hosts can be separated by intermediate gateways (loose source routed). Maximum allowed by IP is 9 |
| Source Route Strict | Describes a complete path that must be followed to a destination When selected, routes packets via the hosts specified in the host list Consecutive hosts cannot be separated by intermediate gateways (strict source routed). Maximum allowed by IP is 9 |

Device to IP Address Options

Table 61: Device to IP address advanced ping parameters

| Parameters | Description |
|----------------|--|
| Timeout (secs) | Time ping waits for each reply in seconds |
| Data Size | Specifies the size of the ICMP payload |
| Data Fill | Specifies the contents of the ICMP payload |

Table 61: Device to IP address advanced ping parameters (continued)

| Parameters | Description |
|-----------------|---|
| Type of Service | Sets the ToS value in the ICMP packet for routers that are set up to treat packets with certain types of service differently than others. ToS is not used very often, and most routers ignore it. |
| Probe Count | Number of ICMP packets to send |
| Max Rows | Number of rows displayed |

- (Optional) Enter a host IP address (NMC-RX to Device origination only), and click Add.

The address is added to the IP Address list.

- Click OK to close the Advanced Ping dialog box.
- Click Ping.

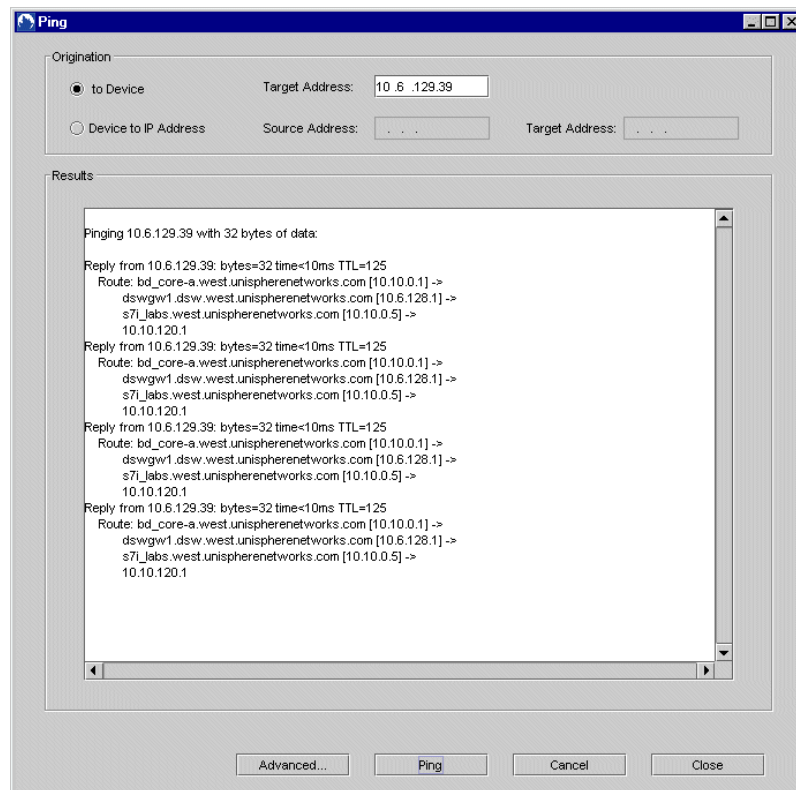
The results appear in the dialog box.



NOTE: Depending on the origin selected, different results appear.



NOTE: Clicking Ping again clears the previous results, executes the command, and displays the new results.



Using Traceroute

Traceroute can be used to discover the paths that router packets follow when travelling to their destinations. There are three ways to launch the Traceroute utility:

From the Tools menu – Select Device Utilities, and click Traceroute. You must then manually enter the IP address.

