CHAPTER 46

Configuring Layer 2 NAT

This chapter provides information to help you configure the Layer 2 NAT features introduced in Cisco IOS Release 15.0(2)EB.

Note For complete information about Cisco Industrial Ethernet 2000 Series switches, see the Release Notes, Command Reference, and Configuration Guide at www.cisco.com/en/US/products/ps12451/tsd_products_support_series_home.html

Finding Feature Information

Your software release may not support all the features documented in this document. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Layer 2 NAT

Layer 2 NAT is included in the Enhanced LAN Base feature set, available for Cisco IOS 15.0(2)EB or later. It may require a license upgrade and a software upgrade, depending on the model. For detailed instructions, see www.cisco.com/en/US/docs/switches/lan/cisco_ie2000/software/release/15_0_2_eb/upgrade/guide/ie2000_ug.html

Restrictions for Configuring Layer 2 NAT

- Layer 2 NAT is included in the Enhanced LAN Base feature set, available for Cisco IOS 15.0(2)EB or later.
- Only IPv4 addresses can be translated.
- Layer 2 NAT applies only to unicast traffic. You can permit or allow untranslated unicast traffic, multicast traffic, and IGMP traffic.
- If you configure a translation for an Layer 2 NAT host, do not configure it as a DHCP client.
- Layer 2 NAT is not capable of adjusting application layer headers for FTP. This causes FTP to break.

Guidelines

You need to configure Layer 2 NAT instances that specify the address translations. Then you attach these instances to interfaces and VLANs. For unmatched traffic and traffic types that are not configured to be translated, you can choose to permit or drop the traffic. You can view detailed statistics about the packets sent and received.

- You can configure Layer 2 NAT on the two uplink ports of this switch.
- The downlink port can be VLAN, trunk, or Layer 2channel.
- You can configure 128 Layer 2 NAT instances on the switch.
- You can configure 128 translation entries.
- Up to 128 VLANs are allowed to have Layer 2 NAT configuration.
- Certain protocols such as ARP and ICMP do not work transparently across Layer 2 NAT but are “fixed up” by default.

Information About Configuring Layer 2 NAT

Conceptual Overview

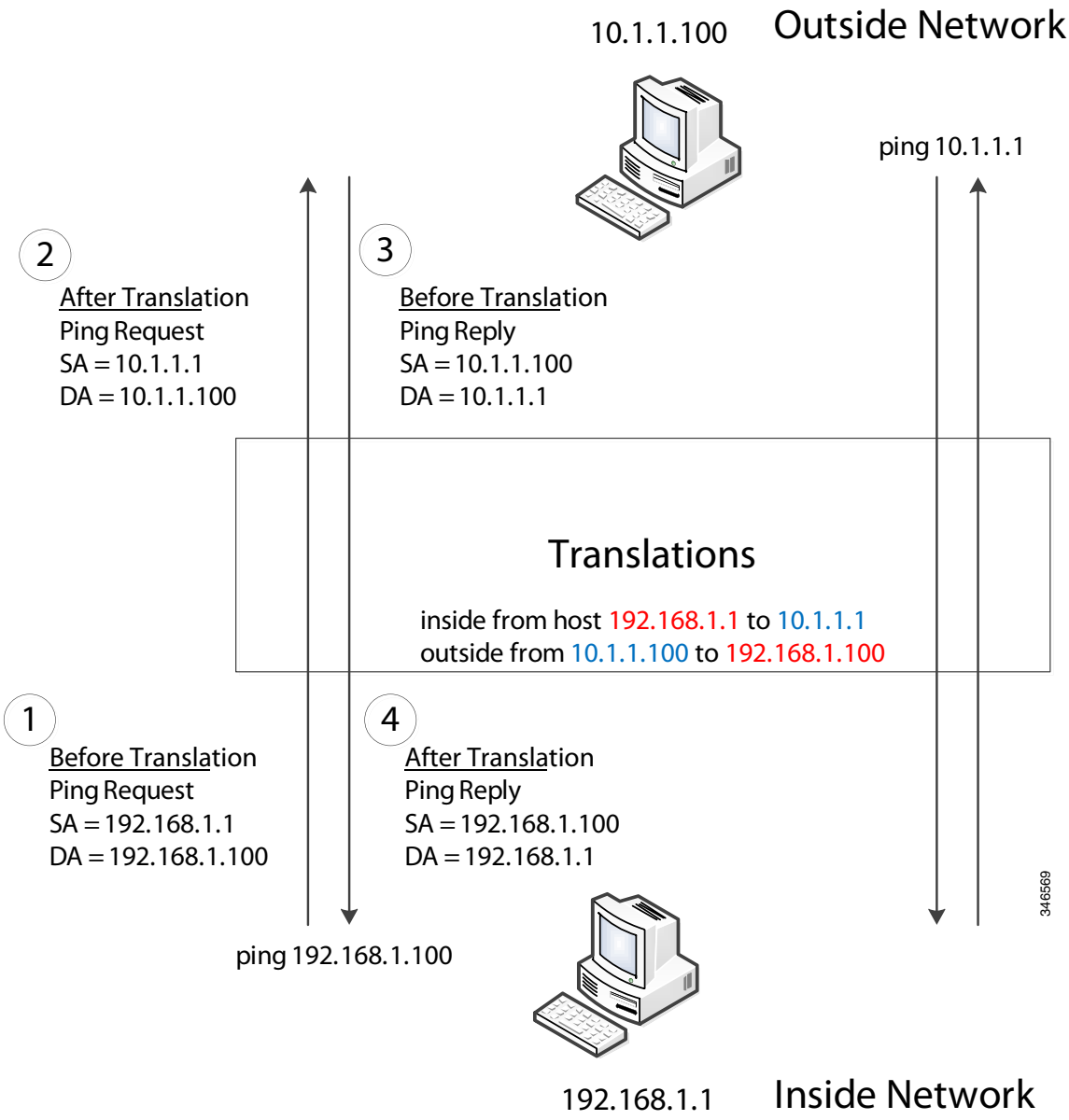
One-to-one (1:1) Layer 2 NAT is a service that allows the assignment of a unique public IP address to an existing private IP address (end device), so that the end device can communicate on both the private and public subnets. This service is configured in a NAT enabled device and is the public “alias” of the IP address physically programmed on the end device. This is typically represented by a table in the NAT device.

