



# NAT Commands

---

Use the commands in this chapter to configure and monitor Network Address Translation (NAT).

# clear ip nat translation

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

**clear ip nat translation** { \* | [**inside** *global-ip* *global-port* *local-ip* *local-port*] / [**outside** *local-ip* *global-ip*] [**piggyback-internal** | **esp** | **tcp** | **udp**] }

**clear ip nat translation** { \* | [**inside** *global-ip* *global-port* *local-ip* *local-port*] / [**outside** *local-ip* *global-ip*] [**piggyback-internal** | **esp** | **tcp** | **udp**] }

## 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 <i>global</i> and <i>local</i> addresses.
<b>piggyback-internal</b>	(Optional) Clears translations created off of piggyback data.
<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

EXEC

## Command History

Release	Modification
11.2	This command was introduced.
12.2(15)T	The <b>esp</b> keyword was added.
12.4(2)T	The <b>piggyback-internal</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 172.69.233.209:1220 192.168.1.95:1220 172.69.2.132:53    172.69.2.132:53
```

```
tcp 172.69.233.209:11012 192.168.1.89:11012 172.69.1.220:23 172.69.1.220:23
tcp 172.69.233.209:1067 192.168.1.95:1067 172.69.1.161:23 172.69.1.161:23
```

```
Router# clear ip nat translation udp inside 10.69.233.209 1220 10.168.1.95 1220
10.69.2.132 53 10.69.2.132 53
```

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

```
Pro      Inside global      Inside local      Outside local      Outside global
tcp      10.69.233.209:11012 10.168.1.89:11012 10.69.1.220:23    10.69.1.220:23
tcp      10.69.233.209:1067 10.168.1.95:1067 10.69.1.161:23    10.69.1.161:23
```

## 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.

# clear ip snat sessions

To clear dynamic Stateful Network Address Translation (SNAT) sessions from the translation table, use the **clear ip snat sessions** command in EXEC mode.

**clear ip snat sessions** \* [*ip-address-peer*]

## Syntax Description

*	Removes all dynamic entries.
<i>ip-address-peer</i>	(Optional) Removes SNAT entries of the peer translator.

## Command Modes

EXEC

## Command History

Release	Modification
12.2(13)T	This command was introduced.

## Usage Guidelines

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

## Examples

The following example shows the SNAT entries before and after using the **clear ip snat sessions** command:

```
Router> show ip snat distributed
```

```
SNAT:Mode PRIMARY
  :State READY
  :Local Address 10.168.123.2
  :Local NAT id 100
  :Peer Address 10.168.123.3
  :Peer NAT id 200
  :Mapping List 10
```

```
Router> clear ip snat sessions *
Closing TCP session to peer:10.168.123.3
Router> show ip snat distributed
```

# clear ip snat translation distributed

To clear dynamic Stateful Network Address Translation (SNAT) translations from the translation table, use the **clear ip snat translation distributed** command in EXEC mode.

**clear ip snat translation distributed \***

Syntax Description	* Removes all dynamic SNAT entries.
--------------------	-------------------------------------

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(13)T	This command was introduced.

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

Examples	The following example clears all dynamic SNAT translations from the translation table: Router# <b>clear ip snat translation distributed *</b>
----------	--

# clear ip snat translation peer

To clear peer Stateful Network Address Translation (SNAT) translations from the translation table, use the **clear ip snat translation peer** command in EXEC mode.

**clear ip snat translation peer** *ip-address-peer* [**refresh**]

Syntax Description	<i>ip-address-peer</i>	IP address of the peer translator.
	<b>refresh</b>	(Optional) Provides a fresh dump of the NAT table from the peer.

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines	Use this command to clear peer entries from the translation table before they time out.
------------------	---

**Examples** The following example shows the SNAT entries before and after the peer entry is cleared:

```
Router# show ip snat peer
```

```
Pro Inside global      Inside local      Outside local      Outside global
--- 192.168.25.20      192.168.122.20    ---                ---
tcp 192.168.25.20:33528 192.168.122.20:33528 192.168.24.2:21 192.168.24.2:21
```

```
Router# clear ip snat translation peer 192.168.122.20
```

# 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-208 172.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 172.69.232.182 255.255.255.240
```

```

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 pool1 172.1.1.1 171.1.1.10 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 enable

To configure an interface connecting Virtual Private Networks (VPNs) and the Internet for Network Address Translation (NAT), use the **ip nat enable** command in interface configuration mode.

**ip nat enable**

**no ip nat enable**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(14)T	This command was introduced.

<b>Examples</b>	The following example show how to configure an interface connecting VPNs and the Internet for NAT translation:
-----------------	--

```
interface Ethernet0/0
 ip vrf forwarding vrf1
 ip address 192.168.122.1 255.255.255.0
 ip nat enable
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip nat pool</b>	Defines a pool of IP addresses for Network Address Translation.
	<b>ip nat source</b>	Enables Network Address Translation on a virtual interface without inside or outside specification.

# ip nat inside destination

To enable Network Address Translation (NAT) of the inside destination address, use the **ip nat inside destination** command in global configuration mode. To remove the dynamic association to a pool, use the **no** form of this command.

**ip nat inside destination list** {*access-list-number* | *name*} **pool** *name* [**mapping-id** *map-id*]

**no ip nat inside destination list** {*access-list-number* | *name*} **pool** *name* [**mapping-id** *map-id*]

## Syntax Description

<b>list</b> <i>access-list-number</i>	Standard IP access list number. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
<b>list</b> <i>name</i>	Name of a standard IP access list. Packets with destination addresses that pass the access list are translated using global addresses from the named pool.
<b>pool</b> <i>name</i>	Name of the pool from which global IP addresses are allocated during dynamic translation.
<b>mapping-id</b> <i>map-id</i>	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.

