



## NAT Support for IPsec ESP—Phase II

The NAT Support for IPsec ESP—Phase II feature allows multiple concurrent IP Security (IPsec) Encapsulating Security Payload (ESP) tunnels or connections through a Cisco IOS Network Address Translation (NAT) device configured in overload or Port Address Translation (PAT) mode. IPsec wrapper techniques used with the User Datagram Protocol (UDP) are not used with ESP tunnels.



### Note

This feature can only be used if both VPN endpoints are Cisco devices running Cisco IOS release 12.2(15)T or later.

### Feature Specifications for the NAT Support for IPsec ESP—Phase II Feature

#### Feature History

Release	Modification
12.2(15)T	This feature was introduced.

#### Supported Platforms

For supported platforms in Cisco IOS Release 12.2(15)T, consult Cisco Feature Navigator.

### 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

- [Information About NAT Support for IPsec ESP, page 2](#)
- [How to Configure IPsec ESP Through NAT, page 3](#)
- [Additional References, page 6](#)
- [Command Reference, page 8](#)

# Information About NAT Support for IPsec ESP

Before you configure IPsec ESP through NAT, you should understand the following concepts:

- [Benefits of NAT Support for IPsec ESP, page 2](#)
- [IPsec, page 2](#)
- [SPI Matching, page 3](#)

## Benefits of NAT Support for IPsec ESP

Normally ESP entries in the translation table will be delayed from being transmitted until a reply is received from the destination. With predictable security parameter indexes (SPIs) and SPI matching, the delay can be eliminated since the SPI entries are matched. Some third-party concentrators require both the source and incoming ports to use port 500. Use of the **preserve-port** keyword with the **ip nat service** command will preserve the ports rather than changing one, which is required with regular NAT.

## IPsec

IPsec is a set of extensions to the IP protocol family in a framework of open standards for ensuring secure private communications over the Internet. Based on standards developed by the Internet Engineering Task Force (IETF), IPsec ensures confidentiality, integrity, and authenticity of data communications across the public network and provides cryptographic security services.

Secure tunnels between two peers, such as two routers, are provided and decisions are made as to which packets are considered sensitive and should be sent through these secure tunnels, and which parameters should be used to protect these sensitive packets by specifying characteristics of these tunnels. When the IPsec peer receives a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

IPsec using ESP can pass through a router running NAT without any specific support from it as long as Network Address Port Translation (NAPT) or address overloading are not configured.

There are a number of factors to consider when attempting an IPsec Virtual Private Network (VPN) connection that traverses a NAPT device that represents multiple private internal IP addresses as a single public external IP address. Such factors include the capabilities of the VPN server and client, the capabilities of the NAPT device, and whether more than one simultaneous connection is attempted across the NAPT device.

There are two possible methods for configuring IPsec on a router with NAPT:

- Encapsulate IPsec in a Layer 4 protocol such as TCP or UDP—In this case, IPsec is “sneaking” through NAT. The NAT device is unaware of the encapsulation.
- Add IPsec specific support to NAPT—IPsec works with NAT in this case as opposed to “sneaking” through NAT. The NAT Support for IPsec ESP—Phase II feature provides support for Internet Key Exchange (IKE) and ESP without encapsulation in tunnel mode through a Cisco IOS router configured with NAPT.

**Note**

The recommended protocols to use when conducting IPsec sessions that traverse a NAPT device are TCP and UDP but not all VPN servers or clients support TCP or UDP.

## SPI Matching

SPI matching is used to establish VPN connections between multiple pairs of destinations. NAT entries will immediately be placed in the translation table for endpoints matching the configured access list. This is available only for endpoints that choose SPIs according to the predictive algorithm implemented in Cisco IOS Release 12.2(15)T.

## How to Configure IPsec ESP Through NAT

This section contains the following procedures:

- [Enabling Preserve Port, page 3](#)
- [Enabling SPI Matching, page 4](#)

## Enabling Preserve Port

The configuration in this task is used for IPsec traffic using port 500 for the source and incoming ports. This task enables port 500 to be preserved for both source and incoming ports.

**Note**

---

This task is required by certain VPN concentrators but will cause problems with other concentrators. Cisco VPN devices generally do not use this feature.

---

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip nat service list *access-list-number* IKE preserve-port**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<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>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ip nat service list <i>access-list-number</i> IKE preserve-port</b>  <b>Example:</b> Router(config)# ip nat service list 10 IKE preserve-port	Specifies a port other than the default port. <ul style="list-style-type: none"> <li>Enables NAT to preserve the source and destination port of any IKE packet matching access list 10 where both ports are 500.</li> </ul>

**Prerequisites**

- Cisco IOS software must be running on both the source router and the remote gateway enabling parallel processing.
- SPI matching must be configured on the NAT device and both endpoint devices.