Layer 2 NAT has two translation tables where private-to-public and public-to-private subnet translations can be defined. Layer 2 NAT is a hardware based implementation which provides the same high level of (bump-on-the-wire) performance throughout switch loading. This implementation also supports multiple VLAN's through the NAT boundary for enhanced network segmentation. Ring architecture support is built into Layer 2 NAT which allows for redundancy through the NAT boundary.

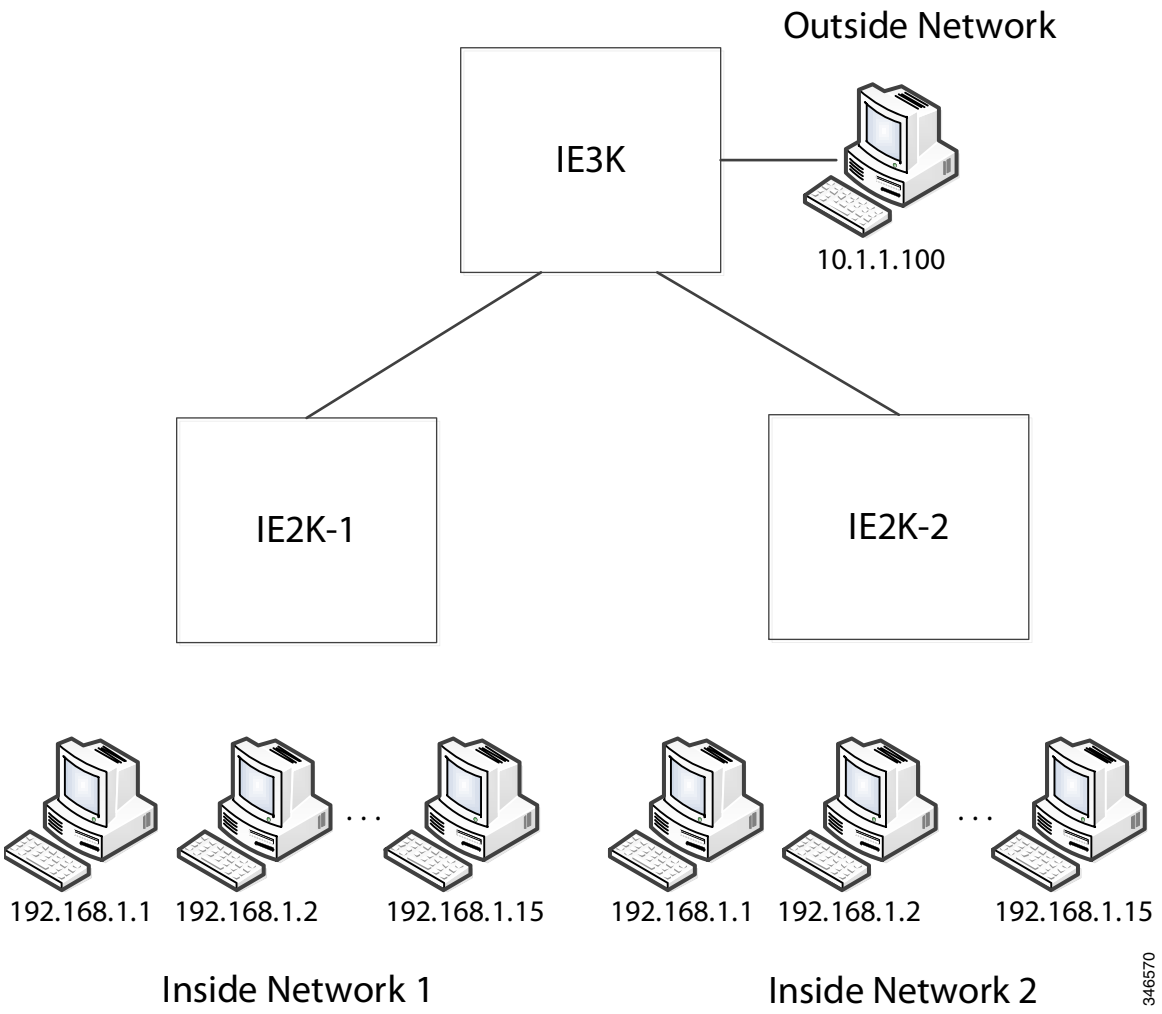
In Figure 46-1 Layer 2 NAT translates addresses between sensors on a 192.168.1.x network and a line controller on a 10.1.1.x network.

