CHAPTER 11

IP Services

This chapter describes provisioning IP on the Cisco IAD1101 and includes the following sections:

Static IP Routing

EMS uses static IP routes to define paths through the Cisco IAD1101 and across the network. You can assign static IP routes to direct IP traffic on the Ethernet interface, and any T1 lines configured for IP (IP over Frame Relay or IP over PPP).

A static IP route consists of the following information:

- **Interface**—Interface that leads to the destination IP address
- **Destination**—Destination IP address
- **Gateway**—Next IP addressed equipment downstream
- **Netmask**—Subnet mask to apply to the destination address

Figure 11-1 shows a sample network, with a Cisco IAD1101 connected to a router over a PPP link.

Note The IP addresses used in this chapter are only for illustration. You must use your own IP addresses, based on your licensing.

To assign a static route from the Cisco IAD1101 to Host A, over a T1 line, enter the following information:

Network Route:

- Interface—IP over PPP
- Destination—10.0.0.0
- Gateway—10.10.10.1
- Netmask—255.0.0.0

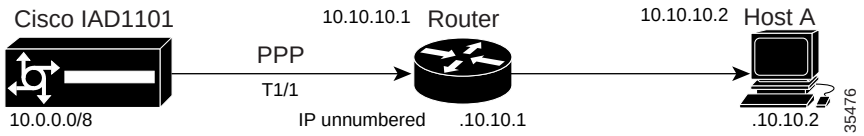
Default Route:

- Gateway—10.10.10.1

Host Route:

- Destination—10.0.0.2
- Gateway—10.10.10.1

Figure 11-1 Static IP Route Example – over T1



To assign a static route from the Cisco IAD1101 to Host A, over Ethernet, enter the following information:

Network Route:

- Interface—IP over Ethernet
- Destination—10.0.0.0
- Gateway—150.150.150.2
- Netmask—255.0.0.0

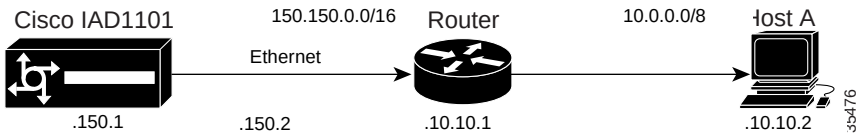
Default Route:

- Gateway—150.150.150.2

Host Route:

- Destination—10.10.10.2
- Gateway—150.150.150.2

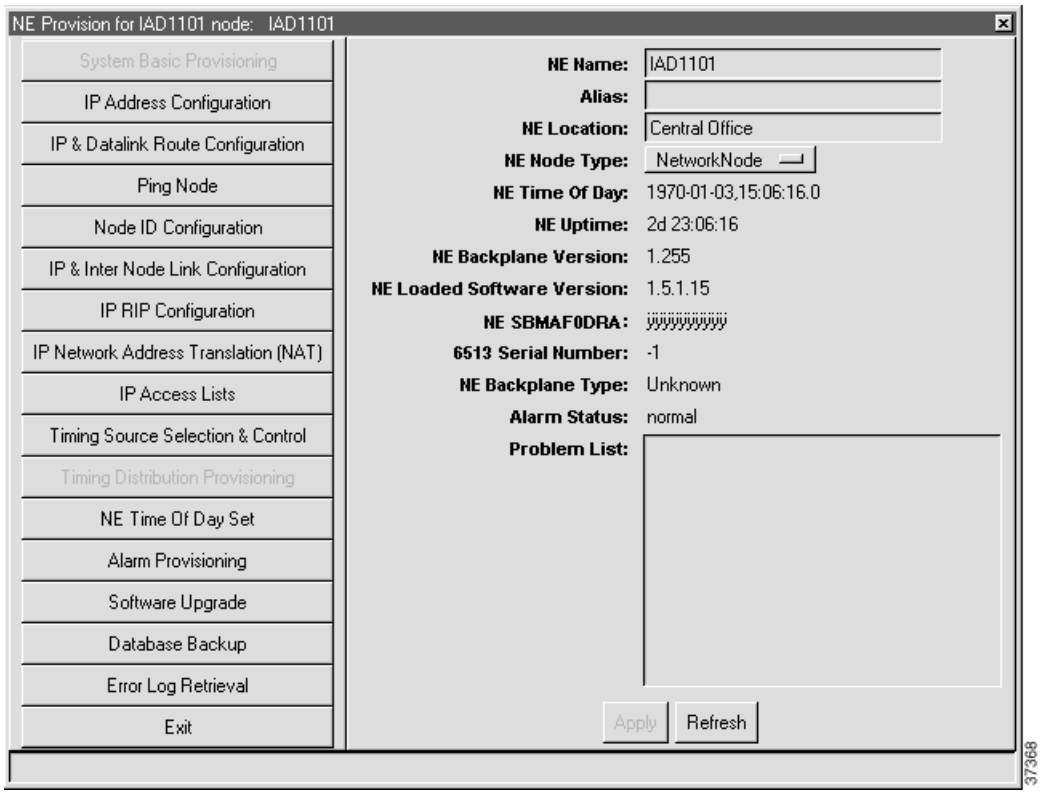
Figure 11-2 Static IP Route Example – over Ethernet