**Enabling SPI Matching**

This section contains the following procedures:

- [Enabling SPI Matching on the NAT Device, page 4](#)
- [Enabling SPI Matching on the Endpoints, page 5](#)

**Enabling SPI Matching on the NAT Device**

This task enables SPI matching to be configured on the NAT device.

**SUMMARY STEPS**

- enable**
- configure terminal**
- ip nat service list *access-list-number* ESP spi-match**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<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>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ip nat service list access-list-number ESP spi-match</b>  <b>Example:</b> Router(config)# ip nat service list 10 ESP spi-match	Specifies a port other than the default port. <ul style="list-style-type: none"> <li>Enters ESP traffic matching list 10 into the NAT translation table, making the assumption that both devices are Cisco devices and are configured to provide matchable SPIs.</li> </ul>

**Enabling SPI Matching on the Endpoints**

This task enables SPI matching on both endpoints.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **crypto ipsec nat-transparency spi-matching**

## 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>crypto ipsec nat-transparency spi-matching</b>  <b>Example:</b> Router(config)# crypto ipsec nat-transparency spi-matching	Enables SPI matching on both endpoints.

## Additional References

For additional information related to NAT Support for IPsec ESP—Phase II features, see the following sections:

- [Related Documents, page 7](#)
- [Standards, page 7](#)
- [MIBs, page 7](#)
- [RFCs, page 8](#)
- [Technical Assistance, page 8](#)

## Related Documents

Related Topic	Document Title
NAT configuration tasks	“Configuring IP Addressing” chapter of the <i>Cisco IOS IP Configuration Guide</i> , Release 12.2
NAT commands	“IP Addressing Commands” chapter of the <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i> , Release 12.2 T
Support for IPsec ESP through NAT	<i>Support for IPsec Through NAT</i> feature document, Release 12.2(13)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 obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## 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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 T command reference publications.

### Modified Commands

- **clear ip nat translation**
- **crypto ipsec nat-transparency**
- **ip nat service**
- **show ip nat translations**

# clear ip nat translation

To clear dynamic Network Address Translation (NAT) translations from the translation table, use the **clear ip nat translation** command in privileged EXEC mode.

```
clear ip nat translation { * | [inside global-ip global-port local-ip local-port] | [outside local-ip global-ip] }
```

```
clear ip nat translation [esp | tcp | udp] [inside global-ip global-port local-ip local-port] | [outside local-ip global-ip]
```

## Syntax Description

<b>*</b>	Clears all dynamic translations.
<b>inside</b>	(Optional) Clears the inside translations containing the specified <i>global-ip</i> and <i>local-ip</i> addresses.
<i>global-ip</i>	(Optional) Global IP address.
<i>global-port</i>	(Optional) Global port.
<i>local-ip</i>	(Optional) Local IP address.
<i>local-port</i>	(Optional) Local port.
<b>outside</b>	(Optional) Clears the outside translations containing the specified global and local addresses.
<b>esp</b>	(Optional) Clears Encapsulating Security Payload (ESP) entries from the translation table.
<b>tcp</b>	(Optional) Clears the TCP entries from the translation table.
<b>udp</b>	(Optional) Clears the User Datagram Protocol (UDP) entries from the translation table.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
11.2	This command was introduced.
12.2(15)T	The <b>esp</b> keyword was added.

## Usage Guidelines

Use this command to clear entries from the translation table before they time out.

## Examples

The following example shows the NAT entries before and after the User Datagram Protocol (UDP) entry is cleared:

```
Router# show ip nat translations

Pro Inside global      Inside local      Outside local      Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53    171.69.2.132:53
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
```

## clear ip nat translation

```
Router# clear ip nat translation udp inside 171.69.233.209 1220 192.168.1.95 1220
171.69.2.132 53 171.69.2.132 53
```

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

```
Pro Inside global      Inside local      Outside local      Outside global
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
```

### Related Commands

Command	Description
<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>	Changes the amount of time after which NAT translations time out.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

## crypto ipsec nat-transparency

To enable security parameter index (SPI) matching or User Datagram Protocol (UDP) encapsulation between two Virtual Private Network (VPN) devices, use the **crypto ipsec nat-transparency** command on both devices in global configuration mode. To disable both SPI matching and UDP encapsulation, use the **no** form of this command with each keyword.

```
crypto ipsec nat-transparency {spi-matching | udp-encaps}
```

```
no crypto ipsec nat-transparency {spi-matching | udp-encaps}
```

Syntax Description	spi-matching	Enables SPI matching on both endpoints.
	udp-encaps	Enables UDP encapsulation on both endpoints.

**Defaults** When this command is entered, UDP encapsulation is enabled by default.

**Command Modes** Global configuration (config)

Command History	Release	Modification
	12.2(13)T	This command was introduced.
	12.2(15)T	The <b>spi-matching</b> keyword was added.