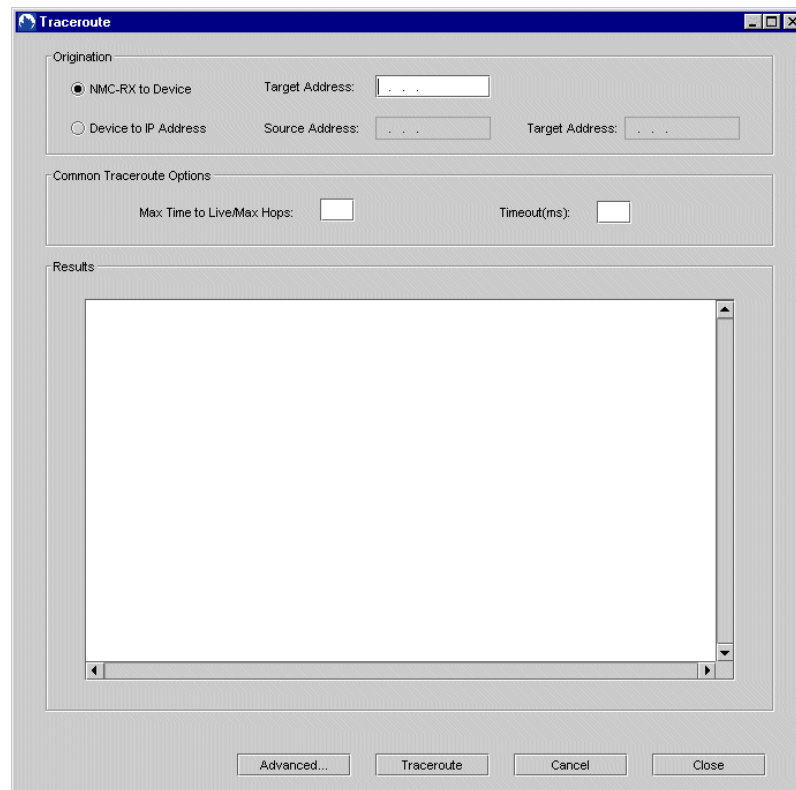
From the Network Workshop – Select the device, right-click, and click Traceroute. The IP address of the selected device is automatically entered in the Address field.

From the Device Workshop – Select the System folder, right-click, and click Traceroute. The IP address of the selected device is automatically entered in the Address field.

Using Basic Traceroute Settings

To check a device traceroute by using basic settings:

1. Launch the Traceroute utility by using one of the methods described above. The Traceroute dialog box appears.



2. Select the Origination method (see descriptions in Ping section):
 - NMC-RX to Device
 - Device to IP Address
3. Enter the target address and source address (if applicable).
4. Enter Common Traceroute Options. See Table 62.

Table 62: Traceroute parameters

| Parameter | Description |
|---------------------------|---|
| Max Time to Live/Max Hops | Maximum number of hops to search for target |
| Timeout | Time traceroute waits for each reply: NMC-RX to Device uses milliseconds (ms) Device to IP Address uses seconds (sec) |

5. Click Traceroute.

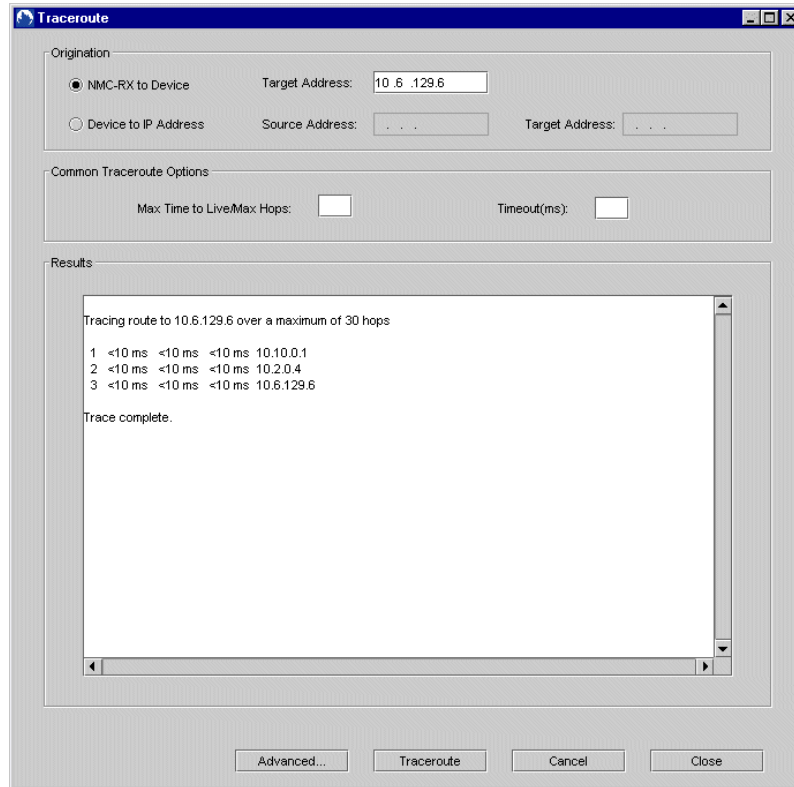
The results appear in the dialog box.