Assigning Static IP Routes

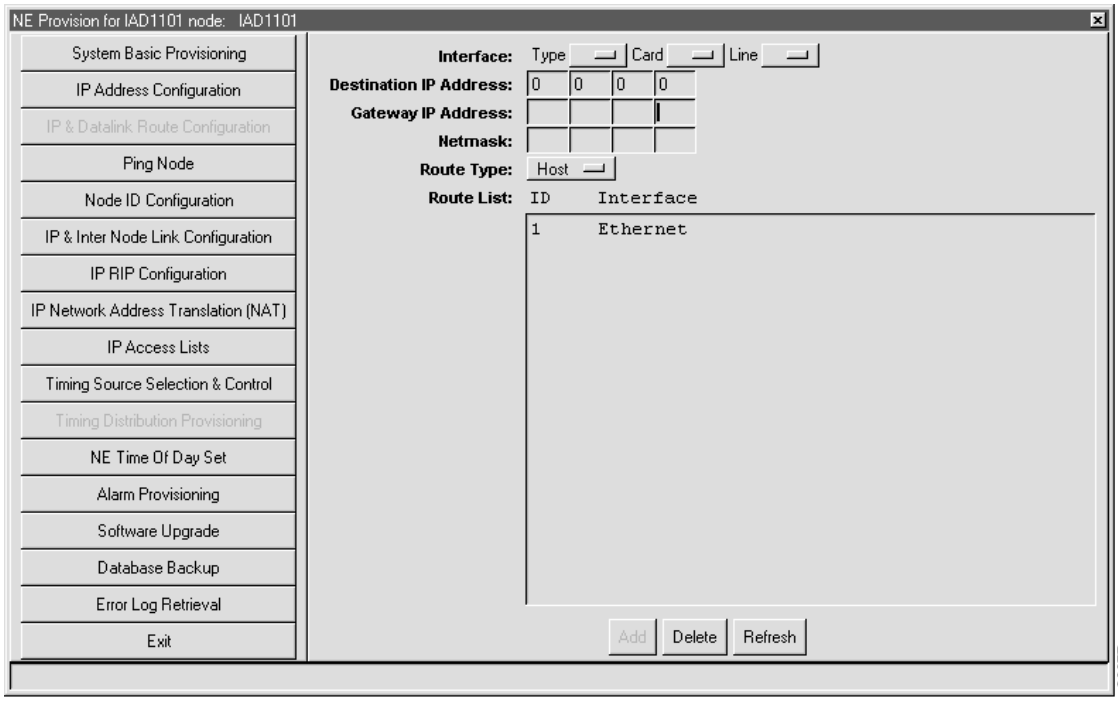
Step 1 From Cisco 6700 NodeView, double-click the node nameplate. EMS launches the NE provision window. (See Figure 11-3.)

Figure 11-3 IAD1101 NE Provision Window



Step 2 From the function bar on the left, click the **IP & Datalink Route Configuration** button. EMS launches the data link route configuration window. (See Figure 11-4.)

Figure 11-4 IP & Datalink Route Configuration Window



Step 3 Set the following parameters in the data link route configuration window:

- **Interface**—Select the outgoing interface for the route. You must identify the interface type, card, slot, and line number. To use the Ethernet port, select **Ethernet**.
- **Destination IP Address**—The destination address for the route. To configure a default route, leave this field at the default (**0.0.0.0**).
- **Gateway IP Address**—The next IP addressed equipment downstream.
- **Netmask**—The netmask for the destination IP address. To configure a default route, leave blank.
- **Route Type**—Select one of the following route types:
  - **Default**—This route is always used, unless another static route (Host or Network) is created.
  - **Host**—This route points to a specific host.
  - **Network**—This route points to a specific network of hosts.

Step 4 Click **Add** when finished.

Step 5 Click the **Exit** button (on the function bar) to return to the NodeView.

