Configuring Layer 2 NAT

Layer 2 Network Address Translation

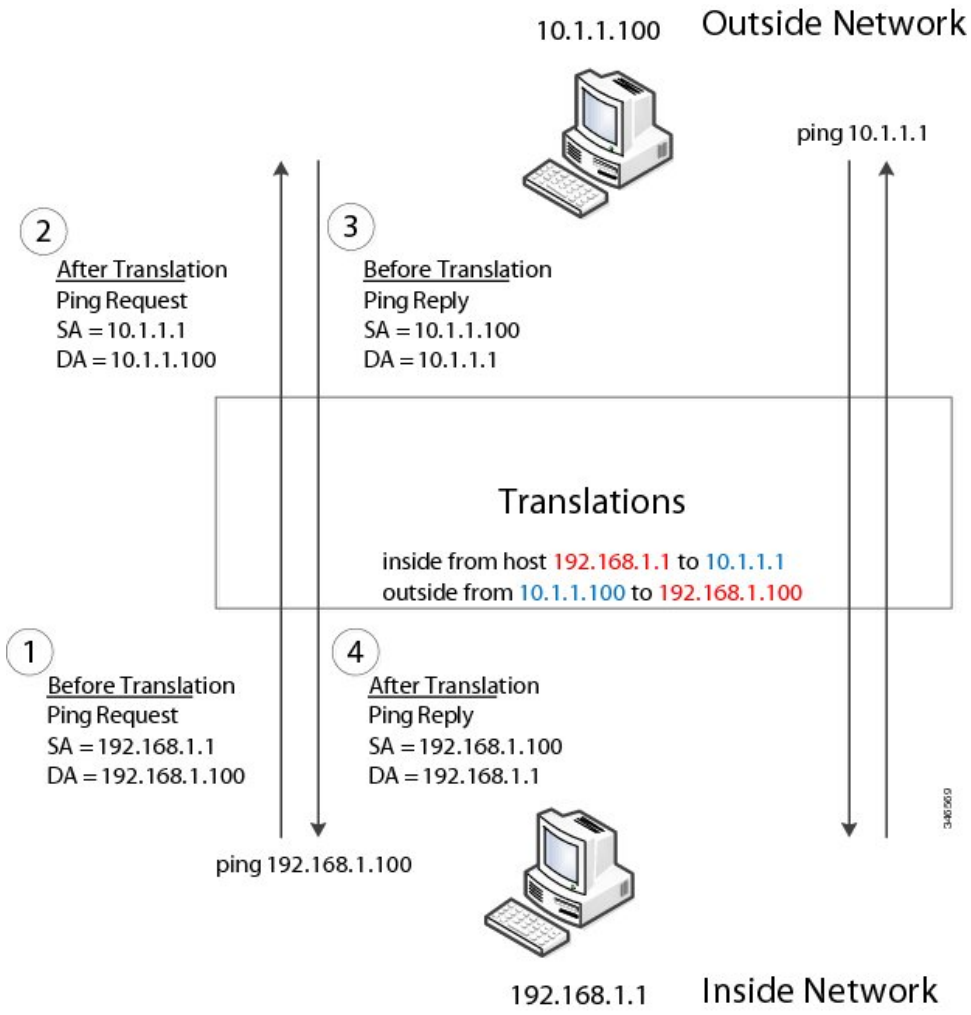
One-to-one (1:1) Layer 2 Network Address Translation (NAT) is a service that allows the assignment of a unique public IP address to an existing private IP address (end device). The assignment enables the end device to communicate on both the private and public subnets. This service is configured in a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

Layer 2 NAT uses a table to translate IPv4 addresses both public-to-private, and private-to-public at line rate. Layer 2 NAT is a hardware-based implementation that provides the same high level of (bump-on-the-wire) wire-speed performance. This implementation also supports multiple VLANs through the NAT boundary for enhanced network segmentation.

In the following example, 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.

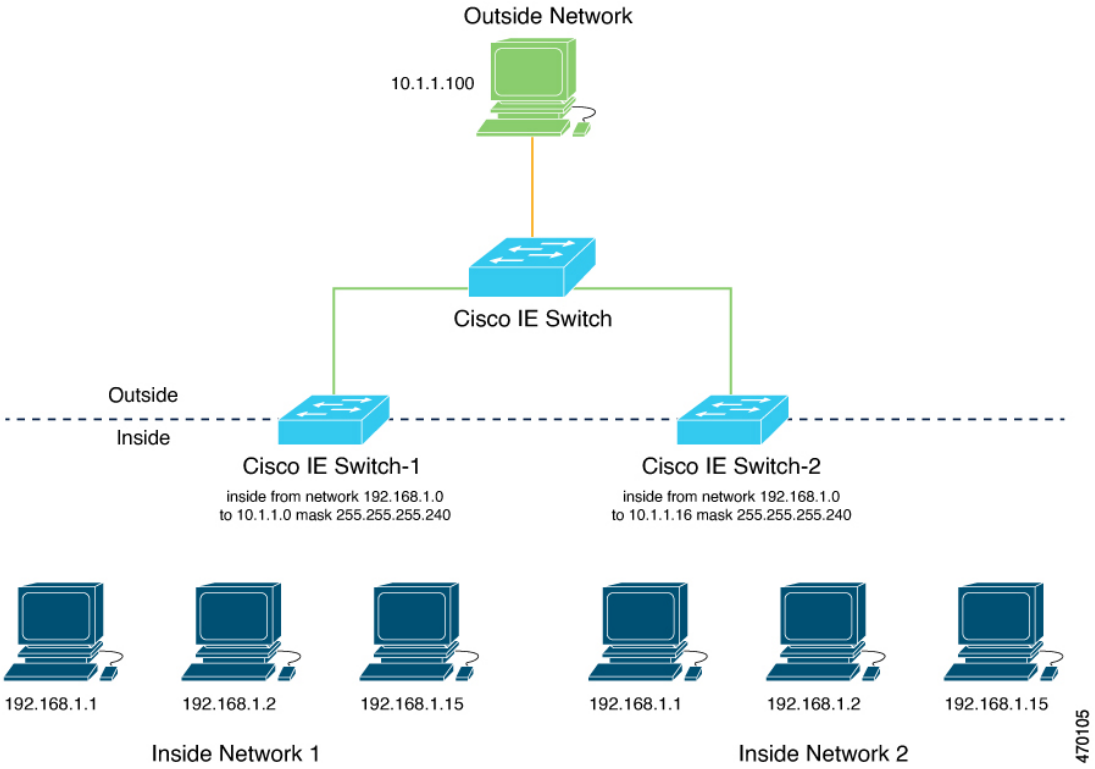
1. The 192.168.1.x network is the inside/internal IP address space and the 10.1.1.x network is the outside or external IP address space.
2. The sensor at 192.168.1.1 sends a ping request to the line controller by using an “inside” address, 192.168.1.100.
3. Before the packet leaves the internal network, Layer 2 NAT translates the source address (SA) to 10.1.1.1 and the destination address (DA) to 10.1.1.100.
4. The line controller sends a ping reply to 10.1.1.1.
5. 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 1: Translating Addresses Between Networks



For large numbers of nodes, you can quickly enable translations for all devices in a subnet. In the scenario shown in the following figure, 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. The benefit of using subnet-based translations saves in Layer L2 NAT rules. The switch has limits on the number of Layer 2 NAT rules. A rule with a subnet allows for multiple end devices to be translated with a single rule.

Figure 2: Inside-Outside Address Translation



The following figure shows a Cisco Catalyst IE3400 Rugged Series Switch at the aggregation layer forwarding Ethernet packets based on Layer 2 MAC Addresses. In this example, the router is the Layer 3 gateway for all subnets and VLANs.

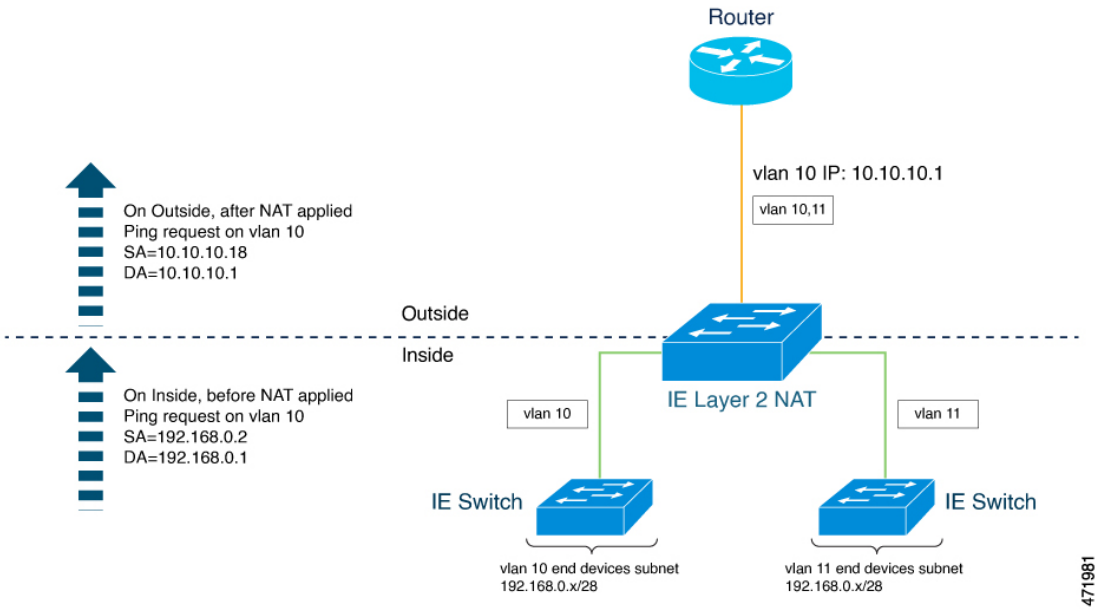
The L2NAT instance definitions use the `network` command to define a translation row for multiple devices in the same subnet. In this the case it's a /28 subnet. With this subnet mask, the last nibble in 4th byte of the inside IP address will not change. The last byte will be in range 16 – 31 because the translated IP address is 10.10.10.16.

The gateway for the VLAN is the router with the last byte of the IP address ending with .1. An outside host translation is provided for the gateway router. The `network` command in the Layer 2 NAT definition translates a subnet's worth of host with a single command, saving on Layer 2 NAT translation rules.

The Gi1/1 uplink interface has two Layer 2 NAT translation instances for vlan 10 and vlan 11 subnets. Interfaces can support multiple Layer 2 NAT instance definitions.

The downstream IE switches are examples of access layer switches that do not perform Layer 2 NAT and rely on the upstream aggregation layer switch to do it.

Figure 3: NAT on the IE3400 Switch



The IE3400 NAT configuration for the diagram shown in the preceding figure is as follows:

```
!
l2nat instance Subnet10-NAT
 instance-id 1
 permit all
 fixup all
 outside from host 10.10.10.1 to 192.168.0.1
 inside from network 192.168.0.0 to 10.10.10.16 mask 255.255.255.240
!
l2nat instance Subnet11-NAT
 instance-id 1
 permit all
 fixup all
 outside from host 10.10.11.1 to 192.168.0.1
 inside from network 192.168.0.0 to 10.10.11.16 mask 255.255.255.240
!
interface GigabitEthernet1/1
 switchport mode trunk
 l2nat Subnet10-NAT 10
 l2nat Subnet11-NAT 11
!
Interface vlan 1
  ip address 10.10.1.2
```

Layer 2 NAT Switch Support

- IE3105: Layer 2 NAT feature is supported only on uplink ports (Gig 1/1 and Gig 1/2) and available in both (essential and advantage) licenses.
- IE3300: Layer 2 NAT feature is supported only on uplink ports (Gig 1/1 and Gig 1/2) and available in both (essential and advantage) licenses.

- IE3400: Layer 2 NAT feature is supported only on uplink ports (Gig 1/1 and Gig 1/2) and available in both (essential and advantage) licenses.

Guidelines and Limitations

- 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.
- Layer 2 NAT does not support one-to-many and many-to-one IP address mapping.
- Layer 2 NAT supports one-to-one mapping between external and internal IP addresses.
- Layer 2 NAT cannot save on public IP addresses.
- If you configure a translation for a Layer 2 NAT host, do not configure it as a DHCP client.
- Certain protocols such as ARP and ICMP do not work transparently across Layer 2 NAT but are "fixed up" by default. "Fixed up" means that changes are made to IP addresses embedded in the payload of IP packets for the protocols to work.
- The downlink port can be VLAN, trunk, or Layer 2 channel.
- You can configure 128 Layer 2 NAT rules on the switch.
- Up to 128 VLANs are allowed to have Layer 2 NAT configuration.
- 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.
- Because L2NAT is designed to separate outside and inside addresses, we recommend that you do not configure addresses of the same subnet as both outside and inside addresses.
- The interfaces that support NAT instance configurations are Gig 1/1 and Gig 1/2 (uplinks).

Default 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	Fixup is enabled for ARP and ICMP.

Note In the preceding table, *unmatched* refers to any host without an IP address defined for translation as a rule in the Layer 2 NAT instance that is applied to the interface.

Configuring Layer 2 NAT

You need to configure Layer 2 NAT instances that specify the address translations. You then attach these rules to uplink interfaces. For unmatched traffic and traffic types that are not configured to be translated, you can choose to permit or drop the traffic. The IE switch management interface is behind the management interfaces (CLI/SNMP/CIP/WebUI). You can view detailed statistics about the packets sent and received (see Verifying Configuration , on page 7).

To configure Layer 2 NAT, follow these steps. Refer to the examples in Basic Inside-to-Outside Communications Example, on page 7 and Duplicate IP Addresses Example, on page 9 for more details.

Step 1 Enter global configuration mode:

configure terminal

Step 2 Create a new Layer 2 NAT instance:

l2nat instance *instance_name*

After creating an instance, you use this same command to enter the sub-mode for that instance.

Step 3 Translate an inside address to an outside address:

inside from [*host* | *range* | *network*] *original ip* to *translated ip* [*mask*] *number* | *mask*

You can translate a single host address, a range of host addresses, or all of the addresses in a subnet. Translate the source address for outbound traffic and the destination address for inbound traffic. Use the `inside from` command when the host or hosts are physically present on the inside and have private IP addresses.

Step 4 Translate an outside address to an inside address:

outside from [*host* | *range* | *network*] *original ip* to *translated ip* [*mask*] *number* | *mask*

You can translate a single host address, a range of host addresses, or all of the addresses in a subnet. Translate the destination address for outbound traffic and the source address for inbound traffic. Use the `outside from` command when the host or hosts are physically present on the outside and have public IP addresses.

Step 5 Fix the translation for ICMP and IGMP through NAT translation. By default, fixups for both ARP and ICMP are enabled, so this command is not normally needed unless you change the defaults.

fixup arp | icmp | all

Note For ICMP, only fixups for ICMP Error messages are supported.

Step 6 (Optional) Permit untranslated unicast traffic (it is dropped by default):

permit { **multicast** | **igmp** | **all** }

Step 7 Exit config-l2nat mode:

exit

Step 8 Access interface configuration mode for the specified interface (gi1/1 and gi1/2 for IE3105, IE3300, and IE3400):

interface *interface-id*

Step 9 Apply 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.

l2nat *instance_name* [*vlan* | *vlan_range*]

Step 10 Exit interface configuration mode:

end

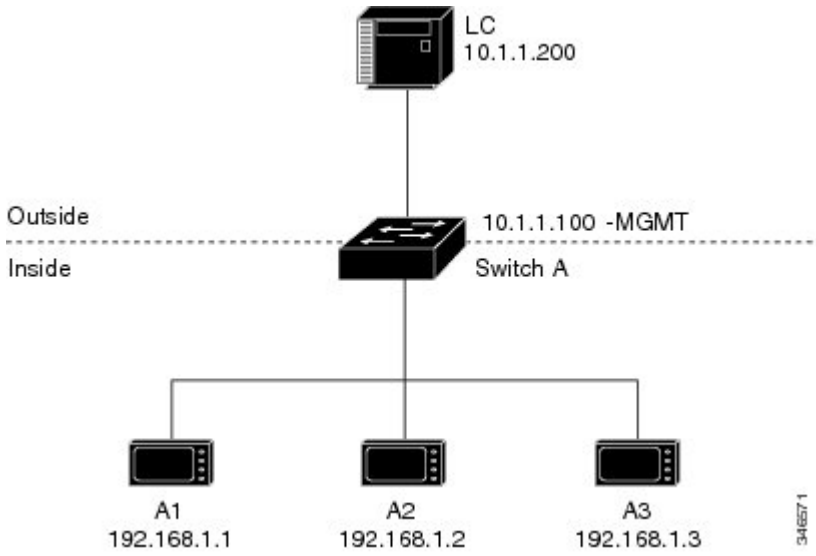
Verifying Configuration

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

Basic Inside-to-Outside Communications Example

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).

Figure 4: Basic Inside-to-Outside Communications



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 It is a good practice to put the management interface of the switch on a different VLAN from the inside network 192.168.1.x.

The following table 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 1: Configuration of Cisco Switch A for Basic Inside-to-Outside Example

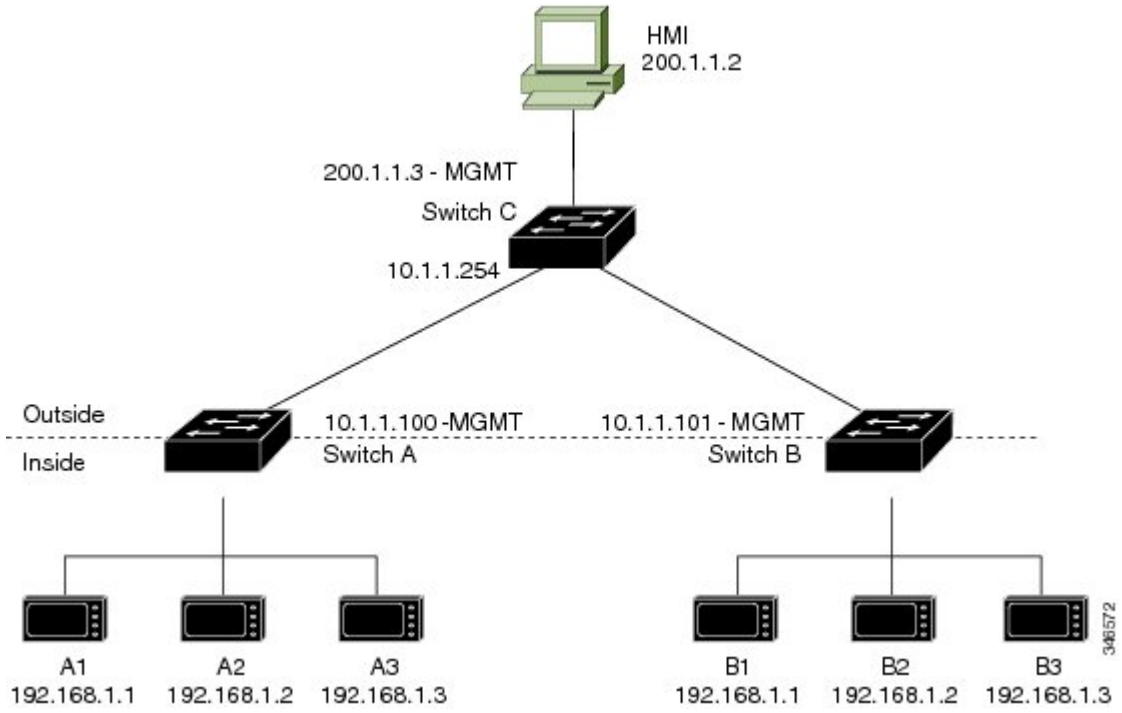
	Command	Purpose
1.	Switch# **configure**	Enters global configuration mode.
2.	Switch(config)# **l2nat instance A-LC**	Creates a new Layer 2 NAT instance called A-LC.
3.	Switch(config-l2nat)# **inside from host 192.168.1.1 to 10.1.1.1**	Translates A1's inside address to an outside address.
4.	Switch(config-l2nat)# **inside from host 192.168.1.2 to 10.1.1.2**	Translates A2's inside address to an outside address.

	Command	Purpose
5.	Switch(config-l2nat)# **inside from host 192.168.1.3 to 10.1.1.3**	Translates A3's inside address to an outside address.
6.	Switch(config-l2nat)# **outside from host 10.1.1.200 to 192.168.1.250**	Translates LC's outside address to an inside address.
7.	Switch(config-l2nat)# **exit**	Exits config-l2nat mode.
8.	Switch(config)# **interface Gi1/1**	Accesses interface configuration mode for the uplink port.
9.	Switch(config-if)# **l2nat A-LC**	Applies this Layer 2 NAT instance to the native VLAN on this interface. **Note** For tagged traffic on a trunk, add the VLAN number when attaching the instance to an interface as follows: l2nat *instance vlan*
10.	Switch# **end**	Returns to privileged EXEC mode.

Duplicate IP Addresses Example

In this scenario, two machine nodes are preconfigured with addresses in the 192.168.1.x space. Layer 2 NAT translates 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.

Figure 5: Duplicate IP Addresses



- For switch C to act as a gateway for the private network, Switch C needs an address in the 192.168.1.x space. When packets come into Node A or Node B, the 10.1.1.254 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:

Table 2: Translated IP Addresses

Node	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

Node	Address in Node A	Address in Outside Network	Address in Node B
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 3: Configuration of Switch A for Duplicate Addresses Example, on page 11 shows the configuration tasks for Switch A. Table 4: Configuration of Switch B for Subnet Example, on page 12 shows the configuration tasks for Switch B.

Note This example is based on the IE 2000 switch. For the IE3x00 and ESS3300 switches, the interface numbers may vary.

Table 3: Configuration of Switch A for Duplicate Addresses Example

	Command	Purpose
1	Switch# **configure**	Enters global configuration mode.
2	Switch(config)# **l2nat instance A-Subnet**	Creates a new Layer 2 NAT instance called A-Subnet.
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.
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.
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.
6	Switch(config-l2nat)# **exit**	Exits config-l2nat mode.
7	Switch(config)# **interface Gi1/1**	Accesses interface configuration mode for the uplink port.
8	Switch(config-if)# **l2nat A-Subnet**	Applies this Layer 2 NAT instance to the native VLAN on this interface. **Note** For tagged traffic on a trunk, add the VLAN number when attaching the instance to an interface as follows: l2nat *instance vlan*
9	Switch# **end**	Returns to privileged EXEC mode.

Table 4: Configuration of Switch B for Subnet Example

	Command	Purpose
1.	Switch# **configure**	Enters global configuration mode.
2.	Switch(config)# **l2nat instance B-Subnet**	Creates a new Layer 2 NAT instance called B-Subnet.
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.
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.
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.
6.	Switch(config-l2nat)# **exit**	Exits config-l2nat mode.
7.	Switch(config)# **interface Gi1/1**	Accesses interface configuration mode for the uplink port.
8.	Switch(config-if)# **l2nat B-Subnet**	Applies this Layer 2 NAT instance to the native VLAN on this interface. **Note** For tagged traffic on a trunk, add the VLAN number when attaching the instance to an interface as follows: l2nat *instance vlan*
9.	Switch# **show l2nat instance name1**	Shows the configuration details for the specified Layer 2 NAT instance.
10.	Switch# **show l2nat statistics**	Shows Layer 2 NAT statistics.
11.	Switch# **end**	Returns to privileged EXEC mode.