NOTE: Depending on the origin selected, different results appear.



NOTE: Clicking Ping again clears the previous results, executes the command, and displays the new results.



Using Advanced Traceroute Settings

To check a device traceroute using advanced settings:

1. Perform steps 1–4 in the previous section.
2. Click Advanced.

Depending on the Origination type selected, one of the following Advanced Traceroute Options dialog boxes appears.

Figure 6: NMC-RX to device advanced traceroute options (Windows)

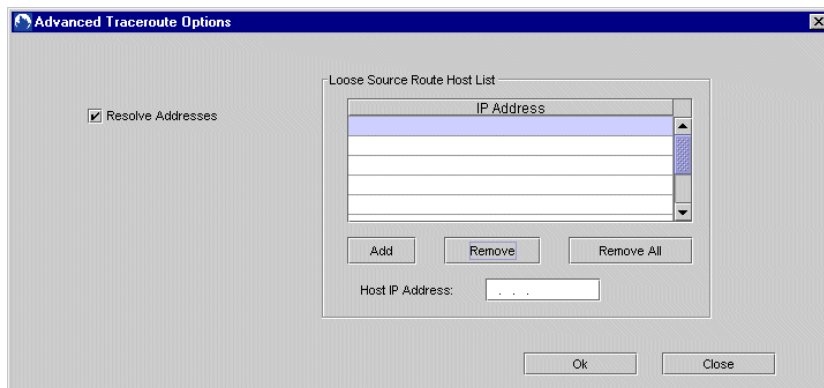
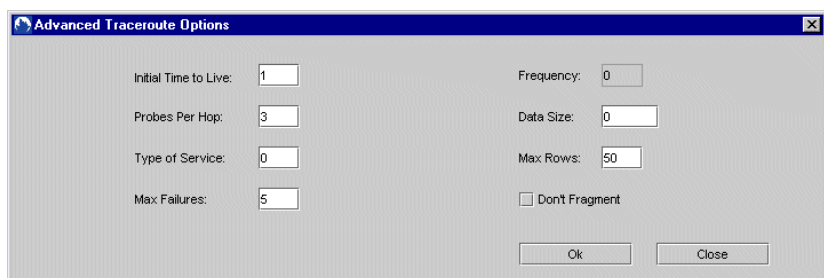


Figure 7: Device to IP address advanced traceroute options (Windows)



3. Set the Advanced Traceroute options. See Table 63 or Table 64.

NMC-RX to Device Options

Table 63: NMC-RX to device advanced traceroute parameters

| Parameter | Description |
|------------------------------|---|
| Resolve Addresses | Select to resolve addresses to host names |
| Loose Source Route Host List | Identifies certain milestone routers that must be used in route to the destination address. However, any path can be used to get to these milestone routers. Routes packets via the hosts specified by the host list Consecutive hosts can be separated by intermediate gateways (loose source routed). Maximum allowed by IP is 9 |

Device to IP Address Options

Table 64: Device to IP address advanced traceroute parameters

| Parameter | Description |
|----------------------|--|
| Initial Time to Live | Sets the number of hops (routers) that the traceroute request can traverse before it is discarded. The TTL field in the packet is decremented by one each time it passes through a router. When the number reaches zero, the router discards the packet and sends a TTL Expired ICMP message back. |

