



NAT Commands

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 { * | forced | [piggyback-internal | esp | tcp | udp] [inside global-ip
[global-port] local-ip [local-port] outside local-ip global-ip] | inside global-ip local-ip
[forced] | outside local-ip global-ip [forced] }
```

Syntax Description	
*	Clears all dynamic translations.
forced	(Optional) Forces the clearing of either: <ul style="list-style-type: none"> all dynamic entries, whether or not there are any child translations. a single dynamic half-entry and any existing child translations, whether or not there are any child translations.
piggyback-internal	(Optional) Clears translations created off of piggyback data.
esp	(Optional) Clears Encapsulating Security Payload (ESP) entries from the translation table.
tcp	(Optional) Clears the TCP entries from the translation table.
udp	(Optional) Clears the User Datagram Protocol (UDP) entries from the translation table.
inside	(Optional) Clears the inside translations containing the specified <i>global-ip</i> and <i>local-ip</i> addresses. If used without the forced keyword, clears only those entries that do not have child translations.
<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.
outside	(Optional) Clears the outside translations containing the specified <i>global</i> and <i>local</i> addresses. If used without the forced keyword, clears only those entries that do not have child translations.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(15)T	The esp keyword was added.
	12.4(2)T	The piggyback-internal keyword was added.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 2.4.2	The forced keyword was extended to support the removal of a half entry regardless of whether it has any child translations.

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   10.69.233.209:1220  10.168.1.95:1220  10.69.2.132:53   10.69.2.132:53
tcp   10.69.233.208       10.168.1.94
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
```

```
Router# clear ip nat translation udp inside 10.69.233.209 1220 10.168.1.95 1220
outside 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   10.69.233.208       10.168.1.94
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
```

```
Router# clear ip nat translation inside 10.69.233.208 10.168.1.94 forced
```

```
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
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	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# clear ip snat translation distributed *
```

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.
refresh	(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** | **Stateful** | **create** | **piggyback-support** | **pool** | **portmap** | **service** | **sip-sbc** | **source** | **log** | **translations** | **syslog** | **allow-static-host**]

no ip nat [**inside** | **outside** | **Stateful** | **create** | **piggyback-support** | **pool** | **portmap** | **service** | **sip-sbc** | **source** | **log** | **translations** | **syslog** | **allow-static-host**]

Syntax Description

allow-static-host	(Optional) Enables static IP address support for NAT translation.
create	(Optional) Creates NAT flow entries.
inside	(Optional) Indicates that the interface is connected to the inside network (the network subject to NAT translation).
log	(Optional) Enables NAT logging.
outside	(Optional) Indicates that the interface is connected to the outside network.
piggyback-support	(Optional) Enables NAT Piggybacking support.
pool	(Optional) Defines pool of addresses.
portmap	(Optional) Defines portmap of portranges.
service	(Optional) Indicates special translation for application using non-standard port.
sip-sbc	(Optional) Indicates SIP Session Border Controller commands.
source	(Optional)
Stateful	(Optional)
syslog	(Optional) Enables syslog for NAT logging translations.
translations	(Optional) Enables NAT logging translations.

Command Default

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 allow-static-host keyword was added.
12.3(7)T	This command was implemented in Cisco IOS Release 12.3(7)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(22)T	This command is integrated into the Cisco IOS Release 12.2(22)T. The allow-static-host keyword was removed.

ip nat create flow-entries

To create Network Address Translation (NAT) flow entries, use the **ip nat create** command in global configuration mode. To disable the flow cache, use the **no** form of this command.

ip nat create flow-entries

no ip nat create flow-entries

Syntax Description

This command has no arguments or keywords.

Command Default

Flow entries are created.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

To scale the performance of NAT, an enhancement is created that allows for a flow table for NAT entries.

Examples

The following example shows how to create NAT flow entries:

```
Router(config)# no ip nat create flow-entries
```

Related Commands

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

Syntax Description This command has no arguments or keywords.