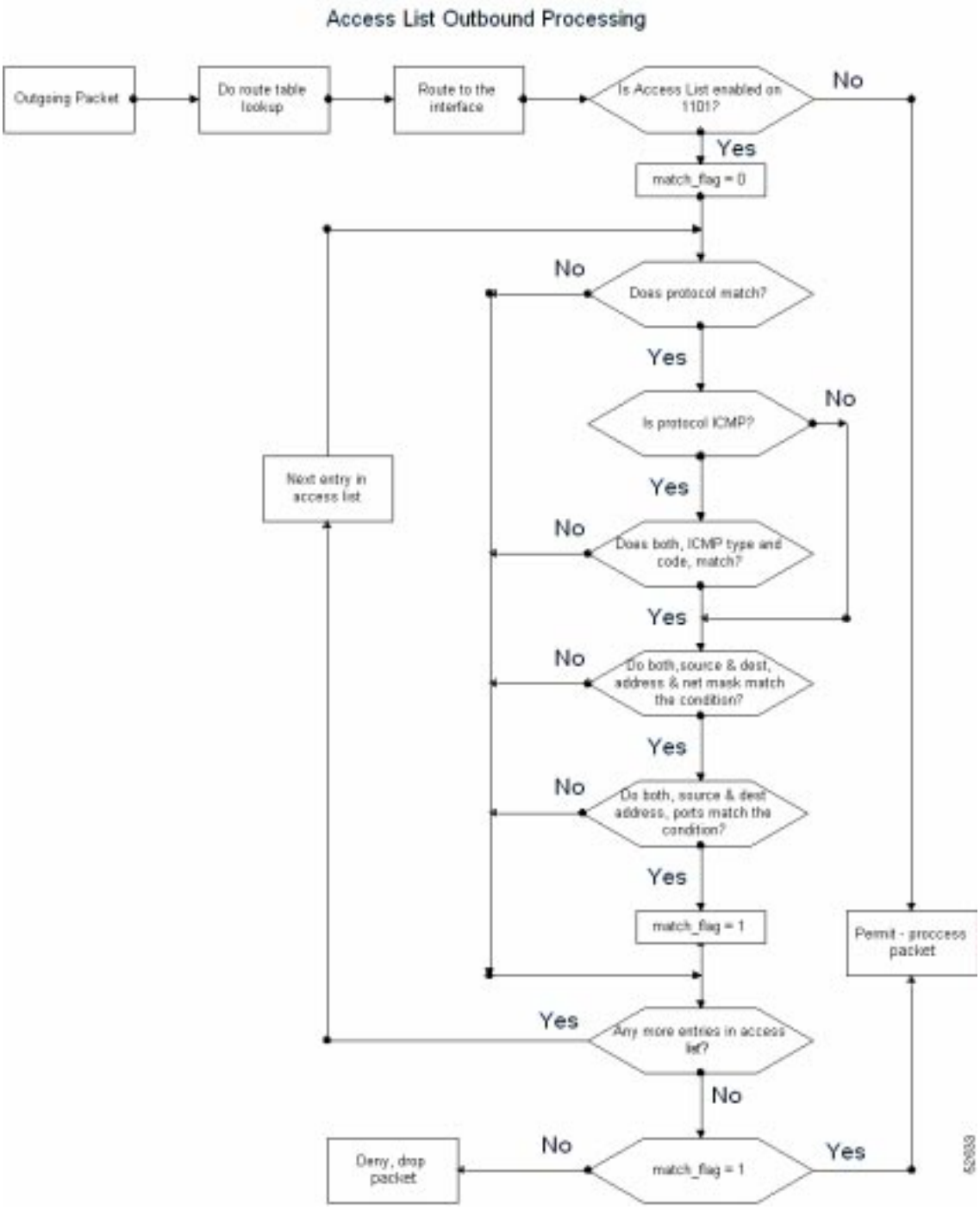
Note You can add as many routes as needed, but only one route can be the default route.

Access Lists

An access list is a sequential collection of permit and deny conditions that apply to IP addresses. EMS tests addresses against the conditions in an access list one by one. All entries in the list are checked. If at any point there is a mismatch, the software rejects the address. The following flow charts illustrate how the decisions are made. (See

Figure 11-5 Access List – Inbound Decision Tree

Figure 11-6 Access List – Outbound Decision Tree



Access lists allow the Cisco IAD1101 to filter incoming or outgoing IP packets based on the following criteria:

- Interface
- Direction of traffic (incoming or outgoing)
- Source IP address, subnet mask, and port

- Destination IP address, subnet mask, and port
- Layer 4 protocol (TCP, UDP, ICMP)
- ICMP message type

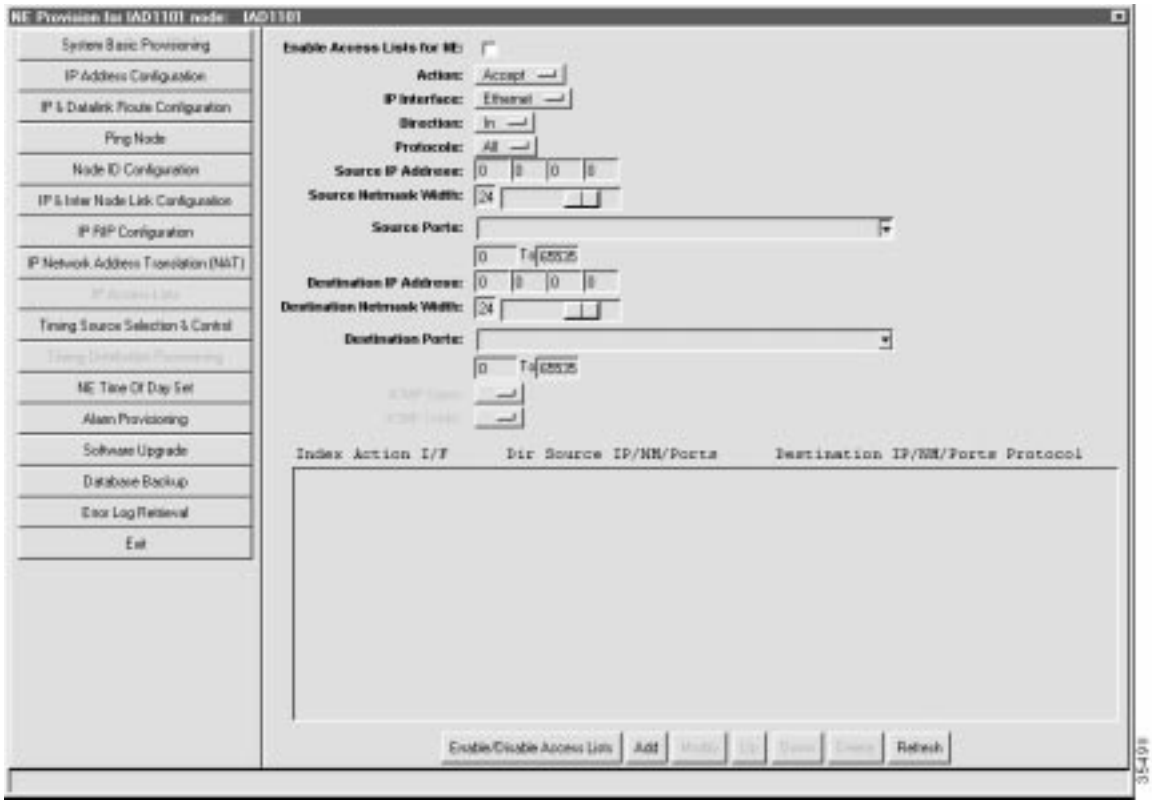
Note UDP ports 161 and 162 are used for management and alarm traffic, respectively.