1. The sensor at 192.168.1.1 sends a ping request to the line controller by using an "inside" address, 192.168.1.100.
2. Before the packet leaves the internal network, Layer 2 NAT translates the source address to 10.1.1.1 and the destination address to 10.1.1.100.
3. The line controller sends a ping reply to 10.1.1.1.
4. When the packet is received on the internal network, Layer 2 NAT translates the source address to 192.168.1.100 and the destination address to 192.168.1.1.

Figure 46-1 Translating Addresses Between Networks



For large nodes, you can quickly enable translations for all devices in a subnet. In this scenario, addresses from Inside Network 1 can be translated to outside addresses in the 10.1.1.0/28 subnet, and addresses from Inside Network 2 can be translated to outside addresses in the 10.1.1.16/28 subnet. All addresses in each subnet can be translated with one command.



Using the Management Interfaces

The management interface is behind the Layer 2 NAT function. Therefore this interface should not be on the private network VLAN. If it is on the private network VLAN, assign an inside address and configure an inside translation.

How to Configure Layer 2 NAT

Default Layer 2 NAT Settings

Feature	Default Setting
Permit or drop packets for unmatched traffic and traffic types that are not configured to be translated	Drop all unmatched, multicast, and IGMP packets
Protocol fixups	Fix up ARP

Setting Up Layer 2 NAT

To set up Layer 2 NAT, follow these steps. Refer to the examples in this chapter for more details.

	Command	Purpose
Step 1	**configure**	Enters global configuration mode.
Step 2	**l2nat instance** *instance_name*	Creates a new Layer 2 NAT instance. After creating an instance, you use this same command to enter the sub-mode for that instance.
Step 3	**inside from** [*host* | *range* | *network*] *original ip* to *translated ip*[*mask*] *number* | *mask*	Translates an inside address to an outside address. You can translate a single host address, a range of host addresses, or all of the addresses in a subnet. Translates the source address for outbound traffic and the destination address for inbound traffic.
Step 4	**outside from** [*host* | *range* | *network*] *original ip* to *translated ip*[*mask*] *number* | *mask*	Translates an outside address to an inside address. You can translate a single host address, a range of host addresses, or all of the addresses in a subnet. Translates the destination address for outbound traffic and the source address for inbound traffic.
Step 5	**exit**	Exits config-l2nat mode.
Step 6	**interface** *interface-id*	Accesses interface configuration mode for the specified interface (uplink ports only).
Step 7	**l2nat** *instance_name* [*vlan* | *vlan_range*]	Applies the specified Layer 2 NAT instance to a VLAN or VLAN range. If this parameter is missing, the Layer 2 NAT instance applies to the native VLAN.
Step 8	**end**	Exits interface configuration mode.
Step 9	**show l2nat instance** *instance_name*	Shows the configuration details for the specified Layer 2 NAT instance.
Step 10	**show l2nat statistics**	Shows Layer 2 NAT statistics for both uplink ports.
Step 11	**end**	Returns to privileged EXEC mode.