Table 64: Device to IP address advanced traceroute parameters (continued)

| Parameter | Description |
|-----------------|---|
| Probes Per Hop | Number of ICMP packets to send for each hop |
| Type of Service | Sets the ToS value in the ICMP packet for routers that are set up to treat packets with certain types of service differently than others. ToS is not used very often, and most routers ignore it. |
| Max Failures | Maximum number of failures before the command is terminated |
| Data Size | Specifies the size of the ICMP payload |
| Max Row | Maximum number of rows displayed |
| Don't Fragment | Sets the don't fragment (DF) bit. Routers that see these packets will not fragment them. |

- (Optional) Enter a host IP address in Host IP Address, press Enter, and click Add.

The host IP address is added to the list.

- Click OK to close the Advanced Traceroute dialog box.
- Click Traceroute.

The results appear in the dialog box.



NOTE: Depending on the origin selected, different results appear.



NOTE: Clicking Ping again clears the previous results, executes the command, and displays the new results.

Using the Config Save and Restore Utilities

The Configuration Save utility saves a device's running configuration to a staging area and then transfers it to a user-specified location via FTP. The Configuration Restore utility transfers saved config files via FTP back to the originating device.

The staging area is specified in the Resources Configurator on the Save/Restore tab of the main ConfigSync Service tab (see *Configuring the ConfigSync Service* in Chapter 13, *Using the Resource Configurator and NMC-RX Services*).

Saving a Configuration File

There are three ways to save a configuration file:

From the Tools menu – Select Device Utilities, and click Save Running Config File. You then must select a device and enter FTP destination information.

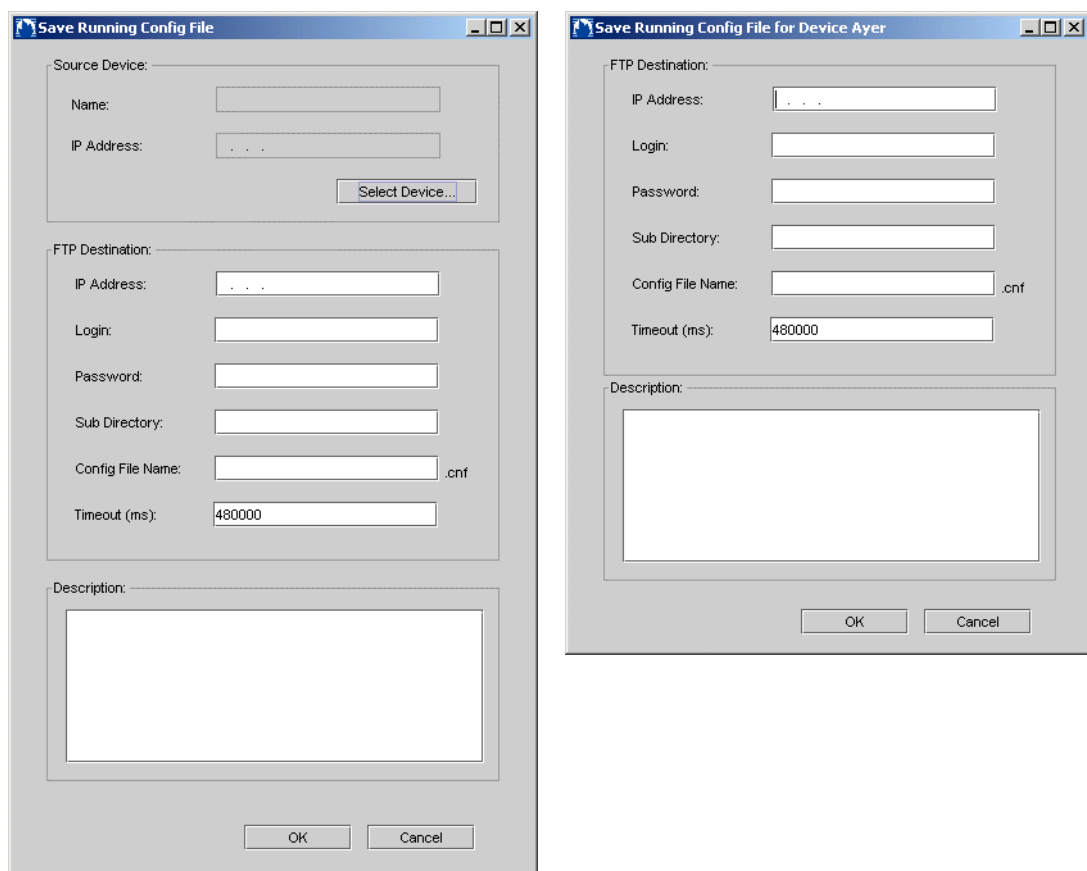
From the Network Workshop – Select the device, right-click, and click Save Running Config File. The name of the selected device is added to the dialog box title bar, and you only have to enter FTP destination information.