Provisioning Access Lists

To provision access lists on the NE, complete the following steps starting in the NE provisioning window:

Step 1 Click **IP Access Lists** in the function bar. EMS launches the access list provisioning window. (See Figure 11-7.)

Figure 11-7 Provisioning IP Access Lists



Step 2 Set the following fields to configure the access list:

- **Action**—Select **Accept** or **Reject**.
- **IP Interface**—Select an individual PPP link, or select **Ethernet**.
- **Direction**—Select **In** or **Out**.
- **Protocols**—Select the protocols to be filtered (All, TCP, UDP, or ICMP).

  - **ICMP Type**—Select the ICMP protocol type to be filtered.
  - **ICMP Code**—Select the code for the ICMP protocol type.
- **Source IP Address**—Select the source IP address to filter.
- **Source Netmask Width**—Select the netmask for the IP address.
- **Source Ports**—Select the ports to be filtered.
  - **Include** or **Exclude**—Select the action to be applied to the ports.
- **Destination IP Address**—Select the destination IP address to filter.
- **Destination Netmask Width**—Select the netmask for the IP address.
- **Destination Ports**—Select the ports to be filtered.

Step 3 Click **Add** when finished.

Step 4 Repeat Step 2 and Step 3 to configure additional access lists. You can configure as many as 32 access lists.

Step 5 Click **Enable/Disable Access Lists**.

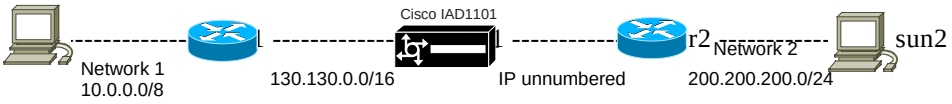
Caution EMS rejects traffic on every interface that does not have an access list definition. Before you proceed, you must create at least one entry per interface to accept traffic, or the NE will reject all traffic on the unprovisioned interface, including management traffic. Be sure to enable the SNMP protocol in the access list, and provision an accept statement to allow packets in and out of the interface on UDP port 161.

Step 6 Click **Apply NE Enable** to activate access lists.

Caution Enabling access lists might prevent user traffic from entering or exiting the NE, including management traffic.

Blocking Telnet Sessions–Examples

Figure 11-8 Sample Network



There are two ways to provision the access list to block a Telnet session from network 2 (200.200.200.0) to network 1 (10.0.0.0). Method 1 (see Figure 11-9) filters on the inbound interface, preventing the Cisco IAD1101 from routing the packet first, then having to possibly reject it later because of an access list condition. Method 2 (see Figure 11-10) sets up filtering on the outbound interface.

Figure 11-9 Method 1

reject either	out	200.200.200.0/24/all	10.0.0.0/8/23	TCP
accept 1	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept 1	out	0.0.0.0/0/all	0.0.0.0/0/all	all
accept either	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept either	out	0.0.0.0/0/all	0.0.0.0/0/all	all

Figure 11-10 Method 2

reject 1	out	200.200.200.0/24/all	10.0.0.0/8/23	TCP
accept 1	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept 1	out	0.0.0.0/0/all	0.0.0.0/0/all	all
accept ether	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept ether	out	0.0.0.0/0/all	0.0.0.0/0/all	all

There are two ways to provision the access list to block a Telnet session from network 1 (10.0.0.0) to network 2 (200.200.200.0). Method 1 (see Figure 11-11) filters on the inbound interface, preventing the Cisco IAD1101 from routing the packet first, then having to possibly reject it later because of an access list condition. Method 2 (see Figure 11-12) sets up filtering on the outbound interface.