Monitoring the Layer 2 NAT Configuration

Table 46-1 Displaying the Layer 2 NAT Settings

Command	Purpose
show l2nat instance	Displays the configuration details for a specified Layer 2 NAT instance.
show l2nat interface	Displays the configuration details for Layer 2 NAT instances on one or more interfaces.
show l2nat statistics	Displays the Layer 2 NAT statistics for all interfaces.
show l2nat statistics interface	Displays the Layer 2 NAT statistics for a specified interface.

Troubleshooting the Layer 2 NAT Configuration

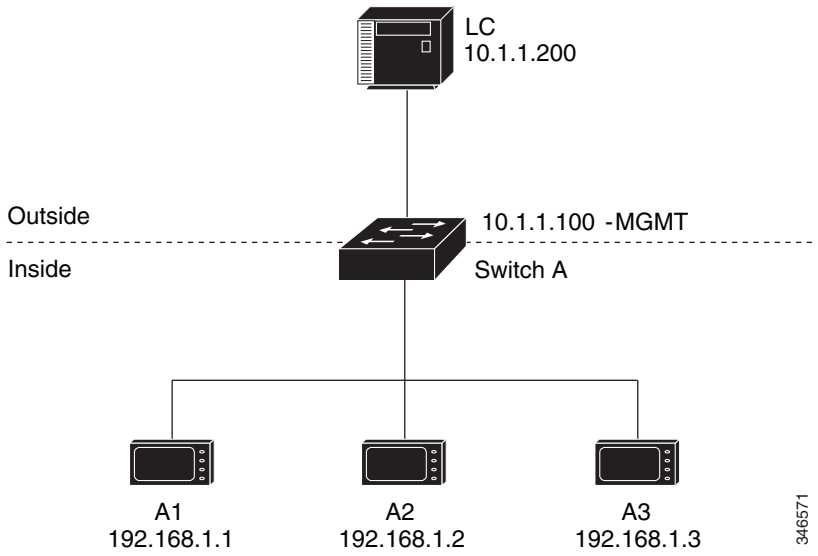
Table 46-2 Troubleshooting the Layer 2 NAT Configuration

Command	Purpose
debug l2nat	Enables showing real-time Layer 2 NAT configuration details when the configuration is applied.

Configuration Examples

Basic Inside-to-Outside Communications Example

Figure 46-2 Basic Inside-to-Outside Communications



In this scenario, A1 needs to communicate with a logic controller LC that is directly connected to the uplink port. An Layer 2 NAT instance is configured to provide an address for A1 on the outside network (10.1.1.1) and an address for the LC on the inside network (192.168.1.250).

Now this communication can occur:

1. A1 sends an ARP request:
   SA: 192.168.1.1
   DA: 192.168.1.250
2. Cisco Switch A fixes up the ARP request:
   SA:10.1.1.1
   DA: 10.1.1.200
3. LC receives the request and learns the MAC Address of 10.1.1.1.
4. LC sends a response:
   SA: 10.1.1.200
   DA: 10.1.1.1
5. Cisco Switch A fixes up the ARP response:
   SA: 192.168.1.250
   DA: 192.168.1.1
6. A1 learns the MAC address for 192.168.1.250, and communication starts.

Note The management interface of the switch must be on a different VLAN from the inside network 192.168.1.x.