Command Modes Interface configuration

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

Examples 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
```

Related Commands	Command	Description
	ip nat pool	Defines a pool of IP addresses for Network Address Translation.
	ip nat source	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

list <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.
list <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.
pool <i>name</i>	Name of the pool from which global IP addresses are allocated during dynamic translation.
mapping-id <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 mapping-id <i>map-id</i> keyword and argument combination was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	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]
[match-in-vrf] [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]
[match-in-vrf] [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 | reversible
| vrf name] [match-in-vrf]
```

```
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 |
reversible | vrf name] [match-in-vrf]
```

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 | reversible | vrf name] [match-in-vrf]
```

```
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 | reversible | vrf name] [match-in-vrf]
```

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 | 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 | vrf name]
```

Syntax Description

list <i>access-list-number</i>	Specifies the 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.
list <i>access-list-name</i>	Specifies the 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.
route-map <i>name</i>	Specifies the named route map.

interface <i>type number</i>	Specifies the interface type and number for the global address.
pool <i>name</i>	Specifies the name of the pool from which global IP addresses are allocated dynamically.
mapping-id <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.
overload	(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.
reversible	(Optional) Enables outside-to-inside initiated sessions to use route maps for destination-based NAT.
vrf <i>name</i>	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
match-in-vrf	(Optional) Enables NAT inside and outside traffic in the same VRF.
oer	(Optional) Allows Optimized Edge Routing (OER) to operate NAT and control traffic class routing.
static <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>	The local TCP/UDP port in a range from 1 to 65535.
static <i>global-ip</i>	Sets up a single static translation. The <i>global-ip</i> argument establishes the globally unique IP address of an inside host as it appears to the outside network.
<i>global-port</i>	The global TCP/UDP port in a range from 1 to 65535.
extendable	(Optional) Extends the translation.
no-alias	(Optional) Prohibits an alias from being created for the global address.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
redundancy <i>group-name</i>	(Optional) Establishes NAT redundancy.
esp <i>local-ip</i>	Establishes IPsec-ESP (tunnel mode) support.
tcp	Establishes the Transmission Control Protocol (TCP).
udp	Establishes the User Datagram Protocol (UDP).
network <i>local-network</i>	Specifies the local subnet translation.
<i>global-network</i>	The global subnet translation.
<i>mask</i>	The IP Network mask to be used with subnet translations.

Defaults

No NAT translation of inside source addresses occurs.

Command Modes

Global configuration (config)

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 route-map <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 redundancy <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 no-payload keyword was added.
12.2(13)T	The interface keyword was added for static translations. The mapping-id <i>map-id</i> keyword and argument combination was added for dynamic translations. The vrf <i>name</i> keyword and argument combination was added.
12.3(7)T	The static mapping-id <i>map-id</i> keyword and argument combination was added.
12.4(3)T	The reversible keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	The oer keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

For information about the limitations when this command was integrated into Cisco IOS XE Release 2.5, see the [Cisco IOS XE 2 Release Notes](#).

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 keyword **static** establishes a single static translation.



Note

When a session is initiated from outside with the source IP as the outside global address, the router is unable to determine the destination VRF of the packet. Use the **match-in-vrf** keyword to enable the IP alias installation to work correctly when routing NAT inside and outside traffic in the same VRF.

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 171.69.233.208/28 network:

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
```

```

interface ethernet 1
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255

```

The following example shows how to translate only traffic local to the provider's edge device running NAT (NAT-PE):

```

ip nat inside source list 1 interface ethernet 0 vrf shop overload
ip nat inside source list 1 interface ethernet 0 vrf bank overload
!
ip route vrf shop 0.0.0.0 0.0.0.0 192.1.1.1
ip route vrf bank 0.0.0.0 0.0.0.0 192.1.1.1
!
access-list 1 permit 10.1.1.1.0 0.0.0.255
!
ip nat inside source list 1 interface ethernet 1 vrf shop overload
ip nat inside source list 1 interface ethernet 1 vrf bank overload
!
ip route vrf shop 0.0.0.0 0.0.0.0 172.1.1.1 global
ip route vrf bank 0.0.0.0 0.0.0.0 172.1.1.1 global
access-list 1 permit 10.1.1.0 0.0.0.255

```

The following example shows how to translate sessions from outside-to-inside.