## Defaults

No inside destination addresses are translated.

## Command Modes

Global configuration

## Command History

Release	Modification
11.2	This command was introduced.
12.3(7)T	The <b>mapping-id</b> <i>map-id</i> keyword and argument combination was added.

## Usage Guidelines

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

## Examples

The following example shows how to translate between inside hosts addressed to either the 192.168.1.0 or 192.168.2.0 network to the globally unique 10.69.233.208/28 network:

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside destination list 1 pool net-208
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 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>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 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 inside source

To enable Network Address Translation (NAT) of the inside source address, use the **ip nat inside source** command in global configuration mode. To remove the static translation or remove the dynamic association to a pool, use the **no** form of this command.

## Dynamic NAT

**ip nat inside source** {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} {**interface** *type number* | **pool** *name*} [**mapping-id** *map-id* | **overload** | **reversible** | **vrf** *name*] [**oer**]

**no ip nat inside source** {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} {**interface** *type number* | **pool** *name*} [**mapping-id** *map-id* | **overload** | **reversible** | **vrf** *name*] [**oer**]

## Static NAT

**ip nat inside source** {**static** {**esp** *local-ip* **interface** *type number* | *local-ip* *global-ip*} } [**extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **route-map** | **vrf** *name*]

**no ip nat inside source** {**static** {**esp** *local-ip* **interface** *type number* | *local-ip* *global-ip*} } [**extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **route-map** | **vrf** *name*]

## Port Static NAT

**ip nat inside source** {**static** {**tcp** | **udp** {*local-ip* *local-port* *global-ip* *global-port* | **interface** *global-port*} } } [**extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **route-map** | **vrf** *name*]

**no ip nat inside source** {**static** {**tcp** | **udp** {*local-ip* *local-port* *global-ip* *global-port* | **interface** *global-port*} } } [**extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **route-map** | **vrf** *name*]

## Network Static NAT

**ip nat inside source static network** *local-network* *global-network* *mask* [**extendable** | **no-alias** | **no-payload** | **mapping-id** *map-id* | **redundancy** *group-name* | **route-map** | **vrf** *name*]

**no ip nat inside source static network** *local-network* *global-network* *mask* [**extendable** | **no-alias** | **no-payload** | **mapping-id** *map-id* | **redundancy** *group-name* | **route-map** | **vrf** *name*]

## Syntax Description

<b>list</b> <i>access-list-number</i>	Number of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
<b>list</b> <i>access-list-name</i>	Name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
<b>route-map</b> <i>name</i>	Specifies the named route map.
<b>interface</b> <i>type</i>	Specifies the interface type for the global address.

<b>interface</b> <i>number</i>	Specifies the interface number for the global address.
<b>pool</b> <i>name</i>	Name of the pool from which global IP addresses are allocated dynamically.
<b>mapping-id</b> <i>map-id</i>	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.
<b>overload</b>	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.
<b>reversible</b>	(Optional) Enables outside-to-inside initiated sessions to use routemaps for destination-based NAT.
<b>vrf</b> <i>name</i>	(Optional) Associates the NAT translation rule with a particular virtual routing and forwarding (VRF) instance.
<b>oer</b>	(Optional) Allows Optimized Edge Routing (OER) to operate with NAT and control traffic class routing.
<b>static</b> <i>local-ip</i>	Sets up a single static translation. The <i>local-ip</i> argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
<i>local-port</i>	Sets the local TCP/UDP port in a range from 1 to 65535.
<b>static</b> <i>global-ip</i>	Sets up a single static translation. The <i>local-ip</i> argument establishes the globally unique IP address of an inside host as it appears to the outside network.
<i>global-port</i>	Sets the global TCP/UDP port in a range from 1 to 65535.
<b>extendable</b>	(Optional) Extends the translation.
<b>no-alias</b>	(Optional) Prohibits an alias from being created for the global address.
<b>no-payload</b>	(Optional) Prohibits the translation of an embedded address or port in the payload.
<b>redundancy</b> <i>group-name</i>	(Optional) Establishes NAT redundancy.
<b>esp</b> <i>local-ip</i>	Establishes IPSec-ESP (tunnel mode) support.
<b>tcp</b>	Establishes the Transmission Control Protocol.
<b>udp</b>	Establishes the User Datagram Protocol.
<b>network</b> <i>local-network</i>	Specifies the local subnet translation.
<i>global-network</i>	Specifies the global subnet translation.
<i>mask</i>	Established the IP Network mask to be used with subnet translations.

**Defaults**

No NAT translation of inside source addresses occurs.

**Command Modes**

Global configuration

## Command History

Release	Modification
11.2	This command was introduced.
12.2(4)T	This command was modified to include the ability to use route maps with static translations, and the <b>route-map</b> <i>name</i> keyword and argument combination was added. This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the <b>redundancy</b> <i>group-name</i> keyword and argument combination was added. This command was modified to enable the translation of the IP header address only, and the <b>no-payload</b> keyword was added.
12.2(13)T	The <b>interface</b> keyword was added for static translations. The <b>mapping-id</b> <i>map-id</i> keyword and argument combination was added for dynamic translations. The <b>vrf</b> <i>name</i> keyword and argument combination was added.
12.3(7)T	The static <b>mapping-id</b> <i>map-id</i> keyword and argument combination was added.
12.3(14)T	The <b>reversible</b> keyword was added.
12.4(15)T	The <b>oer</b> keyword was added.