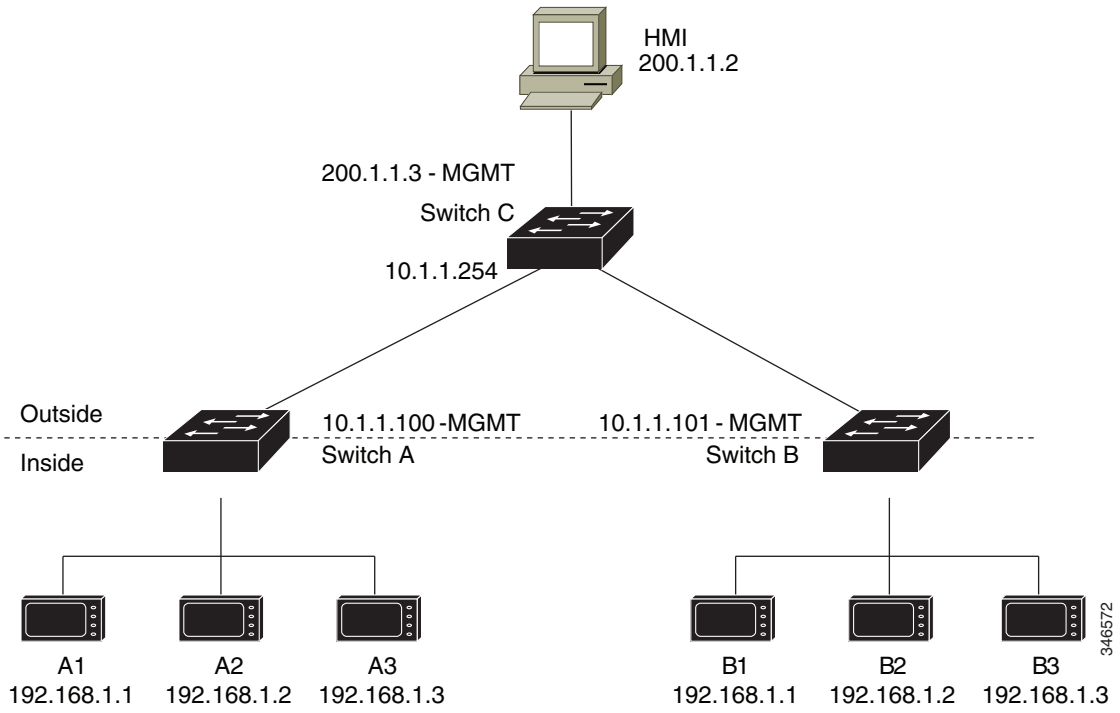
Table 46-2 shows the configuration tasks for this scenario. The Layer 2 NAT instance is created, two translation entries are added, and the instance is applied to the interface. ARP fixups are enabled by default.

Table 46-3 Configuration of Cisco Switch A for Basic Inside-to-Outside Example

	Command	Purpose
Step 1	Switch# **configure**	Enters global configuration mode.
Step 2	Switch(config)# **l2nat instance A-LC**	Creates a new Layer 2 NAT instance called A-LC.
Step 3	Switch(config-l2nat)# **inside from host 192.168.1.1 to 10.1.1.1**	Translates A1's inside address to an outside address.
Step 4	Switch(config-l2nat)# **outside from host 10.1.1.200 to 192.168.1.250**	Translates LC's outside address to an inside address.
Step 5	Switch(config-l2nat)# **exit**	Exits config-l2nat mode.
Step 6	Switch(config)# **interface Gi1/1**	Accesses interface configuration mode for the uplink port.
Step 7	Switch(config-if)# **l2nat A-LC**	Applies this Layer 2 NAT instance to the native VLAN on this interface.
Step 8	Switch# **end**	Returns to privileged EXEC mode.

Duplicate IP Addresses Example

Figure 46-3 Duplicate IP Addresses



In this scenario, two machine nodes are pre-configured with addresses in the 192.168.1.x space. Layer 2 NAT is used to translate these addresses to unique addresses on separate subnets of the outside network. In addition, for machine-to-machine communications, the Node A machines need unique addresses on the Node B space and the Node B machines need unique addresses in the Node A space.

- Switch C needs an address in the 192.168.1.x space. When packets come into Node A or Node B, the 10.1.254 address of Switch C is translated to 192.168.1.254. When packets leave Node A or Node B, the 192.168.1.254 address of Switch C is translated to 10.1.1.254.
- Node A and Node B machines need unique addresses in the 10.1.1.x space. For quick configuration and ease of use, the 10.1.1.x space is divided into subnets: 10.1.1.0, 10.1.1.16, 10.1.1.32, and so on. Each subnet can then be used for a different node. In this example, 10.1.1.16 is used for Node A, and 10.1.1.32 is used for Node B.
- Node A and Node B machines need unique addresses to exchange data. The available addresses are divided into subnets. For convenience, the 10.1.1.16 subnet addresses for the Node A machines are translated to 192.168.1.16 subnet addresses on Node B. The10.1.1.32 subnet addresses for the Node B machines are translated to 192.168.1.32 addresses on Node A.