From the Device Workshop – Select the System folder, right-click, and click Save Running Config File. The name of the device is added to the dialog box title bar, and you only have to enter FTP destination information.

To save a running configuration file:

1. Launch the Configuration Save utility by using one of the methods described above.

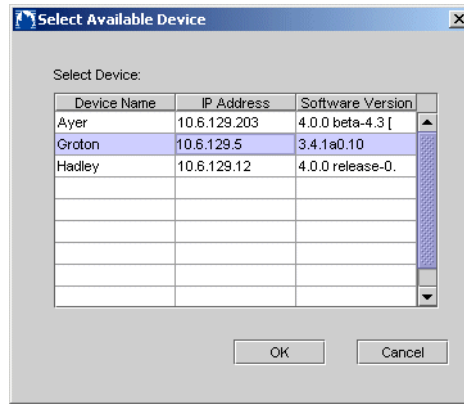
One of two possible Save Running Config File dialog boxes appear.



NOTE: If you launched the utility from a pop-up menu (right-click), the Source Device group box does not appear in the dialog box (example on right). Instead, the device name is added to the dialog box title bar.

2. Click the Select Device button, or, if you launched the utility from a device, skip to step 4.

The Select Available Device dialog box appears.



3. Select the device that is running the configuration you want to save, and click OK.

The device information is added to the Source Device group box.

4. Enter the FTP destination parameters. (This is where the config file will be saved.) See Table 65.

Table 65: Save running configuration file parameters

| Parameter | Description |
|------------------|--|
| IP Address | IP Address of configuration file destination |
| Login | Login user name for the FTP site |
| Password | Login password for the FTP site; cannot be empty |
| Sub Directory | <p>Directory where file will be saved (from the point of the FTP root directory)</p> <p>Cannot exceed 255 characters when combined with file name</p> <p>Cannot contain the following characters: * ? " < > % :</p> <p>Cannot contain ASCII values:</p> <p style="padding-left: 20px;">Less than or equal to 31</p> <p style="padding-left: 20px;">Greater than or equal to 127</p> |
| Config File Name | <p>Name of saved configuration file</p> <p>.CNF is appended to the file name</p> <p>128 characters (except / and \); leading spaces are not allowed</p> <p>Cannot exceed 255 characters when combined with Sub-Directory</p> <p>Cannot contain the following characters: / : \ * ? " < > %</p> <p>Cannot contain ASCII values:</p> <p style="padding-left: 20px;">Less than or equal to 31</p> <p style="padding-left: 20px;">Greater than or equal to 127</p> |
| Timeout (ms) | Number of milliseconds to wait for the FTP process to complete; range 300–2147483647 |

Table 65: Save running configuration file parameters (continued)

| Parameter | Description |
|-------------|--|
| Description | Additional information describing the configuration file |

5. Click OK. The config file is saved to the designated directory.

Restoring a Configuration File

There are four ways to restore a configuration file:

From the Tools menu – Select Device Utilities, and click Restore Config File. You then must select a device and enter FTP source information.

From the Network Workshop – Select the device, right-click, and click Restore Config File. The name of the selected device is automatically listed in the window title bar, and you only have to enter FTP source information.