## Usage Guidelines

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Packets that enter the router through the inside interface and packets sourced from the router are checked against the access list for possible NAT candidates. The access list is used to specify which traffic is to be translated.

Alternatively, the syntax form with the **static** keyword establishes a single static translation.

## Examples

The following example shows how to translate between inside hosts addressed from either the 192.168.1.0 or 192.168.2.0 network to the globally unique 10.69.233.208/28 network:

```
ip nat pool net-208 10.69.233.208 192.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 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 shows how to translate only traffic local to the providers edge device running NAT (NAT-PE):

```
ip nat inside source list 1 interface e 0 vrf host1 overload
ip nat inside source list 1 interface e 0 vrf host2 overload
!
ip route vrf host1 0.0.0.0 0.0.0.0 192.1.1.1
ip route vrf host2 0.0.0.0 0.0.0.0 192.1.1.1
!
```

```
access-list 1 permit 10.1.1.0 0.0.0.255
!
ip nat inside source list 1 interface e 1 vrf host1 overload
ip nat inside source list 1 interface e 1 vrf host2 overload
!
ip route vrf host1 0.0.0.0 0.0.0.0 10.1.1.1 global
ip route vrf host2 0.0.0.0 0.0.0.0 10.1.1.1 global
access-list 1 permit 10.1.1.0 0.0.0.255
```

**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 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 outside source

To enable Network Address Translation (NAT) of the outside source address, use the **ip nat outside source** command in global configuration mode. To remove the static entry or the dynamic association, use the **no** form of this command.

## Dynamic NAT

**ip nat outside source** {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} **pool** *pool-name* [**add-route** | **mapping-id** *map-id* | **vrf** *name*]

**no ip nat outside source** {**list** {*access-list-number* | *access-list-name*} | **route-map** *name*} **pool** *pool-name* [**add-route** | **mapping-id** *map-id* | **vrf** *name*]

## Static NAT

**ip nat outside source static** *global-ip local-ip* [**add-route** | **extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **vrf** *name*]

**no ip nat outside source static** *global-ip local-ip* [**add-route** | **extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **vrf** *name*]

## Port Static NAT

**ip nat outside source static** {**tcp** | **udp**} *global-ip global-port local-ip local-port* [**add-route** | **extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **vrf** *name*]

**no ip nat outside source static** {**tcp** | **udp**} *global-ip global-port local-ip local-port* [**add-route** | **extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** *group-name* | **vrf** *name*]

## Network Static NAT

**ip nat outside source static network** *global-network local-network mask* [**add-route** | **extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** | **vrf** *name*]

**no ip nat outside source static network** *global-network local-network mask* [**add-route** | **extendable** | **mapping-id** *map-id* | **no-alias** | **no-payload** | **redundancy** | **vrf** *name*]

## Syntax Description

<b>list</b> <i>access-list-number</i>	Number of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
<b>list</b> <i>access-list-name</i>	Name of a standard IP access list. Packets with source addresses that pass the access list are translated using global addresses from the named pool.
<b>route-map</b> <i>name</i>	Specifies a named route map.
<b>pool</b> <i>pool-name</i>	Name of the pool from which global IP addresses are allocated.
<b>mapping-id</b> <i>map-id</i>	(Optional) Specifies whether the local Stateful NAT Translation (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.
<b>vrf</b> <i>name</i>	(Optional) Associates the NAT translation rule with a particular VPN.
<b>add-route</b>	(Optional) Adds a static route for the outside local address.



<b>static</b> <i>global-ip</i>	Sets up a single static translation. This argument establishes the globally unique IP address assigned to a host on the outside network by its owner. It was allocated from globally routable network space.
<i>local-ip</i>	Local IP address of an outside host as it appears to the inside network. The address was allocated from address space routable on the inside (RFC 1918, <i>Address Allocation for Private Internets</i> ).
<b>extendable</b>	(Optional) Extends the transmission.
<b>no-alias</b>	(Optional) Prohibits an alias from being created for the local address.
<b>no-payload</b>	(Optional) Prohibits the translation of embedded address or port in the payload.
<b>redundancy</b> <i>group-name</i>	(Optional) Enables the NAT redundancy operation.
<b>tcp</b>	Establishes the Transmission Control Protocol.
<b>udp</b>	Establishes the User Datagram Protocol.

**Defaults**

No translation of source addresses coming from the outside to the inside network occurs.

**Command Modes**

Global configuration

**Command History**

Release	Modification
11.2	This command was introduced.
12.2(4)T	This command was modified to include static translation with Hot Standby Routing Protocol (HSRP), and the <b>redundancy</b> <i>group-name</i> keyword and argument combination was added. This command was modified to enable the translation of the IP header address only, and the <b>no-payload</b> keyword was added.
12.2(13)T	The <b>mapping-id</b> <i>map-id</i> keyword and argument combination was added for dynamic translations. The <b>vrf</b> <i>name</i> keyword and argument combination was added.
12.3(7)T	The <b>mapping-id</b> <i>map-id</i> keyword and argument combination was added for static translations.

**Usage Guidelines**

You might have IP addresses that are not legal, officially assigned IP addresses. Perhaps you chose IP addresses that officially belong to another network. The case of an address used illegally and legally is called *overlapping*. You can use NAT to translate inside addresses that overlap with outside addresses. Use this command if your IP addresses in the stub network happen to be legitimate IP addresses belonging to another network, and you need to communicate with those hosts or routers.

This command has two forms: dynamic and static address translation. The form with an access list establishes dynamic translation. Packets from addresses that match the standard access list are translated using global addresses allocated from the pool named with the **ip nat pool** command.

Alternatively, the syntax form with the **static** keyword establishes a single static translation.

## Examples

The following example shows how to translate between inside hosts addressed from the 10.114.11.0 network to the globally unique 10.69.233.208/28 network. Further packets from outside hosts addressed from the 10.114.11.0 network (the true 10.114.11.0 network) are translated to appear to be from the 10.0.1.0/24 network.

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 10.114.11.39 255.255.255.0
 ip nat inside
!
access-list 1 permit 10.114.11.0 0.0.0.255
```