**Usage Guidelines** You can use this command to resolve issues that arise when Network Address Translation (NAT) is configured in an IP Security (IPsec)-aware network. This command has two mutually exclusive options:

- The default option is UDP encapsulation of the IPsec protocols.
- The alternative is to match the inbound SPI to the outbound SPI.

When you enter the **crypto ipsec nat-transparency** command, UDP encapsulation is configured unless you either specifically disable it or configure SPI matching. You can disable both options, but doing so might cause problems if the device you are configuring uses NAT and is part of a VPN.

To disable SPI matching, configure UDP encapsulation or use the **no** form of this command with the keyword **spi-matching**. To disable UDP encapsulation, configure SPI matching or use the **no** form of this command with the keyword **udp-encaps**. To disable both SPI matching and UDP encapsulation, first disable UDP encapsulation, and then disable SPI matching. If you disable both options, the **show running-config** command displays **no crypto ipsec nat-transparency udp-encaps**.

**Examples** The following example shows how to enable SPI matching on the endpoint routers:

```
crypto ipsec nat-transparency spi-matching
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<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>show ip nat statistics</b>	Displays NAT statistics.
	<b>show ip nat translations</b>	Displays active NAT translations.
	<b>show crypto isakmp sa detail nat</b>	Displays NAT translations of source and destination addresses.

## ip nat service

To specify a port other than the default port, use the **ip nat service** command in global configuration mode. To disable the port, use the **no** form of this command.

```
ip nat service {H225 | list {access-list-number | access-list-name} {ESP spi-match | IKE preserve-port | ftp tcp port port-number} | ras | sip {tcp | udp} port port-number | skinny tcp port port-number}
```

```
no ip nat service {H225 | list {access-list-number | access-list-name} {ESP spi-match | IKE preserve-port | ftp tcp port port-number} | ras | sip {tcp | udp} port port-number | skinny tcp port port-number}
```

Syntax Description		
<b>H225</b>		H323-H225 protocol.
<b>list</b> <i>access-list-number</i>		Standard access list number in the range from 1 to 199.
<i>access-list-name</i>		Name of a standard IP access list.
<b>ESP</b>		Security Parameter Index (SPI) matching IPsec pass-through.
<b>spi-match</b>		SPI matching IPsec pass-through. The ESP endpoints must also have SPI matching enabled.
<b>IKE</b>		Preserve Internet Key Exchange (IKE) port, as required by some IPsec servers.
<b>preserve-port</b>		Preserve User Datagram Protocol (UDP) port in IKE packets.
<b>ftp</b>		FTP protocol.
<b>tcp</b>		TCP protocol.
<b>udp</b>		User Datagram Protocol.
<b>port</b> <i>port-number</i>		Port other than the default port in the range from 1 to 65533.
<b>ras</b>		H323-RAS protocol.
<b>sip</b>		SIP protocol.
<b>skinny</b>		Skinny protocol.

**Defaults** Disabled

**Command Modes** Global configuration (config)

Command History	Release	Modification
	11.3	This command was introduced.
	12.1(5)T	The <b>skinny</b> keyword was added.
	12.2(8)T	The <b>sip</b> keyword was added.
	12.2(15)T	The <b>esp</b> and <b>spi-match</b> keywords were added to enable SPI matching on outside IPsec gateways. The <b>ike</b> and <b>preserve-port</b> keywords were added to enable outside IPsec gateways that require IKE source port 500.

**Usage Guidelines**

A host with an FTP server using a port other than the default port can have an FTP client using the default FTP control port. When a port other than the default port is configured for an FTP server, Network Address Translation (NAT) prevents FTP control sessions that are using port 21 for that particular server. If an FTP server uses the default port and a port other than the default port, both ports need to be configured using the **ip nat service** command.

NAT listens on the default port of the Cisco CallManager to translate the skinny messages. If the CallManager uses a port other than the default port, that port needs to be configured using the **ip nat service** command.

**Examples**

The following example shows how to configure the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example shows how to configure the standard FTP port 21 and the nonstandard port 2021:

```
ip nat service list 10 ftp tcp port 21
ip nat service list 10 ftp tcp port 2021
access-list 10 permit 10.1.1.1
```

The following example shows how to configure the 20002 port of the CallManager:

```
ip nat service skinny tcp port 20002
```

The following example shows how to configure TCP port 500 of the third-party concentrator:

```
ip nat service list 10 IKE preserve-port
```

The following example shows how to configure SPI matching on the endpoint routers:

```
ip nat service list 10 ESP spi-match
```

**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>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

# show ip nat translations

To display active Network Address Translation (NAT) translations, use the **show ip nat translations** command in privileged EXEC mode.