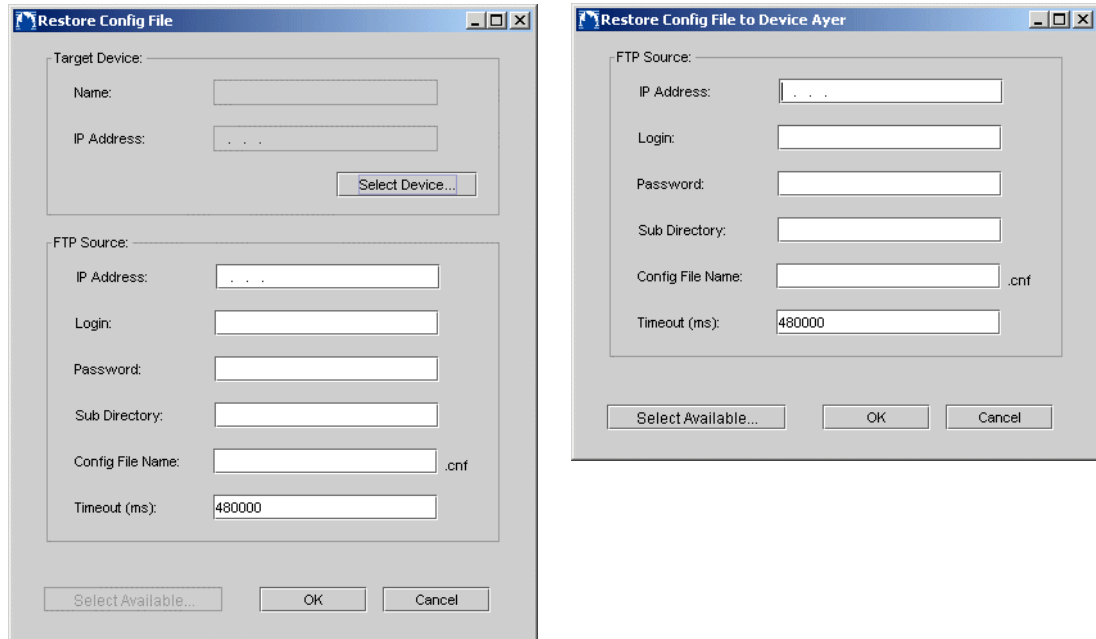
From the Device Workshop – Select the System folder, right-click, and click Restore Config File. The name of the device is automatically listed in the window title bar, and you only have to enter FTP source information.

From the Device-Wide Explorer – In the System folder, select Config Files, right-click, and click List All. Then select a configuration file in the list area, right-click, and click Restore.

To restore a configuration file:

1. Launch the Configuration Restore utility by using one of the methods described above.

One of two possible Restore Config File dialog boxes appear.



NOTE: If you launched the utility from a pop-up menu (right-click), the Target Device group box does not appear in the dialog box (example on right). Instead, the device name is added to the dialog box title bar.



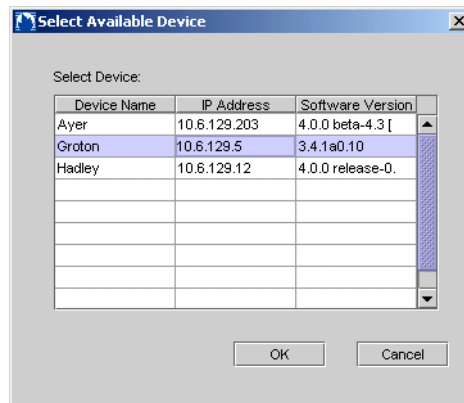
NOTE: If you launched the utility from the list area, the IP Address, Sub Directory, and Config File Name fields are automatically filled, and the Select Available button does not appear.