The following example shows NAT configured on the Provider Edge (PE) router with a static route to the shared service for the gold and silver Virtual Private Networks (VPNs). NAT is configured as inside source static one-to-one translations.

```
ip nat pool outside 10.4.4.1 4.4.4.254 netmask 255.255.255.0
ip nat outside source list 1 pool mypool
access-list 1 permit 10.58.18.0 0.0.0.255
ip nat inside source static 192.168.121.33 10.2.2.1 vrf group1
ip nat inside source static 192.169.121.33 10.2.2.2 vrf group2
```

## 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 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 piggyback-support

To enable a NAT optimized SIP media path, use the **ip nat piggyback-support** command in global configuration mode.

**ip nat piggyback-support sip-alg {sdp-only | all-messages} router *router-id* authentication *authentication-key***

**no ip nat piggyback-support sip-alg {sdp-only | all-messages} router *router-id* authentication *authentication-key***

## Syntax Description

<b>sip-alg</b>	SIP protocol algorithm.
<b>sdp-only</b>	Establishes piggybacking in SDP only.
<b>all-messages</b>	Establishes piggybacking in all messages except SDP.
<b>router <i>router-id</i></b>	Piggyback router id number.
<b>authentication <i>authentication-key</i></b>	MD5 authentication key.

## Command Modes

Global configuration

## Command History

Release	Modification
12.4(2)T	This command was introduced.

## Examples

The following example shows how to configure a NAT optimized SIP media path with SDP:

```
ip nat piggyback-support sip sdp-only router 100 authentication md5-key
```

## 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.

# 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*} [**add-route**] [**type** {**match-host** | **rotary**}] [**accounting** *list-name*] [**arp-ping**]

**no ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} [**add-route**] [**type** {**match-host** | **rotary**}] [**accounting** *list-name*] [**arp-ping**]

## 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>add-route</b>	(Optional) Specifies that a route has been added to the NVI interface for the global address.
<b>type</b>	(Optional) Indicates the type of pool.
<b>match-host</b>	(Optional) Specifies that the host number is to remain the same after translation.
<b>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.
<b>arp-ping</b>	(Optional) Determines static IP client instances and restarts the NAT entry timer.

## 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 integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	The <b>add-route</b> keyword was added.
12.4(6)T	The <b>arp-ping</b> keyword was added.

**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 10.69.233.208/28 network:

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 10.69.232.182 255.255.255.240
 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 shows that a route has been added to the NVI interface for the global address:

```
ip nat pool NAT 192.168.25.20 192.168.25.30 netmask 255.255.255.0 add-route
ip nat source list 1 pool NAT vrf group1 overload
```

**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.

# 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** | **rtsp** {**tcp** | **udp**} **port** *port-number* | **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** | **rtsp** {**tcp** | **udp**} **port** *port-number* | **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>rtsp</b>	Real Time Streaming Protocol. This protocol is enabled by default on port 554.
	<b>sip</b>	SIP protocol.
	<b>skinny</b>	Skinny protocol.

**Defaults**

Disabled

RTSP is enabled

**Command Modes**

Global configuration

Command History	<b>Release</b>	<b>Modification</b>
	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.

Release	Modification
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.
12.3(7)T	The <b>rtsp</b> keyword was added.

### 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.

Use the **no ip nat service H225** command to disable support of H.225 packets by NAT.

Use the **no ip nat service rtsp** command to disable support of RTSP packets by NAT. RSTP uses port 554.

### Examples

The following example configures the nonstandard port 2021:

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

The following example configures 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 configures the 20002 port of the CallManager:

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

The following example configures TCP port 500 of the third-party concentrator:

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

The following example configures 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.

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



# ip nat sip-sbc

To configure a Cisco IOS hosted Network Address Translation (NAT) traversal for Session Border Controller (SBC), use the **ip nat sip-sbc** command in global configuration mode. To disable the Cisco IOS hosted NAT traversal for SBC, use the **no** form of this command.

```
ip nat sip-sbc proxy inside-address inside-port outside-address outside-port protocol {tcp | udp}
[call-id-pool pool-name] [override {address / none / port}] [mode allow-flow-around]
[session-timeout {seconds | nat-default}] [vrf-list vrf-name vrf-name | no | exit]
```

```
no ip nat sip-sbc proxy inside-address inside-port outside-address outside-port protocol {tcp |
udp} [call-id-pool pool-name] [override {address / none / port}] [mode allow-flow-around]
[session-timeout {seconds | nat-default}] [vrf-list vrf-name vrf-name | no | exit]
```