- Machines have unique addresses on each network:

	Address in Node A	Address in Outside Network	Address in Node B
Switch A network address	192.168.1.0	10.1.1.16	192.168.1.16
A1	192.168.1.1	10.1.1.17	192.168.1.17
A2	192.168.1.2	10.1.1.18	192.168.1.18
A3	192.168.1.3	10.1.1.19	192.168.1.19
Cisco Switch B network address	192.168.1.32	10.1.1.32	192.168.1.0
B1	192.168.1.33	10.1.1.33	192.168.1.1
B2	192.168.1.34	10.1.1.34	192.168.1.2
B3	192.168.1.35	10.1.1.35	192.168.1.3
Switch C	192.168.1.254	10.1.1.254	192.168.1.254

Table 46-4 shows the configuration tasks for Switch A. Table 46-5 shows the configuration tasks for Cisco Switch B.

Table 46-4 Configuration of Switch A for Duplicate Addresses Example

	Command	Purpose
Step 1	Switch# **configure**	Enters global configuration mode.
Step 2	Switch(config)# **l2nat instance A-Subnet**	Creates a new Layer 2 NAT instance called A-Subnet.
Step 3	Switch(config-l2nat)# **inside from network 192.168.1.0 to 10.1.1.16 mask 255.255.255.240**	Translates the Node A machines' inside addresses to addresses in the 10.1.1.16 255.255.255.240 subnet.
Step 4	Switch(config-l2nat)# **outside from host 10.1.1.254 to 192.168.1.254**	Translates the outside address of Switch C to an inside address.
Step 5	Switch(config-l2nat)# **outside from network 10.1.1.32 to 192.168.1.32 255.255.255.240**	Translates the Node B machines' outside addresses to their inside addresses.
Step 6	Switch(config-l2nat)# **exit**	Exits config-l2nat mode.
Step 7	Switch(config)# **interface Gi1/1**	Accesses interface configuration mode for the uplink port.
Step 8	Switch(config-if)# **l2nat A-Subnet**	Applies this Layer 2 NAT instance to the native VLAN on this interface.
Step 9	Switch# **end**	Returns to privileged EXEC mode.

Table 46-5 Configuration of Switch B for Subnet Example

	Command	Purpose
Step 1	Switch# **configure**	Enters global configuration mode.
Step 2	Switch(config)# **l2nat instance B-Subnet**	Creates a new Layer 2 NAT instance called B-Subnet.
Step 3	Switch(config-l2nat)# **inside from network 192.168.1.0 to 10.1.1.32 255.255.255.240**	Translates the Node B machines' inside addresses to addresses in the 10.1.1.32 255.255.255.240 subnet.
Step 4	Switch(config-l2nat)# **outside from host 10.1.1.254 to 192.168.1.254**	Translates the outside address of Switch C to an inside address.
Step 5	Switch(config-l2nat)# **outside from network 10.1.1.16 to 192.168.1.16 255.255.255.240**	Translates the Node A machines' outside addresses to their inside addresses.
Step 6	Switch(config-l2nat)# **outside from network 10.1.1.32 to 192.168.1.0 255.255.255.240**	Translates the Node B machines' outside addresses to their inside addresses.
Step 7	Switch(config-l2nat)# **exit**	Exits config-l2nat mode.
Step 8	Switch(config)# **interface Gi1/1**	Accesses interface configuration mode for the uplink port.
Step 9	Switch(config-if)# **l2nat name1**	Applies this Layer 2 NAT instance to the native VLAN on this interface.
Step 10	Switch# **show l2nat instance name1**	Shows the configuration details for the specified Layer 2 NAT instance.
Step 11	Switch# **show l2nat statistics**	Shows Layer 2 NAT statistics.
Step 12	Switch# **end**	Returns to privileged EXEC mode.

Additional References

The following sections provide references related to switch administration:

Related Documents

Related Topic	Document Title
Cisco IOS commands for this switch	*Cisco IE2000 Switch Series Command Reference*
Cisco IOS basic commands	*Cisco IOS Configuration Fundamentals Command Reference*
License Upgrade Instructions	*Software Activation Licensing Upgrade Instructions for the Cisco IE2000 Switch Series*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport