



Configuring Translation Rules

Network address translation (NAT) converts private, internal LAN addresses into different public addresses before forwarding packets. In this way, a small number of public IP addresses can provide global connectivity for a large range of hosts.

By using NAT in a hub-and-spoke VPN, you enable the devices in your secured private network to access outside networks for nonconfidential purposes without monopolizing the resources required for VPN connections.

The following topics provide information about the use of NAT in Router MC:

- [Understanding NAT Concepts, page 1-1](#)
- [Defining Translation Rules, page 1-2](#)

Understanding NAT Concepts

Network Address Translation (NAT) enables devices that use internal IP addresses to send and receive data through the public Internet. Private NAT addresses are converted to globally routable IP addresses automatically when they try to access data on the Internet.

The stability of your hub-and-spoke VPN tunnels is enhanced when you use NAT, because resources required for VPN connections are not used for other purposes, and the VPN tunnel is kept available for traffic requiring complete security. Sites inside the VPN can use NAT through a split tunnel to exchange nonconfidential traffic with outside devices, and they do not squander VPN bandwidth or overwhelm the hub at the tunnel head-end by directing nonessential traffic through it.

NAT can be configured with dynamic IP addressing, or static IP addressing. Router MC supports dynamic NAT only, and applies to it an “overload” feature that permits what is known as port-level NAT or Port Address Translation (PAT). PAT can associate thousands of private NAT addresses with a small group of public IP address, through the use of port addressing. Router MC uses PAT if the addressing requirements of your network exceed the available addresses in your dynamic NAT pool.

**Note**

To learn more about network address translation (NAT), visit Cisco.com at http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094e77.shtml.

Defining Translation Rules

Defining a translation rule involves the following two steps:

- Creating a traffic filter. To use the NAT features in Router MC, you must identify the traffic flows that require NAT by defining traffic filters.
- Creating an address pool or specifying a VPN interface. Internal devices that require external connections will draw their translated addresses from an address pool, or will use the IP address of the external (VPN) interface on the devices as the translated IP address.

**Note**

To define NAT on a device group, you must specify a VPN interface. The address pool option is only available for single devices.

**Note**

You must do both these steps. If you attempt to define a traffic filter without defining a NAT address, a validation error will be generated and displayed in the Error Checking page of the Job wizard, on deployment.

You do these steps in the Translation Rules page under the Configuration tab.

Before You Begin

If workflow mode is enabled, make sure you are working within the context of an open activity.

Procedure

- Step 1** Select **Configuration > Translation Rules**. The Translation Rules page appears. [Table 1-1 on page 1-4](#) describes the elements in the Translation Rules page.
 - Step 2** Click **Create** to create a new traffic filter. The Create ACE dialog box appears. See [Table 1-3 on page 1-6](#) for a description of the Create ACE dialog box.
 - Step 3** In the Source fields, either enter the source IP address, or select a network group from the list box.
 - Step 4** In the Destination fields, either enter the destination IP address, or select a network group from the list box.
 - Step 5** Select the Permit check box.
 - Step 6** Click **Apply**. The Create ACE dialog box closes, returning you to the Translation Rules page.
 - Step 7** Click **Select NAT Address**. The NAT Address Type dialog box opens. See [Table 1-2 on page 1-5](#) for a description of the elements in the NAT Address Type dialog box.
 - Step 8** In the Type area, select a radio button, either **Address Pool** or **VPN Interface**.
 - Step 9** If you selected Address Pool, enter a network address in the From and To fields to define the start and end of the address pool range. Enter a subnet mask in the Pool Subnet Mask field.
 - Step 10** Click **Apply** to save your NAT definitions in the database.
The NAT Address Type dialog box closes, returning you to the Translation Rules page. The selected NAT address is displayed in the Address Type field.
-

[Table 1-1](#) describes the elements in the Translation Rules page.

Table 1-1 Translation Rules—GUI Reference

GUI Element	Description
Address Type field	Displays the selected NAT address.
Select NAT Address button	Opens the NAT Address Type dialog box, in which you can select the required address type. See Table 1-2 on page 1-5 for a description of the elements in the NAT Address Type dialog box.
check box	Enables you to select a filter to edit it, delete it, or move it higher or lower in the table. You can select more than one check box at a time.
Source column	Displays the source address.
Destination column	Displays the destination address.
Action column	Identifies the associated action for the specified traffic filter. Available actions include: <ul style="list-style-type: none"> • Permit—Allow the traffic. • Deny—Block the traffic.
Rows per page list box	Enables you to change the number of traffic rule filters displayed per page.
<< link; >> link	Click the << link, when it is available, to return to the previous screen in the filters table. Click the >> link, when it is available, to advance to the next screen in the filters table.
Move Up button	Move the selected filter one row higher in the list of filters. This increases its priority in comparison to those that are lower in the list.
Move Down button	Move the selected filter one row lower in the list of filters. This decreases its priority in comparison to those that are higher in the list.
Create button	Opens the Create ACE (NAT) dialog box. See Table 1-3 on page 1-6 for a description of the elements displayed in the Create ACE (NAT) dialog box. Note If an object other than Global is selected in the Object Selector, creating a new filter adds any existing inherited values to the filter.
Edit button	Opens the Edit Filter dialog box.
Delete button	Deletes the specified traffic filter.

Table 1-1 Translation Rules—GUI Reference (continued)

GUI Element	Description
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions. Note Clicking the Clear button deletes both the traffic filter definition and the selected NAT address.
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited values.

Table 1-2 describes the elements in the NAT Address Type dialog box.

Table 1-2 NAT Address Type—GUI Reference

GUI Element	Description
Type	This area contains the following three radio buttons from which you can select the address type: <ul style="list-style-type: none"> • Address Pool: Only available when a single spoke is selected in the Object Selector. Select this radio button to define an address pool from which IP addresses for NAT will be drawn. • VPN Interface: Select this radio button to specify that the IP address of the VPN interface on the device(s) should be used as the translated address. • None: Select this radio button if you have NAT configurations on a device that were inherited from a higher level object, and you want to remove them.
From field	Only appears when the Address Pool radio button is selected. Enter a network address to define the start of the address pool range.
To field	Only appears when the Address Pool radio button is selected. Enter a network address to define the end of the address pool range.
Pool Subnet Mask field	Only appears when the Address Pool radio button is selected. Enter the subnet mask in bits, such as 192.168.168.0/24.
Apply button	Click to save your NAT selections in the database, and return to the Translation Rules page.
Cancel button	Click to exit without saving your selections.

Table 1-3 describes the elements in the Create ACE (NAT) dialog box.

Table 1-3 Create ACE (NAT)—GUI Reference

GUI Element	Description
Source: IP Address field; Network Group list box	Use this field to specify the source of the flow that will use NAT addressing. Enter the IP address or host name of a device, or the IP address and subnet mask of a network. Alternatively, select a predefined network group representing the required range of networks. The list of available network groups includes inside interfaces and internal networks on the spokes, enabling you to broaden your definition of flows that will use NAT addressing.
Destination: IP Address field; Network Group list box	Enter the IP address or host name of a device, or the IP address and subnet mask of a network. Alternatively, select a predefined network group representing the required range of networks. Traffic transmitted to the specified destination networks will use NAT addressing.
Permit check box	Select to translate this traffic flow. Leave unselected to prevent translation.
Apply button	Click to apply your definitions.
Cancel button	Click to cancel your definitions.