Syntax	Description
<b>proxy</b>	Configures the address or port which the inside phones refer to, and configures the outside proxy's address or port that the NAT SBC translates the destination IP address or port to.
<i>inside-address</i>	Sets the Proxy's private IP address, which is configured on the inside phones.
<i>inside-port</i>	Sets the Proxy's private port.
<i>outside-address</i>	Sets the Proxy's public address, which is the actual proxy's address that NAT SBC changes the destination address to.
<i>outside-port</i>	Sets the Proxy's port.
<b>protocol</b>	Specifies the communication protocol being used.
<b>tcp</b>	Establishes the Transmission Control Protocol.
<b>udp</b>	Establishes the User Datagram Protocol.
<b>call-id-pool</b> <i>pool-name</i>	(Optional) Specifies a dummy pool name from which the inside to outside SIP signaling packets' call ID is translated to a 1:1 maintained association rather than using the regular NAT pool.
<b>override address</b>	(Optional) Specifies the default override address mode.
<b>override none</b>	(Optional) Specifies that no override will be configured.
<b>override port</b>	(Optional) Specifies override port mode.
<b>mode allow-flow-around</b>	(Optional) Configures Real-Time Transport Protocol (RTP) for flow around for traffic between phones in the inside domain.
<b>session-timeout</b> <i>seconds</i>	(Optional) Configures the timeout duration for NAT entries pertaining to SIP signaling flows.
<b>session-timeout nat-default</b>	(Optional) Allows the default timeout to return to the NAT default timeout value of 5 minutes.
<b>none</b>	(Optional) Prevents modification of the out > in destination L3/L4 to the L3/L4 as saved in the sbc_appl_data of the door or NAT entry.
<b>vrf-list</b> <b>vrf-name</b>	(Optional) Defines SIP SBC VPN Routing and Forwarding (VRF) list names.
<b>no</b>	(Optional) Removes a name from the VRF list.
<b>exit</b>	(Required) Exit from SBC VRF configuration mode.

---

**Command Default** Disabled

---

**Command Modes** Global configuration

---

Command History	Release	Modification
	12.4(9)T	This command was introduced.

---



---

**Usage Guidelines** The **proxy** keyword configures the address or port, which the inside phones refer to, and it configures the outside proxy's address or port that the NAT SBC translates the destination IP address or port to. This keyword installs an outside static port half-entry with OL as the inside address or port and OG as the outside address or port.

The **mode allow-flow-around** keyword enables the RTP to be flow around. This keyword is only applicable for traffic between phones in the inside domain.

The optional **vrf-list** keyword must be followed by a list of VRF names. After the outside static port entry is created, a static route is installed with the destination IP address as OL and next hop as OG. The NAT entry created is associated with appropriate VRFs as configured by this command.

---

**Examples** The following example shows how to configure a Cisco IOS hosted NAT traversal for SBC:

```
interface ethernet1/1
 ip nat inside
 ip forwarding A
!
interface ethernet1/2
 ip nat inside
 ip forwarding B
!
interface ethernet1/3
 ip nat outside
!
ip nat pool call-id-pool 1.1.1.1 1.1.1.100
ip nat pool outside-pool 2.2.2.1.1.1 2.2.2.1.1.10
ip nat pool inside-pool-A 169.1.1.1 169.1.1.10
ip nat pool inside-pool-B 170.1.1.1 170.1.1.10
ip nat inside source list 1 pool inside-pool-A vrf A overload
ip nat inside source list 2 pool inside-pool-B vrf B overload
ip nat outside list 3 pool outside-pool
ip nat inside source list 4 pool call-id-pool
!
access-list for VRF-A inside-phones
access-list 1 permit 10.1.1.0 0.0.0.255
access-list 2 permit 172.1.1.0 0.0.0.255
!
access-list for call-id-pool
access-list 4 permit 10.1.1.0 0.0.0.255
access-list 4 permit 20.1.1.0 0.0.0.255
!
ip nat sip-sbc
 proxy 200.1.1.1 5060 192.1.1.1 5060 protocol udp
 vrf-list
  vrf-name A
```

```
vrf-name B
call-id-pool call-id-pool
session-timeout 300

mode allow-flow-around
override address
```

**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>	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 source

To enable Network Address Translation (NAT) on a virtual interface without inside or outside specification, use the **ip nat source** command in global configuration mode.

## Dynamic NAT

```
ip nat source {list {access-list-number / access-list-name} interface type number | pool name}  
[overload / vrf name]
```

```
no ip nat source {list {access-list-number / access-list-name} interface type number | pool name}  
overload / vrf name]
```

## Static NAT

```
ip nat source {static {esp local-ip interface type number | local-ip global-ip} } [extendable |  
no-alias | no-payload | vrf name]
```

```
no ip nat source {static {esp local-ip interface type number | local-ip global-ip} } [extendable |  
no-alias | no-payload | vrf name]
```

## Port Static NAT

```
ip nat source {static {tcp | udp {local-ip local-port global-ip global-port | interface global-port} }  
[extendable | no-alias | no-payload | vrf name]
```

```
no ip nat source {static {tcp | udp {local-ip local-port global-ip global-port | interface  
global-port} } } [extendable | no-alias | no-payload | vrf name]
```

## Network Static NAT

```
ip nat source static network local-network global-network mask [extendable | no-alias |  
no-payload | vrf name]
```

```
no ip nat source static network local-network global-network mask [extendable | no-alias |  
no-payload | vrf name]
```

## Syntax Description

<b>list</b> <i>access-list-number</i>	Number of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
<b>list</b> <i>access-list-name</i>	Name of a standard IP access list. Packets with source addresses that pass the access list are dynamically translated using global addresses from the named pool.
<b>interface</b> <i>type</i>	Specifies the interface type for the global address.
<b>interface</b> <i>number</i>	Specifies the interface number for the global address.
<b>pool</b> <i>name</i>	Name of the pool from which global IP addresses are allocated dynamically.
<b>overload</b>	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or User Datagram Protocol (UDP) port number of each inside host distinguishes between the multiple conversations using the same local IP address.