Figure 11-11 Method 1

r

reject either	in	10.0.0.0/8/all	200.200.200.0/24/23	TCP
accept 1	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept 1	out	0.0.0.0/0/all	0.0.0.0/0/all	all
accept either	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept either	out	0.0.0.0/0/all	0.0.0.0/0/all	all

Figure 11-12 Method 2

reject 1	out	10.0.0.0/8/all	200.200.200.0/24/23	TCP
accept 1	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept 1	out	0.0.0.0/0/all	0.0.0.0/0/all	all
accept ether	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept ether	out	0.0.0.0/0/all	0.0.0.0/0/all	all

Blocking ftp Sessions–Examples

In the same sample network (see Figure 11-8 on page 11-11), there are two ways to provision the access list to block an ftp session from network 2 (200.200.200.0) to network 1 (10.0.0.0). Method 1 (see Figure 11-13) filters on the inbound interface, preventing the Cisco IAD1101 from routing the packet first, then having to possibly reject it later because of an access list condition. Method 2 (see Figure 11-14) sets up filtering on the outbound interface.

Figure 11-13 Method 1

r

reject 1	in	200.200.200.0/24/all	10.0.0.0/8/20	TCP
reject 1	in	200.200.200.0/24/all	10.0.0.0/8/21	TCP
accept 1	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept 1	out	0.0.0.0/0/all	0.0.0.0/0/all	all
accept either	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept either	out	0.0.0.0/0/all	0.0.0.0/0/all	all

Figure 11-14 Method 2

reject ether	out	200.200.200.0/24/all	10.0.0.0/8/20	TCP
reject ether	out	200.200.200.0/24/all	10.0.0.0/8/21	TCP
accept 1	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept 1	out	0.0.0.0/0/all	0.0.0.0/0/all	all
accept ether	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept ether	out	0.0.0.0/0/all	0.0.0.0/0/all	all

There are two ways to provision the access list to block an ftp session from network 1 (10.0.0.0) to network 2 (200.200.200.0). Method 1 (see Figure 11-15) filters on the inbound interface, preventing the Cisco IAD1101 from routing the packet first, then having to possibly reject it later because of an access list condition. Method 2 (see Figure 11-16) sets up filtering on the outbound interface.

Figure 11-15 Method 1

reject either	**in**	**10.0.0.0/8/all**	**200.200.200.0/24/20**	**TCP**
reject either	in	10.0.0.0/8/all	200.200.200.0/24/21	TCP
accept 1	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept 1	out	0.0.0.0/0/all	0.0.0.0/0/all	all
accept either	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept either	out	0.0.0.0/0/all	0.0.0.0/0/all	all

Figure 11-16 Method 2

reject 1	**out**	**10.0.0.0/8/all**	**200.200.200.0/24/20**	**TCP**
reject 1	out	10.0.0.0/8/all	200.200.200.0/24/21	TCP
accept 1	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept 1	out	0.0.0.0/0/all	0.0.0.0/0/all	all
accept ether	in	0.0.0.0/0/all	0.0.0.0/0/all	all
accept ether	out	0.0.0.0/0/all	0.0.0.0/0/all	all

To accept only SNMP traffic to the Cisco IAD1101 from subnet 10.0.0./8, provision the access list as follows:

accept either	**in**	**10.0.0.0/8/161**	**130.130.130.2/32/161**	**UDP**
accept either	out	130.130.130.2/32/161	10.0.0.0/8/161	UDP

Modifying or Deleting Access Lists

Use the following buttons to modify or delete an access list.

Caution Changes made to an access list entry take place immediately. Cisco Systems recommends that you disable access lists for the NE before making changes.

- **Modify**—Changes the settings of an existing access list.
- **Up**/**Down**—Moves an existing access list up or down relative to other list entries.
- **Delete**—Removes an access list.
- **Refresh**—Displays the settings of the selected access list.

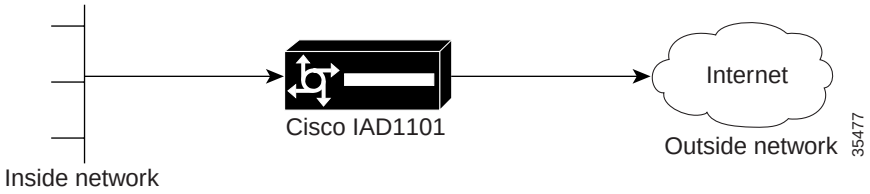
About Network Address Translation

Network Address Translation (NAT) is a feature that allows an organization's IP network to appear from the outside to use different IP address space than what it is actually using. Thus, NAT allows an organization with nonglobally routable addresses to connect to the Internet by translating those addresses into globally routable address space. NAT is described in RFC 1631.

NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT is configured on the router at the border of a stub domain (referred to as the inside network) and a public network such as the Internet (referred to as the outside network). NAT translates the internal local addresses to globally unique IP addresses before sending packets to the outside network.

Figure 11-17 shows an example of NAT configured on a Cisco IAD1101.

Figure 11-17 NAT Example



Using Static and Dynamic NAT

NAT offers two types of address translation, static and dynamic.

- Static translation establishes a one-to-one mapping between the inside address and outside address. Static translation is useful when a host on the inside must be accessible by a fixed address from the outside.

```
10.0.0.1 --> 11.0.0.5
10.0.0.2 --> 11.0.0.6
10.0.0.3 --> 11.0.0.7
```

- Dynamic translation establishes a mapping between an inside address and a pool of outside addresses. With dynamic NAT, a large number of inside addresses can be mapped to a single outside address, using port numbers to keep track of the address maps.

```
10.0.0.1 --> 12.0.0.9
10.0.0.2 --> 12.0.0.9
10.0.0.3 --> 12.0.0.9
```

Note The IP addresses used in this chapter are only for illustration. You must use your own IP addresses, based on your licensing.