```
show ip nat translations [esp] [icmp] [pptp] [tcp] [udp] [verbose] [vrf vrf-name]
```

## Syntax Description

<b>esp</b>	(Optional) Displays Encapsulating Security Payload (ESP) entries.
<b>icmp</b>	(Optional) Displays Internet Control Message Protocol (ICMP) entries.
<b>pptp</b>	(Optional) Displays Point-to-Point Tunneling Protocol (PPTP) entries.
<b>tcp</b>	(Optional) Displays TCP protocol entries.
<b>udp</b>	(Optional) Displays User Datagram Protocol (UDP) entries.
<b>verbose</b>	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.
<b>vrf vrf-name</b>	(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	The <b>vrf vrf-name</b> keyword and argument combination was added.
12.2(15)T	The <b>esp</b> keyword was added.

## Examples

The following is sample output from the **show ip nat translations** command. Without overloading, two inside hosts are exchanging packets with some number of outside hosts.

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

```
Pro Inside global      Inside local      Outside local      Outside global
--- 171.69.233.209     192.168.1.95     ---                ---
--- 171.69.233.210     192.168.1.89     ---                --
```

With overloading, a translation for a Domain Name Server (DNS) transaction is still active, and translations for two Telnet sessions (from two different hosts) are also active. Note that two different inside hosts appear on the outside with a single IP address.

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

```
Pro Inside global      Inside local      Outside local      Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53    171.69.2.132:53
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
```

The following is sample output that includes the **verbose** keyword:

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

■ **show ip nat translations**

```

Pro Inside global      Inside local      Outside local      Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53    171.69.2.132:53
      create 00:00:02, use 00:00:00, flags: extended
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23    171.69.1.220:23
      create 00:01:13, use 00:00:50, flags: extended
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
      create 00:00:02, use 00:00:00, flags: extended

```

The following is sample output that includes the **vrf** keyword:

```

Router# show ip nat translations vrf red
Pro Inside global      Inside local      Outside local      Outside global
--- 2.2.2.1            192.168.121.113  ---              ---
--- 2.2.2.2            192.168.122.49  ---              ---
--- 2.2.2.11           192.168.11.1    ---              ---
--- 2.2.2.12           192.168.11.3    ---              ---
--- 2.2.2.13           140.48.5.20     ---              ---

Pro Inside global      Inside local      Outside local      Outside global
--- 2.2.2.3            192.168.121.113  ---              ---
--- 2.2.2.4            192.168.22.49   ---              ---

```

The following is sample output that includes the **esp** keyword:

```

Router# show ip nat translations esp
Pro Inside global      Inside local      Outside local      Outside global
esp 192.168.22.40:0    192.168.122.20:0 192.168.22.20:0
192.168.22.20:28726CD9
esp 192.168.22.40:0    192.168.122.20:2E59EEF5 192.168.22.20:0 192.168.22.20:0

```

The following is sample output that includes the **esp** and **verbose** keywords:

```

Router# show ip nat translation esp verbose
Pro Inside global      Inside local      Outside local      Outside global
esp 192.168.22.40:0    192.168.122.20:0 192.168.22.20:0
192.168.22.20:28726CD9
      create 00:00:00, use 00:00:00,
      flags:
extended, 0x100000, use_count:1, entry-id:192, lc_entries:0
esp 192.168.22.40:0    192.168.122.20:2E59EEF5 192.168.22.20:0 192.168.22.20:0
      create 00:00:00, use 00:00:00, left 00:04:59, Map-Id(In):20,
      flags:
extended, use_count:0, entry-id:191, lc_entries:0

```

Table 1 describes the significant fields shown in the display.

**Table 1** *show ip nat translations Field Descriptions*

Field	Description
Pro	Protocol of the port identifying the address.
Inside global	The legitimate IP address that represents one or more inside local IP addresses to the outside world.
Inside local	The IP address assigned to a host on the inside network; probably not a legitimate address assigned by the Network Interface Card (NIC) or service provider.

**Table 1** *show ip nat translations Field Descriptions (continued)*

Field	Description
Outside local	IP address of an outside host as it appears to the inside network; probably not a legitimate address assigned by the NIC or service provider.
Outside global	The IP address assigned to a host on the outside network by its owner.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
flags	Indication of the type of translation. Possible flags are: <ul style="list-style-type: none"> <li>• extended—Extended translation</li> <li>• static—Static translation</li> <li>• destination—Rotary translation</li> <li>• outside—Outside translation</li> <li>• timing out—Translation will no longer be used, due to a TCP finish (FIN) or reset (RST) flag.</li> </ul>

**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>	Changes the amount of time after which NAT translations time out.
<b>show ip nat statistics</b>	Displays NAT statistics.

■ show ip nat translations