



# NAT - Static IP Support

---

The NAT - Static IP Support feature provides support for users with static IP addresses, enabling those users to establish an IP session in a Public Wireless LAN environment.

## Feature History for NAT - Static IP Support

Release	Modification
12.3(2)XE	This feature was introduced.
12.3(7)T	This feature was integrated into Cisco IOS Software Release 12.3(7)T.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for NAT - Static IP Support, page 1](#)
- [Information About NAT - Static IP Support, page 2](#)
- [How to Configure NAT - Static IP Support, page 2](#)
- [Configuration Examples for NAT - Static IP Support, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)

## Prerequisites for NAT - Static IP Support

Before enabling static IP support for Network Address Translation (NAT), you must first enable NAT on your router and configure a RADUIS server host. For additional information on NAT and RADUIS configuration, see the “[Related Documents](#)” section on [page 6](#).



---

**Corporate Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003–2004 Cisco Systems, Inc. All rights reserved.

# Information About NAT - Static IP Support

To configure the NAT - Static IP Support feature, you should understand the following concepts:

- [Benefits of NAT - Static IP Support, page 2](#)
- [Public Wireless LAN, page 2](#)
- [RADIUS, page 2](#)

## Benefits of NAT - Static IP Support

The NAT - Static IP Support feature extends the capabilities of Public Wireless LAN providers to support users configured with a static IP address. By configuring a router to support users with a static IP address, Public Wireless LAN providers extend their services to a greater number of potential users, which can lead to greater user satisfaction and additional revenue.

## Public Wireless LAN

A Public Wireless LAN provides users of mobile computing devices with wireless connections to a public network, such as the Internet.

## RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that secures networks against unauthorized access. Communication between a network access server (NAS) and a RADIUS server is based on the User Datagram Protocol (UDP). Generally, the RADIUS protocol is considered a connectionless service. Issues related to server availability, retransmission, and timeouts are handled by the RADIUS-enabled devices rather than the transmission protocol.

RADIUS is a client/server protocol. The RADIUS client is typically a NAS, and the RADIUS server is usually a daemon process running on a UNIX or Windows NT machine. The client passes user information to designated RADIUS servers and acts on the response that is returned. RADIUS servers receive user connection requests, authenticate the user, and then return the configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

## How to Configure NAT - Static IP Support

This section contains the following procedures:

- [Configuring Static IP Support, page 3](#) (required)
- [Verifying Static IP Support, page 4](#) (optional)

## Configuring Static IP Support

To configure the NAT - Static IP Support feature, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip nat inside**
5. **exit**
6. **ip nat allow-static-host**
7. **ip nat pool** *name start-ip end-ip netmask netmask accounting list-name*
8. **ip nat inside source list** *access-list-number pool name*
9. **access-list** *access-list-number deny ip source*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface ethernet 1	Specifies the interface to be configured, and enters interface configuration mode.
Step 4	<b>ip nat inside</b>  <b>Example:</b> Router(config-if)# ip nat inside	Marks the interface as connected to the inside.
Step 5	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 6	<b>ip nat allow-static-host</b>  <b>Example:</b> Router(config)# ip nat allow-static-host	Enables static IP address support. <ul style="list-style-type: none"><li>• Dynamic Address Resolution Protocol (ARP) learning will be disabled on this interface, and NAT will control the creation and deletion of ARP entries for the static-IP host.</li></ul>

	Command or Action	Purpose
Step 7	<pre>ip nat pool name start-ip end-ip netmask netmask accounting list-name</pre> <p><b>Example:</b> Router(config)# ip nat pool xyz 171.1.1.1 171.1.1.10 netmask 255.255.255.0 accounting WLAN-ACCT</p>	Specifies an existing RADUIS profile name to be used for authentication of the static IP host.
Step 8	<pre>ip nat inside source list access-list-number pool name</pre> <p><b>Example:</b> Router(config)# ip nat inside source list 1 pool net-208</p>	Specifies the access list and pool to be used for static IP support. <ul style="list-style-type: none"> <li>The specified access list must permit all traffic.</li> </ul>
Step 9	<pre>access-list access-list-number deny ip source</pre> <p><b>Example:</b> Router(config) # access-list 1 deny ip 192.168.196.51</p>	Removes the router's own traffic from NAT translation. <ul style="list-style-type: none"> <li>The <i>source</i> argument is the IP address of the router that supports the NAT - Static IP Support feature.</li> </ul>

## Verifying Static IP Support

To verify the NAT - Static IP Support feature, perform the following steps.

### SUMMARY STEPS

1. show ip nat translations verbose

### DETAILED STEPS

#### Step 1 show ip nat translations verbose

Use this command to verify that NAT is configured to support static IP addresses, for example:

```
Router# show ip nat translations verbose
```

```
--- 171.1.1.11          10.1.1.1          ---          ---
create 00:05:59, use 00:03:39, left 23:56:20, Map-Id(In): 1, flags: none wlan-flags:
Secure ARP added, Accounting Start sent Mac-Address:0010.7bc2.9ff6 Input-IDB:Ethernet1/2,
use_count: 0, entry-id:7, lc_entries: 0
```

# Configuration Examples for NAT - Static IP Support

This section provides the following configuration examples:

- [Configuring NAT - Static IP Support: Example, page 5](#)
- [Creating a RADIUS Profile for NAT - Static IP Support: Example, page 5](#)

## Configuring NAT - Static IP Support: Example

The following example enables static IP address support for the router at 192.168.196.51:

```
interface ethernet 1
 ip nat inside
 ip nat allow-static-host
 ip nat pool xyz 171.1.1.1 171.1.1.10 netmask 255.255.255.0 accounting WLAN-ACCT
 ip nat inside source list 1 pool net-208
 access-list 1 deny ip 192.168.196.51
```

## Creating a RADIUS Profile for NAT - Static IP Support: Example

The following example shows how create a RADIUS profile for use with the NAT - Static IP Support feature.

```
aaa new-model
!
!
aaa group server radius WLAN-RADIUS
 server 168.58.88.1 auth-port 1645 acct-port 1645
 server 168.58.88.1 auth-port 1645 acct-port 1646
!
aaa accounting network WLAN-ACCT start-stop group WLAN-RADIUS
aaa session-id common
ip radius source-interface Ethernet3/0
radius-server host 168.58.88.1 auth-port 1645 acct-port 1646
radius-server key cisco
```

## Additional References

The following sections provide references related to the NAT - Static IP Support feature.

### Related Documents

Related Topic	Document Title
Configuring Network Address Translation (NAT)	<i>Cisco IOS IP Configuration Guide</i>
IP NAT translation	<i>Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services</i> , Release 12.3(4)T
Public Wireless LAN access routers	<i>PWLAN Access Routers for Cisco IOS Release 12.3(4)XD</i>
RADIUS	<i>Cisco IOS Security Command Reference</i> , Release 12.3(4)T
SSG	<i>Service Selection Gateway</i> , Release 12.3(4)T

### 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
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFCs	Title
RFC 2663	<i>IP Network Address Translator (NAT) Terminology and Considerations</i>
RFC 3022	<i>Traditional IP Network Address Translator (Traditional NAT)</i>

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 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.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

This section documents only modified commands.

### Modified Commands

- [debug ip nat](#)
- [ip nat](#)
- [ip nat pool](#)

# debug ip nat

To display information about IP packets translated by the IP Network Address Translation (NAT) feature, use the **debug ip nat** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

**debug ip nat** [*access-list* | **detailed** | **h323** | **ipsec** | **port** | **pptp** | **route** | **sip** | **skinny** | **vrf** | **wlan-nat**]

**no debug ip nat** [*access-list* | **detailed** | **h323** | **ipsec** | **port** | **pptp** | **route** | **sip** | **skinny** | **vrf** | **wlan-nat**]

## Syntax Description

<i>access-list</i>	(Optional) Standard IP access list number. If the datagram is not permitted by the specified access list, the related debugging output is suppressed.
<b>detailed</b>	(Optional) Displays debug information in a detailed format.
<b>h323</b>	(Optional) Displays H.225 and H.245 protocol information.
<b>ipsec</b>	(Optional) Displays IP Security (IPSec) packet information.
<b>port</b>	(Optional) Displays port information.
<b>pptp</b>	(Optional) Displays Point-to-Point Tunneling Protocol (PPTP) information.
<b>route</b>	(Optional) Displays route information.
<b>sip</b>	(Optional) Displays Session Initiation Protocol (SIP) information.
<b>skinny</b>	(Optional) Displays debug information in a concise format.
<b>vrf</b>	(Optional) Displays Virtual Private Network (VPN) routing and forwarding (VRF) traffic-related information.
<b>wlan-nat</b>	(Optional) Displays Wireless LAN information.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
11.2	This command was introduced.
12.1(5)T	The <b>h323</b> keyword was added.
12.2(8)T	The <b>sip</b> keyword was added.
12.2(13)T	The <b>ipsec</b> and <b>vrf</b> keywords were added.
12.3(2)XE	The <b>wlan-nat</b> keyword was added.
12.3(7)T	This command was implemented in Cisco IOS Release 12.3(7)T.

## Usage Guidelines

The NAT feature reduces the need for unique, registered IP addresses. It can also save private network administrators from needing to renumber hosts and routers that do not conform to global IP addressing.

Use the **debug ip nat** command to verify the operation of the NAT feature by displaying information about every packet that is translated by the router. The **debug ip nat detailed** command generates a description of each packet considered for translation. This command also displays information about certain errors or exceptional conditions, such as the failure to allocate a global address. To display messages related to the processing of H.225 signaling and H.245 messages, use the **debug ip nat h323**

command. To display messages related to the processing of SIP messages, use the **debug ip nat sip** command. To display messages related to the processing of VRF messages, use the **debug ip nat vrf** command.


**Caution**

Because the **debug ip nat** command generates a substantial amount of output, use it only when traffic on the IP network is low, so that other activity on the system is not adversely affected.

**Examples**

The following is sample output from the **debug ip nat** command. In this example, the first two lines show the debugging output produced by a Domain Name System (DNS) request and reply. The remaining lines show the debugging output from a Telnet connection from a host on the inside of the network to a host on the outside of the network. All Telnet packets, except for the first packet, were translated in the fast path, as indicated by the asterisk (\*).

```
Router# debug ip nat

NAT: s=192.168.1.95->172.31.233.209, d=172.31.2.132 [6825]
NAT: s=172.31.2.132, d=172.31.233.209->192.168.1.95 [21852]
NAT: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6826]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23311]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6827]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6828]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23313]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23325]
```

Table 1 describes the significant fields shown in the display.

**Table 1** *debug ip nat Field Descriptions*

Field	Description
NAT	Indicates that the packet is being translated by the NAT feature. An asterisk (*) indicates that the translation is occurring in the fast path. The first packet in a conversation always goes through the slow path (that is, it is process switched). The remaining packets go through the fast path if a cache entry exists.
s=192.168.1.95->172.31.233.209	Source address of the packet and how it is being translated.
d=172.31.2.132	Destination address of the packet.
[6825]	IP identification number of the packet. Might be useful in the debugging process to correlate with other packet traces from protocol analyzers.

The following is sample output from the **debug ip nat detailed** command. In this example, the first two lines show the debugging output produced by a DNS request and reply. The remaining lines show the debugging output from a Telnet connection from a host on the inside of the network to a host on the outside of the network. In this example, the inside host 192.168.1.95 was assigned the global address 172.31.233.193.

```
Router# debug ip nat detailed

NAT: i: udp (192.168.1.95, 1493) -> (172.31.2.132, 53) [22399]
NAT: o: udp (172.31.2.132, 53) -> (172.31.233.193, 1493) [63671]
NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22400]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22002]
```

```

NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22401]
NAT*: i: tcp (192.168.1.95, 1135) -> (172.31.2.75, 23) [22402]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22060]
NAT*: o: tcp (172.31.2.75, 23) -> (172.31.233.193, 1135) [22071]

```

The following is sample output from the **debug ip nat h323** command. In this example, an H.323 call is established between two hosts, one host on the inside and the other host on the outside. The debug displays the H.323 messages names that NAT recognizes and the embedded IP addresses contained in those messages.

```

Router# debug ip nat h323

NAT:H225:[0] processing a Setup message
NAT:H225:[0] found Setup sourceCallSignalling
NAT:H225:[0] fix TransportAddress addr=192.168.122.50 port=11140
NAT:H225:[0] found Setup fastStart
NAT:H225:[0] Setup fastStart PDU length:18
NAT:H245:[0] processing OpenLogicalChannel message, forward channel
number 1
NAT:H245:[0] found OLC forward mediaControlChannel
NAT:H245:[0] fix TransportAddress addr=192.168.122.50 port=16517
NAT:H225:[0] Setup fastStart PDU length:29
NAT:H245:[0] processing OpenLogicalChannel message, forward channel
number 1
NAT:H245:[0] found OLC reverse mediaChannel
NAT:H245:[0] fix TransportAddress addr=192.168.122.50 port=16516
NAT:H245:[0] found OLC reverse mediaControlChannel
NAT:H245:[0] fix TransportAddress addr=192.168.122.50 port=16517
NAT:H225:[1] processing an Alerting message
NAT:H225:[1] found Alerting fastStart
NAT:H225:[1] Alerting fastStart PDU length:25
NAT:H245:[1] processing OpenLogicalChannel message, forward channel

```

Table 2 describes the significant fields shown in the display.

**Table 2** *debug ip nat h323 Field Descriptions*

Field	Description
NAT	Indicates that the packet is being translated by the NAT feature.
H.225 and H.245	Protocol of the packet.
[0]	Indicates that the packet is moving from a host outside the network to one host inside the network.
[1]	Indicates that the packet is moving from a host inside the network to one host outside the network.

The following is sample output from the **debug ip nat ipsec** command:

```

Router# debug ip nat ipsec

5d21h:NAT:new IKE going In->Out, source addr 192.168.122.35, destination addr
192.168.22.20, initiator cookie
0x9C42065D
5d21h:NAT:IPSec:created In->Out ESP translation IL=192.168.122.35 SPI=0xA64B5BB6,
IG=192.168.22.40, OL=192.168.22.20,
OG=192.168.22.20
5d21h:NAT:IPSec:created Out->In ESP translation OG=192.168.22.20 SPI=0xA64B5BB6,
OL=192.168.22.20, IG=192.168.22.40,
IL=192.168.122.35

```

```

5d21h:NAT:new IKE going In->Out, source addr 192.168.122.20, destination addr
192.168.22.20, initiator cookie
0xC91738FF
5d21h:NAT:IPSec:created In->Out ESP translation IL=192.168.122.20 SPI=0x3E2E1B92,
IG=192.168.22.40, OL=192.168.22.20,
OG=192.168.22.20
5d21h:NAT:IPSec:Inside host (IL=192.168.122.20) trying to open an ESP connection to
Outside host (OG=192.168.22.20),
wait for Out->In reply
5d21h:NAT:IPSec:created Out->In ESP translation OG=192.168.22.20 SPI=0x1B201366,
OL=192.168.22.20, IG=192.168.22.40,
IL=192.168.122.20

```

The following is sample output from the **debug ip nat sip** command. In this example, one IP phone registers with a Cisco SIP proxy and then calls another IP phone. The debug output displays the SIP messages that NAT recognizes and the embedded IP addresses contained in those messages.

```
Router# debug ip nat sip
```

```

NAT:SIP:[0] processing REGISTER message
NAT:SIP:[0] translated embedded address
192.168.122.3->2.2.2.2
NAT:SIP:[0] translated embedded address
192.168.122.3->2.2.2.2
NAT:SIP:[0] message body found
NAT:SIP:[0] found address/port in SDP body:192.168.122.20
20332
NAT:SIP:[1] processing SIP/2.0 100 Trying reply message
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] processing SIP/2.0 200 OK reply message
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] processing INVITE message
NAT:SIP:[1] translated embedded address
2.2.2.2->192.168.122.3
NAT:SIP:[1] message body found
NAT:SIP:[1] found address/port in SDP body:192.168.22.20

```

Table 3 describes the significant fields shown in the display.

**Table 3** *debug ip nat sip* Field Descriptions

Field	Description
NAT	Indicates that the packet is being translated by the NAT feature.
SIP	Protocol of the packet.
[0]	Indicates that the packet is moving from a host outside the network to one host inside the network.
[1]	Indicates that the packet is moving from a host inside the network to one host outside the network.

The following is sample output from the **debug ip nat vrf** command:

```
Router# debug ip nat vrf

6d00h:NAT:address not stolen for 192.168.121.113, proto 1 port 7224
6d00h:NAT:creating portlist proto 1 globaladdr 2.2.2.10
6d00h:NAT:Allocated Port for 192.168.121.113 -> 2.2.2.10:wanted 7224 got 7224
6d00h:NAT:i:icmp (192.168.121.113, 7224) -> (168.58.88.2, 7224) [2460]
6d00h:NAT:s=192.168.121.113->2.2.2.10, d=168.58.88.2 [2460] vrf=> shop

6d00h:NAT*:o:icmp (168.58.88.2, 7224) -> (2.2.2.10, 7224) [2460] vrf=> shop
6d00h:NAT*:s=168.58.88.2, d=2.2.2.10->192.168.121.113 [2460] vrf=> shop

6d00h:NAT:Allocated Port for 192.168.121.113 -> 2.2.2.10:wanted 7225 got 7225
6d00h:NAT:i:icmp (192.168.121.113, 7225) -> (168.58.88.2, 7225) [2461]
6d00h:NAT:s=192.168.121.113->2.2.2.10, d=168.58.88.2 [2461] vrf=> shop
6d00h:NAT*:o:icmp (168.58.88.2, 7225) -> (2.2.2.10, 7225) [2461] vrf=> shop
6d00h:NAT*:s=168.58.88.2, d=2.2.2.10->192.168.121.113 [2461] vrf=> shop
6d00h:NAT:Allocated Port for 192.168.121.113 -> 2.2.2.10:wanted 7226 got 7226
6d00h:NAT:i:icmp (192.168.121.113, 7226) -> (168.58.88.2, 7226) [2462]
6d00h:NAT:s=192.168.121.113->2.2.2.10, d=168.58.88.2 [2462] vrf=> shop
```

Table 4 describes the significant fields shown in the display.

**Table 4** *debug ip nat vrf Field Descriptions*

Field	Description
vrf=>	Indicates that NAT is applied to a particular VPN.

The following is sample output from the **debug ip nat wlan-nat** command:

```
Router# debug ip nat wlan-nat

WLAN-NAT: Creating secure ARP entry (10.1.1.1,0010.7bc2.9ff6)
WLAN-NAT: Triggered Acct Start for (171.1.1.10,0010.7bc2.9ff6)
WLAN-NAT: Extracting addr:171.1.1.10,input_idb:Ethernet1/2 from pak
WLAN-NAT: Saving address:171.1.1.10,input_idb:Ethernet1/2 in pak
```

After the WLAN-entry times out, the following debugs will be seen:

```
Router# debug ip nat wlan-nat

WLAN-NAT: Removing secure arp entry (10.1.1.1,0010.7bc2.9ff6)
WLAN-NAT: triggered Acct Stop for (171.1.1.10,0010.7bc2.9ff6)
```

Table 5 describes the significant fields shown in the display.

**Table 5** *debug ip nat wlan-nat Field Descriptions*

Field	Description
WLAN-NAT	Indicates that the packet is being translated by the WLAN-NAT feature.
Creating secure ARP entry	Indicates the IP address and MAC address of the static IP host.
Triggered Acct Start for	Indicates the NAT-assigned address and MAC address of the static IP host.
Extracting addr	Indicates the NAT assigned address of the static IP host.

**Table 5** *debug ip nat wlan-nat Field Descriptions (continued)*

Field	Description
input_idb	Indicates the interface on which the packet will be sent from the static IP host.
Saving address	Indicates the NAT assigned address of the static IP host.
Removing secure arp entry	Indicates removal of the ARP entry for the static IP host (IP address and MAC address).
triggered Acct Stop for	Indicates removal of the RADIUS profile for the static IP host (NAT-assigned address and MAC address).

**Related Commands**

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
<b>ip nat inside destination</b>	Enables NAT of the inside destination address.
<b>ip nat inside source</b>	Enables NAT of the inside source address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.
<b>ip nat pool</b>	Defines a pool of IP addresses for NAT.
<b>ip nat service</b>	Enables a port other than the default port.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

# ip nat

To designate that traffic originating from or destined for the interface is subject to Network Address Translation (NAT), to enable NAT logging, or to enable static IP address support, use the **ip nat** command in interface configuration mode. To prevent the interface from being able to translate or log, use the **no** form of this command.

```
ip nat [{inside | outside} | log | translations | syslog | allow-static-host]
```

```
no ip nat [{inside | outside} | log | translations | syslog | allow-static-host]
```

## Syntax Description

<b>inside</b>	(Optional) Indicates that the interface is connected to the inside network (the network subject to NAT translation).
<b>outside</b>	(Optional) Indicates that the interface is connected to the outside network.
<b>log</b>	(Optional) Enables NAT logging.
<b>translations</b>	(Optional) Enables NAT logging translations.
<b>syslog</b>	(Optional) Enables syslog for NAT logging translations.
<b>allow-static-host</b>	(Optional) Enables static IP address support for NAT translation.

## Defaults

Traffic leaving or arriving at this interface is not subject to NAT.

## Command Modes

Interface configuration

## Command History

Release	Modification
11.2	This command was introduced.
12.3(2)XE	The <b>allow-static-host</b> keyword was added.
12.3(7)T	This command was implemented in Cisco IOS Release 12.3(7)T.

## Usage Guidelines

Only packets moving between inside and outside interfaces can be translated. You must specify at least one inside interface and outside interface for each border router where you intend to use NAT.

When static IP address support is enabled with the **ip nat allow-static-host** command, Cisco IOS software will provide a working IP address within the Public Wireless LAN to users configured with a static IP address.

**Examples**

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

The following example enables static IP address support for the router at 192.168.196.51:

```
interface ethernet 1
 ip nat inside
ip nat allow-static-host
ip nat pool xyz 171.1.1.1 171.1.1.10 netmask 255.255.255.0 accounting WLAN-ACCT
ip nat inside source list 1 pool net-208
access-list 1 deny ip 192.168.196.51
```

**Related Commands**

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>debug ip nat</b>	Displays information about IP packets translated by NAT.
<b>ip nat inside destination</b>	Enables NAT of the inside destination address.
<b>ip nat inside source</b>	Enables NAT of the inside source address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.
<b>ip nat pool</b>	Defines a pool of IP addresses for NAT.
<b>ip nat service</b>	Enables a port other than the default port.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

## ip nat pool

To define a pool of IP addresses for Network Address Translation (NAT), use the **ip nat pool** command in global configuration mode. To remove one or more addresses from the pool, use the **no** form of this command.

```
ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length} [type rotary] |
[accounting list-name]
```

```
no ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length} [type rotary]
| [accounting list-name]
```

### Syntax Description

<i>name</i>	Name of the pool.
<i>start-ip</i>	Starting IP address that defines the range of addresses in the address pool.
<i>end-ip</i>	Ending IP address that defines the range of addresses in the address pool.
<b>netmask</b> <i>netmask</i>	Network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong.
<b>prefix-length</b> <i>prefix-length</i>	Number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong.
<b>type rotary</b>	(Optional) Indicates that the range of addresses in the address pool identifies real, inside hosts among which TCP load distribution will occur.
<b>accounting</b> <i>list-name</i>	(Optional) Indicates the RADIUS profile name that matches the RADIUS configuration in the router.

### Defaults

No pool of addresses is defined.

### Command Modes

Global configuration

### Command History

Release	Modification
11.2	This command was introduced.
12.3(2)XE	The <b>accounting</b> keyword and <i>list-name</i> argument were added.
12.3(7)T	This command was implemented in Cisco IOS Software Release 12.3(7)T.

### Usage Guidelines

This command defines a pool of addresses using start address, end address, and either netmask or prefix length. The pool could define an inside global pool, an outside local pool, or a rotary pool.

**Examples**

The following example translates between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

**Related Commands**

Command	Description
<b>clear ip nat translation</b>	Clears dynamic NAT translations from the translation table.
<b>debug ip nat</b>	Displays information about IP packets translated by NAT.
<b>ip nat</b>	Designates that traffic originating from or destined for the interface is subject to NAT.
<b>ip nat inside source</b>	Enables NAT of the inside destination address.
<b>ip nat outside source</b>	Enables NAT of the outside source address.
<b>ip nat pool</b>	Enables NAT of the outside source address.
<b>ip nat service</b>	Enables a port other than the default port.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