Observing NAT Restrictions

The following conditions apply to NAT provisioned on the Cisco IAD1101:

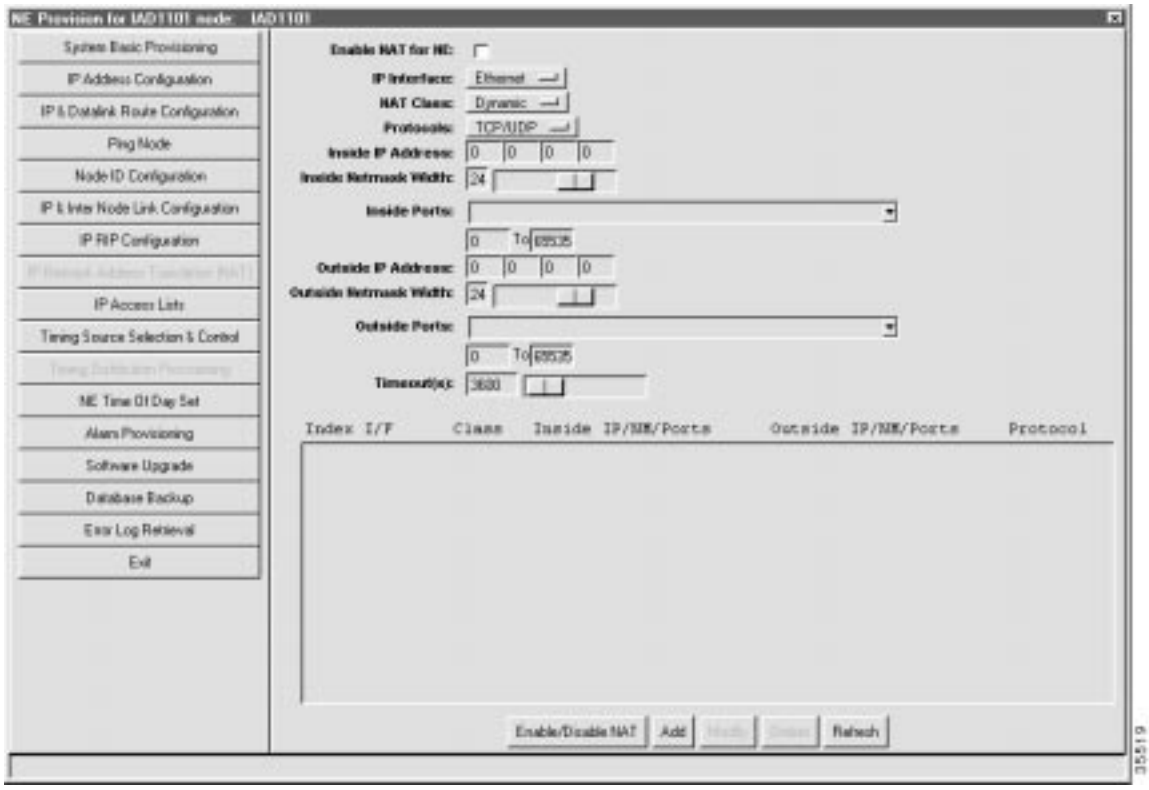
- A Cisco IAD1101 that is provisioned with static NAT does not allow passive FTP attempts from the outside network to the inside network.
- You cannot login using the Reflection X application through a Cisco IAD1101 that is implementing NAT.
- Routing tables contain outside NAT addresses. When sending RIP updates over a NAT-enabled interface, the Cisco IAD1101 looks at both the routing table and the NAT table. If the destination address/subnet for a particular route is part of an inside subnet (based on the address and netmask) for this interface, this entry is suppressed from RIP updates on this interface. Note that NAT translations are unique to each interface.

Caution Enabling NAT might prevent user traffic from entering or exiting the Cisco IAD1101, including management traffic.

Provisioning NAT

Step 1 From the NE provision window, select **IP Network Access Translation (NAT)** in the function bar. EMS launches the NAT provisioning window. (See Figure 11-18.)

Figure 11-18 Provisioning NAT



Step 2 Set the following fields to configure the network address translation:

- **IP Interface**—Select an individual IP data link, or select **Ethernet** to configure the Ethernet port.
- **NAT Class**—Select the type of NAT for this interface:
  - **Static**—A one-to-one translation of IP addresses.
  - **Dynamic**—A scalable translation of IP addresses.
- **Inside IP Address**—Enter the inside IP addresses to translate.
- **Inside Netmask Width**—Enter the netmask for the inside IP addresses to translate.
- **Inside Ports**—Enter the range of ports for the inside IP addresses.
- **Outside IP Address**—Enter the outside IP addresses used for translation.
- **Outside Netmask Width**—Enter the netmask for the outside IP address.
- **Outside Ports**—Enter the range of ports for the outside IP addresses.
- **Protocols**—Select the protocols to be filtered (All, TCP, UDP, TCP/UDP, or ICMP).
- **Timeout**—For dynamic NAT, enter the time in seconds for a NAT table entry to expire.

Step 3 Click **Add** when finished.