2. Click the Select Device button, or:

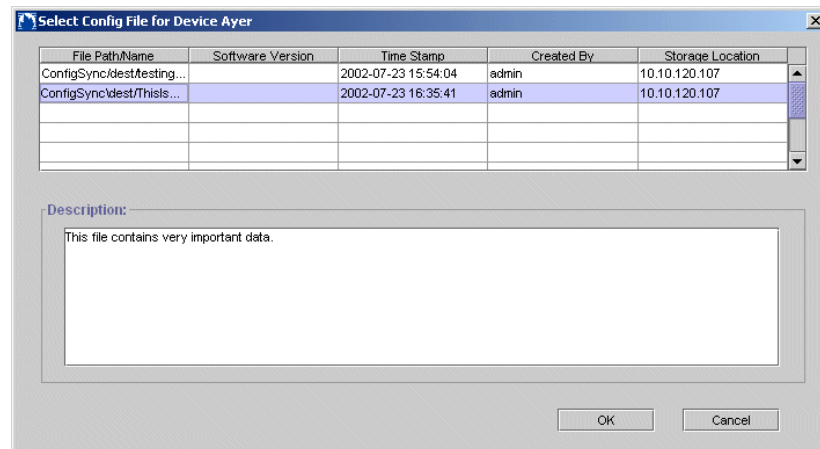
If you launched the utility from a device, skip to step 4.

If you launched the utility from the list area, skip to step 6.

The Select Available Device dialog box appears.



- Select the device where the configuration file will be copied to, and click OK.
The device information is added to the Target Device group box.
- Click the Select Available button to choose the configuration file.
The Select Config File for Device dialog box appears.



- Select a file, and click OK.
The FTP Source group box parameters are filled in. See Table 66.

Table 66: Restore configuration file parameters

| Parameter | Description |
|------------|--|
| IP Address | IP Address of the FTP source where the configuration file is located |
| Login | Login user name for the FTP site |
| Password | Login password for the FTP site; cannot be empty |

Table 66: Restore configuration file parameters (continued)

| Parameter | Description |
|------------------|---|
| Sub Directory | Directory where file resides (from the point of the FTP root directory) Cannot exceed 255 characters when combined with file name Cannot contain the following characters: * ? " < > % : Cannot contain ASCII values: Less than or equal to 31 Greater than or equal to 127 |
| Config File Name | Name of saved configuration file .CNF is appended to the file name 128 characters (except / and \); leading spaces are not allowed Cannot exceed 255 characters when combined with Sub-Directory Cannot contain the following characters: / : \ * ? " < > % Cannot contain ASCII values: Less than or equal to 31 Greater than or equal to 127 |
| Timeout (ms) | Number of milliseconds to wait for the FTP process to complete; range 300–2147483647 |
| Description | Additional information describing the configuration file |

6. Enter a login and password, and then click OK.

The file is restored.



NOTE: The Config Restore utility does not configure the device with the restored file; it simply places a copy of the configuration on the system. You must use the CLI to reload (reboot) the device with the restored file.

Deleting a Configuration File

To delete a saved configuration file for a device:

1. From the Device-Wide Explorer, in the System folder, select Config Files, right-click, and click List All.

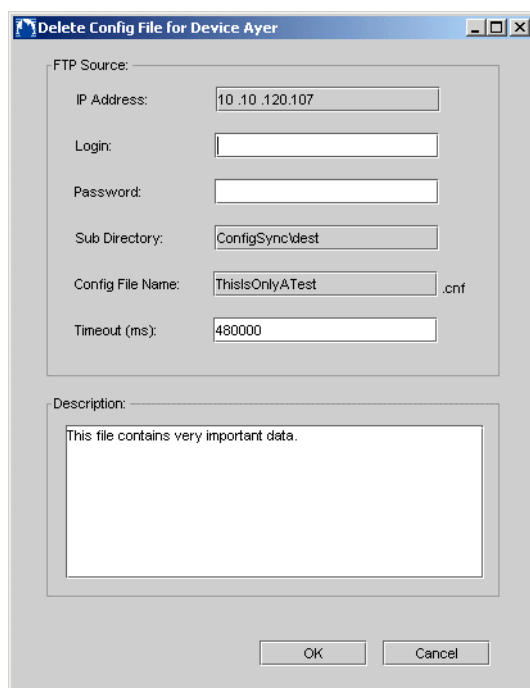
All saved config files for that device are displayed in the list area.

2. Select a configuration file, right-click, and click Restore.

A confirmation pop-up appears.

3. Click Yes.

The Delete Config File for Device dialog box appears.



4. Enter login and password information, and click OK.

The configuration file is deleted.