<b>vrf</b> <i>name</i>	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
<b>static</b> <i>local-ip</i>	Sets up a single static translation. The <i>local-ip</i> argument establishes the local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from the RFC 1918, or obsolete.
<i>local-port</i>	Sets the local TCP/UDP port in a range from 1 to 65535.
<b>static</b> <i>global-ip</i>	Sets up a single static translation. The <i>local-ip</i> argument establishes the globally unique IP address of an inside host as it appears to the outside network.
<i>global-port</i>	Sets the global TCP/UDP port in the range from 1 to 65535.
<b>extendable</b>	(Optional) Extends the translation.
<b>no-alias</b>	(Optional) Prohibits as alias from being created for the global address.
<b>no-payload</b>	(Optional) Prohibits the translation of an embedded address or port in the payload.
<b>esp</b> <i>local-ip</i>	Establishes IPSec-ESP (tunnel mode) support.
<b>tcp</b>	Establishes the Transmission Control Protocol.
<b>udp</b>	Establishes the User Datagram Protocol.
<b>network</b> <i>local-network</i>	Specified the local subnet translation.
<i>global-network</i>	Specifies the global subnet translation.
<i>mask</i>	Establishes the IP network mask to be used with subnet translations.

**Command Modes** Global Configuration

Command History	Release	Modification
	12.3(14)T	This command was introduced.

**Examples** The following example shows how to configure a virtual interface without inside or outside specification for the global address:

```
ip nat source list 1 pool NAT vrf bank overload
ip nat source list 1 pool NAT vrf park overload
ip nat source static 192.168.123.1 192.168.125.10 vrf services
```

Related Commands	Command	Description
	<b>ip nat enable</b>	Configures an interface connecting VPNs and the Internet for NAT translation.
	<b>ip nat pool</b>	Defines a pool of IP addresses for Network Address Translation.

## ip nat stateful id

To designate the members of a translation group, use the **ip nat stateful id** command in global configuration mode. To disable the members of a translation group or reset default values, use the **no** form of this command.

```
ip nat stateful id id-number {redundancy name mapping-id map-number [protocol {tcp | udp}]
[as-queuing {disable | enable}] | {primary ip-address-primary backup ip-address-backup
peer ip-address-peer mapping-id mapping-id-number}
```

```
no ip nat stateful id id-number
```

Syntax Description	<i>id-number</i>	Unique number given to each router in the stateful translation group.
	<b>redundancy name</b>	Establishes Hot Standby Routing Protocol (HSRP) as the method of redundancy.
	<b>mapping-id</b> <i>map-number</i>	Specifies whether or not the local Stateful (SNAT) router will distribute a particular set of locally created entries to a peer SNAT router.
	<b>protocol</b>	(Optional) Enables the HSRP UDP default to be changed to TCP.
	<b>tcp</b>	(Optional) Establishes the Transmission Control Protocol.
	<b>udp</b>	(Optional) Establishes the User Datagram Protocol.
	<b>as-queuing</b>	(Optional) Enables asymmetric routing during queuing for HSRP to be disabled.
	<b>disable</b>	(Optional) Disables asymmetric routing during queuing in HSRP mode.
	<b>enable</b>	(Optional) Enables asymmetric routing during queuing in HSRP mode.
	<b>primary</b> <i>ip-address-primary</i>	Manually establishes redundancy for the primary router.
	<b>backup</b> <i>ip-address-backup</i>	Manually establishes redundancy for the backup router.
	<b>peer</b> <i>ip-address-peer</i>	Specifies the IP address of the peer router in the translation group.

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.2(13)T	This command was introduced.
	12.4(3)	The <b>protocol</b> and <b>as-queuing</b> keywords were added.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

## Usage Guidelines

This command has two forms: HSRP stateful NAT and manual stateful NAT. The form that uses the keyword **redundancy** establishes the HSRP redundancy method. When HSRP mode is set, the primary and backup NAT routers are elected according to the HSRP standby state. To enable stateful NAT manually, configure the primary router and backup router.

In HSRP mode, the default TCP can be changed to UDP by using the optional **protocol udp** keywords with the **redundancy** keyword.

To disable the queuing during asymmetric routing in HSRP mode, use the optional **as-queuing disable** keywords with the **redundancy** keyword.

## Examples

The following example shows how to configure SNAT with HSRP:

```
!
standby SNATSRSP ip 10.1.1.1 secondary
standby delay reload 60
standby 1 preempt delay minimum 60 reload 60 sync 60
!
ip nat Stateful id 1
redundancy SNATSRSP
mapping-id 10
as-queuing disable
protocol udp
ip nat pool SNATPOOL1 10.1.1.1 10.1.1.9 prefix-length 24
ip nat inside source route-map rm-101 pool SNATPOOL1 mapping-id 10 overload
ip classless
ip route 10.1.1.0 255.255.255.0 Null0
no ip http server
ip pim bidir-enable
```

The following example shows how to manually configure SNAT:

```
ip nat stateful id 1
primary 10.88.194.17
peer 10.88.194.18
mapping-id 10

ip nat stateful id 2
backup 10.88.194.18
peer 10.88.194.17
mapping-id 10
```

## 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.

# ip nat translation

The **ip nat translation** command is replaced by the **ip nat translation (timeout)** and **ip nat translation max-entries** commands. See these commands for more information.