Step 4 Repeat Step 2 and Step 3 to configure additional NAT entries. You can configure as many as 8 NAT entries.

Step 5 Click **Enable/Disable NAT** to activate NAT.

Caution Enabling NAT might prevent user traffic from entering or exiting the Cisco IAD1101, including management traffic.

Modifying or Deleting NAT

Click a NAT entry in the list window, and use the following buttons to modify or delete a NAT entry:

- **Modify**—Changes the settings of an existing NAT entry.
- **Delete**—Removes a NAT entry.

  Note If a dynamic NAT entry is in use, you must uncheck the **Enable NAT for NE** box before deleting the NAT entry.

- **Refresh**—Displays the settings of the selected NAT entry.

Securing the Network with NAT

On a Cisco IAD1101 with a static or dynamic NAT translation, an outside host can still gain access to an inside (untranslated) host address. To block outside access to the inside network, create a static NAT that translates inbound addresses into a "dummy" address, then create an access list that filters out the dummy address. See "Access Lists" on page 11-6 for access list information and procedures.

The following security procedure uses a "dummy" address, as previously described.

Note The IP addresses used in this chapter are only for illustration. You must use your own IP addresses, based on your licensing.

Step 1 Provision the Cisco IAD1101 with a static NAT entry:

- IP Interface—Select the PPP link to the router.
- NAT Class—Select **Static**.
- Inside IP Address—**10.0.0.0**.
- Inside Netmask Width—**8**.
- Inside Ports—**0 to 65535** (default).
- Outside IP Address—1**2.0.0.0**.
- Outside Netmask Width—**8**.
- Outside Ports—**0 to 65505** (default).
- Protocols—**All** (default).
- Timeout—**86400** (default).

Step 2 Create a dynamic NAT entry to prevent direct outside access to 10.0.0.0/8. Use **99.0.0.1** as the dummy address.

Step 3 Create an access list entry that rejects all inbound traffic with IP address 99.0.0.1:

- Action—**Reject**.
- IP Interface—Select the PPP link to the router.
- Direction—**In**.
- Protocols—**All**.
- Source IP Address—**0.0.0.0**.
- Source Netmask Width—**32**.
- Source Ports—Include **0** to **65535**.
- Destination IP Address—**99.0.0.1**.
- Destination Netmask Width—**0**.
- Destination Ports—Include **0** to **65535**.

Routing Information Protocol

The Routing Information Protocol (RIP) is a distance-vector protocol that uses hop count as its metric (where hop is defined as the next IP addressed equipment downstream). RIP sends routing-update messages at regular intervals, and whenever the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route.

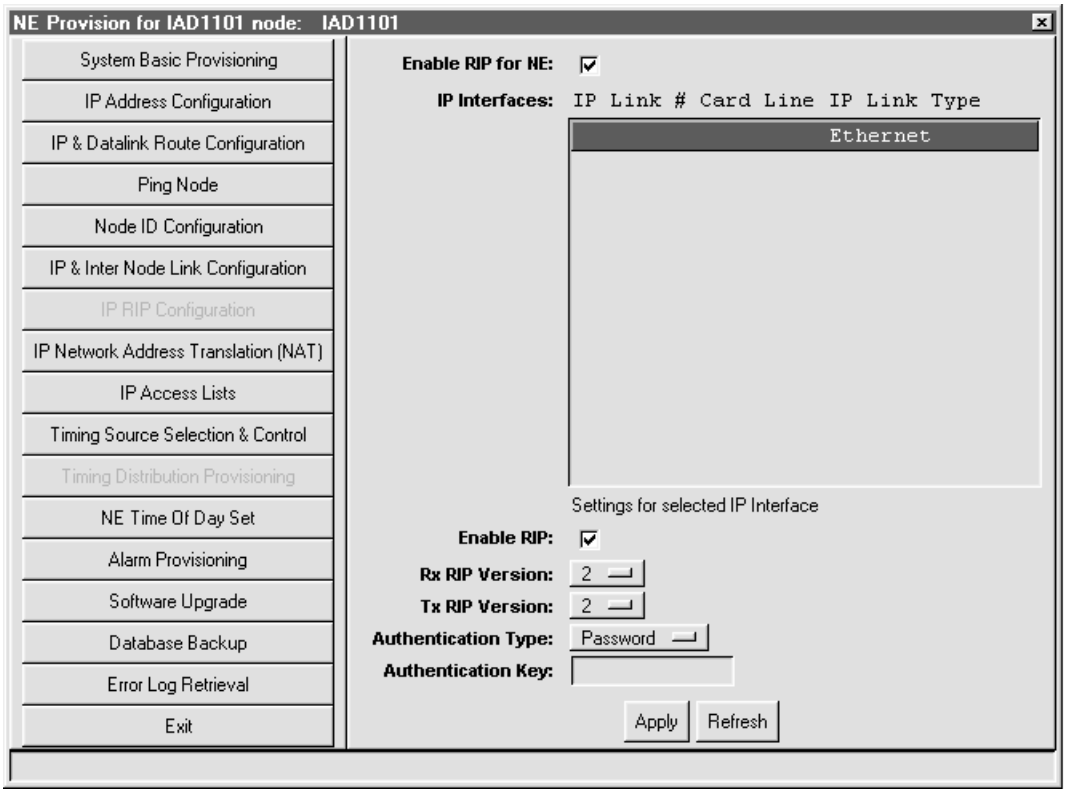
Note On a Cisco IAD1101 with a Frame Relay link, but without a PPP link, RIP does not advertise the node IP address over the Frame Relay link. To gain access to the Cisco IAD1101 over the Frame Relay link, use the Frame Relay address (not the node address) as the address for the Cisco IAD1101. This is not needed when both Frame Relay and PPP links exist on the Cisco IAD1101.

Provisioning RIP

To provision RIP on the NE, complete the following steps starting in the NE provision window:

Step 1 Click **IP RIP Configuration**. EMS launches the RIP provisioning window. (See Figure 11-19.)

Figure 11-19 Provisioning RIP



Step 2 Click **Enable RIP for NE**.

Step 3 In the **IP Interfaces** list, select the interfaces to be provisioned for RIP.

Step 4 Click **Enable RIP**.

Step 5 Select the **Rx RIP Version**—**1**, **2**, or **1 or 2**.

Step 6 Select the **Tx RIP Version**—**None**, **1**, **RIP1Compatible**, or **2**.

Step 7 Select the **Authentication**—**None** or **Password**.

Step 8 If password authentication is selected (RIPv2 only), enter the password in the **Authentication Key** field.

Step 9 Click **Apply** to provision RIP for the selected interfaces.

Note When you activate RIP on a Cisco IAD1101 interface, RIP advertises all directly-connected nodes over the interface.

Note RIP1Compatible is a version of RIPv2 that can be processed by a node using RIPv1.

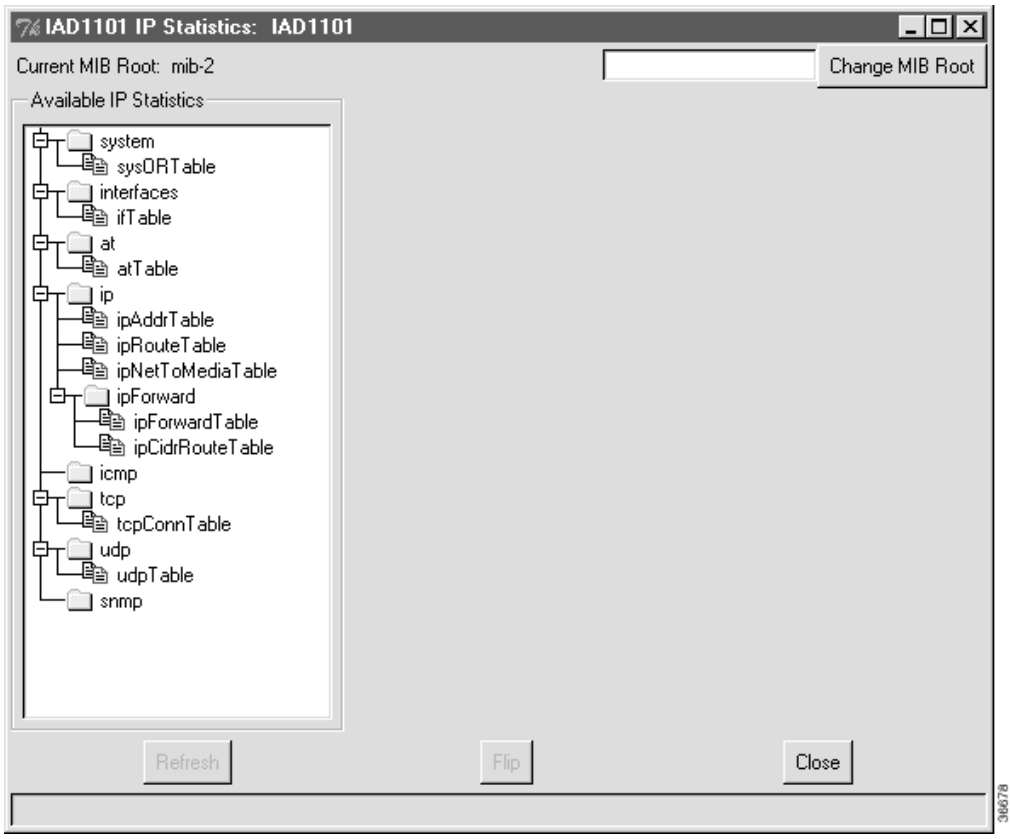
IP Statistics

EMS maintains statistics for all IP activity on the Cisco IAD1101, including routing tables, interface activity, and Layer 4 protocol statistics.

Monitoring IP Statistics

Step 1 From Cisco 6700 NodeView, select **Objects > IP Statistics** from the NodeView menu bar. EMS launches the IP statistics window (See Figure 11-20.)

Figure 11-20 IP Statistics Window



Step 2 Under **Available IP Statistics**, click the icon for the desired display. Statistic information appears in the a new frame on the right side of the window. Statistic information and descriptions can be found in RFC1213 (Management Information Base for Network Management of TCP/IP-based internets: MIB-II).

Step 3 Use the following buttons to alter the display:

- **Refresh**—Updates the table with the latest information
- **Flip**—Changes the orientation of the table, from horizontal to vertical

Step 4 Click **Close** to close the display.