# ip nat translation (timeout)

To change the amount of time after which Network Address Translation (NAT) translations time out, use the **ip nat translation** command in global configuration mode. To disable the timeout, use the **no** form of this command.

```
ip nat translation { timeout | udp-timeout | dns-timeout | tcp-timeout | finrst-timeout |  
                    icmp-timeout | pptp-timeout | syn-timeout | port-timeout | arp-ping-timeout } {seconds |  
                    never}
```

```
no ip nat translation { timeout | udp-timeout | dns-timeout | tcp-timeout | finrst-timeout |  
                    icmp-timeout | pptp-timeout | syn-timeout | port-timeout | arp-ping-timeout}
```

Syntax Description		
<b>timeout</b>		Specifies that the timeout value applies to dynamic translations except for overload translations. Default is 86,400 seconds (24 hours).
<b>udp-timeout</b>		Specifies that the timeout value applies to the User Datagram Protocol (UDP) port. Default is 300 seconds (5 minutes).
<b>dns-timeout</b>		Specifies that the timeout value applies to connections to the Domain Name System (DNS). Default is 60 seconds.
<b>tcp-timeout</b>		Specifies that the timeout value applies to the TCP port. Default is 86,400 seconds (24 hours).
<b>finrst-timeout</b>		Specifies that the timeout value applies to Finish and Reset TCP packets, which terminate a connection. Default is 60 seconds.
<b>icmp-timeout</b>		Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. Default is 60 seconds.
<b>pptp-timeout</b>		Specifies the timeout value for NAT Point-to-Point Tunneling Protocol (PPTP) flows. Default is 86,400 seconds (24 hours).
<b>syn-timeout</b>		Specifies the timeout value for TCP flows immediately after a synchronous transmission (SYN) message that consists of digital signals that are sent with precise clocking. The default is 60 seconds.
<b>port-timeout</b>		Specifies that the timeout value applies to the TCP/UDP port.
<b>arp-ping-timeout</b>		Specifies that the timeout value applies to the arp ping.
<i>seconds</i>		Number of seconds after which the specified port translation times out. The default is 0.
<b>never</b>		Specifies no port translation time out.

## Defaults

**timeout:** 86,400 seconds (24 hours)  
**udp-timeout:** 300 seconds (5 minutes)  
**dns-timeout:** 60 seconds (1 minute)  
**tcp-timeout:** 86,400 seconds (24 hours)  
**finrst-timeout:** 60 seconds (1 minute)  
**icmp-timeout:** 60 seconds (1 minute)  
**pptp-timeout:** 86,400 seconds (24 hours)  
**syn-timeout:** 60 seconds (1 minute)  
*seconds:* 0 (never)

**Command Modes** Global configuration

Command History	Release	Modification
	11.2	This command was introduced.
	12.3(4)T	The timeout functions of the <b>ip nat translation</b> command were documented under the command name <b>ip nat translation (timeout)</b> .
	12.4(6)T	The <b>arp-ping-timeout</b> keyword was added.

**Usage Guidelines** When port translation is configured, each entry contains more context about the traffic that is using it, which gives you finer control over translation entry timeouts. Non-DNS UDP translations time out after 5 minutes, and DNS times out in 1 minute. TCP translations time out in 24 hours, unless an RST or FIN bit is seen on the stream, in which case they will time out in 1 minute.

**Examples** The following example configures the router to cause UDP port translation entries to time out after 10 minutes (600 seconds):

```
ip nat translation udp-timeout 600
```

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>ip nat translation max-entries</b>	Limits the maximum number of NAT entries.
	<b>show ip nat statistics</b>	Displays NAT statistics.
	<b>show ip nat translations</b>	Displays active NAT translations.

# ip nat translation max-entries

To limit the size of a Network Address Translation (NAT) table to a specified maximum, use the **ip nat translation max-entries** command in global configuration mode. To remove a specified limit, use the **no** form of this command.

**ip nat translation max-entries** {*number* | **all-host** *number* | **all-vrf** *number* | **host** *ip-address* *number* | **list** {*listname* | *number*} | **vrf** *name* *number*}

**no ip nat translation max-entries** {*number* | **all-host** *number* | **all-vrf** *number* | **host** *ip-address* *number* | **list** {*listname* | *number*} | **vrf** *name* *number*}

## Syntax Description

<i>number</i>	Maximum number of allowed NAT entries. Range is from 1 to 2147483647.
<b>all-host</b>	Constrains each host by the specified number of NAT entries.
<b>all-vrf</b>	Constrains each VPN routing and forwarding (VRF) instance by the specified NAT limit.
<b>host</b>	Constrains an IP address by the specified NAT limit.
<i>ip-address</i>	The IP address subject to the NAT limit.
<b>list</b>	Constrains an access control list (ACL) by the specified NAT limit.
<i>listname</i>	The ACL name subject to the NAT limit.
<b>vrf</b>	Constrains an individual VRF instance by the specified NAT limit.
<i>name</i>	The name of the VRF instance subject to the NAT limit.

## Defaults

No maximum size is specified for the NAT table.

## Command Modes

Global configuration (config)

## Command History

Release	Modification
12.3(4)T	This command was introduced.

## Usage Guidelines

Before you configure a NAT rate limit, you should first classify current NAT usage and determine the sources of requests for NAT translations. If a specific host, access control list, or VRF instance is generating an unexpectedly high number of NAT requests, it may be the source of a malicious virus or worm attack.

Once you have identified the source of excess NAT requests, you can set a NAT rate limit that constrains a specific host, access control list, or VRF instance, or you can set a general limit for the maximum number of NAT requests allowed regardless of their source.



### Note

When using the **no** form of **ip nat translation max-entries**, you must specify the type of NAT rate limit you wish to remove and its current value. For more information about how to display current NAT rate limit settings, refer to the **show ip nat statistics** command.

## Examples

The following examples show how to configure rate limiting NAT translation.

### Setting a General NAT Limit

The following example shows how to limit the maximum number of allowed NAT entries to 300:

```
ip nat translation max-entries 300
```

### Setting NAT Limits for VRF Instances

The following example shows how to limit each VRF instance to 200 NAT entries:

```
ip nat translation max-entries all-vrf 200
```

The following example shows how to limit the VRF instance named vrf1 to 150 NAT entries:

```
ip nat translation max-entries vrf vrf1 150
```

The following example shows how to limit the VRF instance named vrf2 to 225 NAT entries, but limit all other VRF instances to 100 NAT entries each:

```
ip nat translation max-entries all-vrf 100
ip nat translation max-entries vrf vrf2 225
```

### Setting NAT Limits for Access Control Lists

The following example shows how to limit the access control list named vrf3 to 100 NAT entries:

```
ip nat translation max-entries list vrf3 100
```

### Setting NAT Limits for an IP Address

The following example shows how to limit the host at IP address 10.0.0.1 to 300 NAT entries:

```
ip nat translation max-entries host 10.0.0.1 300
```

## 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>ip nat translation (timeout)</b>	Changes the NAT timeout value.
<b>show ip nat statistics</b>	Displays NAT statistics.
<b>show ip nat translations</b>	Displays active NAT translations.

# show ip snat

To display active Stateful Network Address Translation (SNAT) translations, use the **show ip snat** command in EXEC mode.

**show ip snat** [**distributed** [**verbose**] | **peer** *ip-address*]

Syntax Description	<b>distributed</b>	(Optional) Displays information about the distributed NAT, including its peers and status.
	<b>verbose</b>	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.
	<b>peer</b> <i>ip-address</i>	(Optional) Displays TCP connection information between peer routers.

Command Modes	EXEC
---------------	------

Command History	<b>Release</b>	<b>Modification</b>
	12.2(13)T	This command was introduced.

**Examples** The following is sample output from the **show ip snat distributed** command for stateful NAT connected peers:

```
Router# show ip snat distributed
```

```
Stateful NAT Connected Peers
```

```
SNAT: Mode PRIMARY
:State READY
:Local Address 192.168.123.2
:Local NAT id 100
:Peer Address 192.168.123.3
:Peer NAT id 200
:Mapping List 10
```

The following is sample output from the **show ip snat distributed verbose** command for stateful NAT connected peers:

```
Router# show ip snat distributed verbose
```

```
SNAT: Mode PRIMARY
Stateful NAT Connected Peers

:State READY
:Local Address 192.168.123.2
:Local NAT id 100
:Peer Address 192.168.123.3
:Peer NAT id 200
:Mapping List 10
:InMsgs 7, OutMsgs 7, tcb 0x63EBA408, listener 0x0
```

# show ip nat statistics

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

## show ip nat statistics

**Syntax Description** This command has no arguments or keywords.

**Command Modes** EXEC

Command History	Release	Modification
	11.2	This command was introduced.

**Examples** The following is sample output from the **show ip nat statistics** command:

```
Router# show ip nat statistics

Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135 Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208 refcount 2
  pool net-208: netmask 255.255.255.240
    start 172.69.233.208 end 172.69.233.221
    type generic, total addresses 14, allocated 2 (14%), misses 0
```

[Table 25](#) describes the significant fields shown in the display.

**Table 25** *show ip nat statistics Field Descriptions*

Field	Description
Total translations	Number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or times out.
Outside interfaces	List of interfaces marked as outside with the <b>ip nat outside</b> command.
Inside interfaces	List of interfaces marked as inside with the <b>ip nat inside</b> command.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.
Expired translations	Cumulative count of translations that have expired since the router was booted.

**Table 25** *show ip nat statistics Field Descriptions (continued)*

Field	Description
Dynamic mappings	Indicates that the information that follows is about dynamic mappings.
Inside Source	The information that follows is about an inside source translation.
access-list	Access list number being used for the translation.
pool	Name of the pool (in this case, net-208).
refcount	Number of translations using this pool.
netmask	IP network mask being used in the pool.
start	Starting IP address in the pool range.
end	Ending IP address in the pool range.
type	Type of pool. Possible types are generic or rotary.
total addresses	Number of addresses in the pool available for translation.
allocated	Number of addresses being used.
misses	Number of failed allocations from the pool.

**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 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 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</b> <i>vrf-name</i>	(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.

## Command Modes

EXEC

## Command History

Release	Modification
11.2	This command was introduced.
12.2(13)T	The <b>vrf</b> <i>vrf-name</i> 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
--- 10.69.233.209      192.168.1.95      ---                ---
--- 10.69.233.210      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 10.69.233.209:1220  192.168.1.95:1220  172.69.2.132:53    172.69.2.132:53
tcp 10.69.233.209:11012 192.168.1.89:11012 172.69.1.220:23     172.69.1.220:23
tcp 10.69.233.209:1067   192.168.1.95:1067  172.69.1.161:23     172.69.1.161:23
```

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

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



```

Pro Inside global      Inside local      Outside local      Outside global
udp 172.69.233.209:1220 192.168.1.95:1220 172.69.2.132:53    172.69.2.132:53
      create 00:00:02, use 00:00:00, flags: extended
tcp 172.69.233.209:11012 192.168.1.89:11012 172.69.1.220:23     172.69.1.220:23
      create 00:01:13, use 00:00:50, flags: extended
tcp 172.69.233.209:1067 192.168.1.95:1067 172.69.1.161:23     172.69.1.161:23
      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 abc
```

```

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    192.168.22.20:0
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    192.168.22.20:0
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 26 describes the significant fields shown in the display.

**Table 26** *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 26 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>	Enables a port other than the default port.
<b>show ip nat statistics</b>	Displays NAT statistics.