```

ip nat pool POOL-A 10.1.10.1 10.1.10.126 255.255.255.128
ip nat pool POOL-B 10.1.20.1 10.1.20.126 255.255.255.128

ip nat inside source route-map MAP-A pool POOL-A reversible
ip nat inside source route-map MAP-B pool POOL-B reversible
!
ip access-list extended ACL-A
 permit ip any 10.1.10.128 0.0.0.127
ip access-list extended ACL-B
 permit ip any 10.1.20.128 0.0.0.127
!
MAP-A permit 10
 match ip address ACL-A
!
route-map MAP-B permit 10
 match ip address ACL-B
!

```

The following example shows how to configure route map R1 to allow outside-to-inside translation for static NAT:

```

ip nat inside source static 10.1.1.1 10.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
 permit ip any 10.1.10.128 0.0.0.127

route-map R1 permit 10
 match ip address ACL-A

```

The following example shows how to configure NAT inside and outside traffic in the same VRF:

```

interface Loopback1
 ip vrf forwarding blue
 ip address 192.168.199.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!

```

```

interface Ethernet0/0
 ip vrf forwarding blue
 ip address 192.168.1.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly

ip nat pool MYPPOOL 192.168.1.5 192.168.1.5 prefix-length 24
ip nat inside source list acl-nat pool MYPPOOL vrf blue overload
!
!
ip access-list extended acl-nat
 permit ip 192.168.199.0 0.0.0.255 any

```

Related Commands

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

ip nat log

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

ip nat log translations syslog

no ip nat log translations syslog

Syntax Description

translations	Enables the NAT logging translations.
syslog	Enables the writing of NAT log to syslog.

Command Default

No pool of addresses is defined.

Command Modes

Global configuration (config)

Command History

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

Examples

The following example shows how to define a set of log translations.

```
Router(config)# ip nat log translations syslog
```

Related Commands

Command	Description
clear ip nat translation	Clears dynamic NAT translations from the translation table.
debug ip nat	Displays information about IP packets translated by NAT.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside source	Enables NAT of the inside destination address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Enables NAT of the outside source address.
show ip nat translations	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

list <i>access-list-number</i>	Specifies the 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.
list <i>access-list-name</i>	Specifies the 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.
route-map <i>name</i>	Specifies a named route map.
pool <i>pool-name</i>	Specifies the name of the pool from which global IP addresses are allocated.
add-route	(Optional) Adds a static route for the outside local address.

mapping-id <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.
vrf <i>name</i>	(Optional) Associates the NAT translation rule with a particular Virtual Private Network (VPN).
static	Sets up a single static translation.
<i>global-ip</i>	Specifies the globally unique IP address assigned to a host on the outside network by its owner. The address was allocated from globally routable network space.
<i>local-ip</i>	Specifies the 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>).
<i>global-port</i>	Specifies the port number assigned to a host on the outside network by its owner.
<i>local-port</i>	Specifies the port number of an outside host as it appears to the inside network.
static network	Sets up a single static network translation.
<i>global-network</i>	Specifies the globally unique network address assigned to a host on the outside network by its owner. The address was allocated from globally routable network space.
<i>local-network</i>	Specifies the local network address of an outside host as it appears to the inside network. The address was allocated from address space routable on the inside.
<i>mask</i>	Subnet mask for the networks that will be translated.
extendable	(Optional) Extends the transmission.
no-alias	(Optional) Prohibits an alias from being created for the local address.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
redundancy <i>group-name</i>	(Optional) Enables the NAT redundancy operation.
tcp	Establishes the Transmission Control Protocol (TCP).
udp	Establishes the User Datagram Protocol (UDP).

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 redundancy <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 no-payload keyword was added.

Release	Modification
12.2(13)T	The mapping-id <i>map-id</i> keyword and argument combination was added for dynamic translations. The vrf <i>name</i> keyword and argument combination was added.
12.3(7)T	The mapping-id <i>map-id</i> keyword and argument combination was added for static translations.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

For information about the limitations when this command was integrated into Cisco IOS XE Release 2.5, see the [Cisco IOS XE 2 Release Notes](#).

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 general 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 group1 and group2 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
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	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. To disable a NAT optimized SIP media path, use the **no** form of this command.

```
ip nat log piggyback-support sip-alg {sdp-only | all-messages} router router-id
md5-authentication [md5-authentication-key]
```

```
no ip nat log piggyback-support sip-alg {sdp-only | all-messages} router router-id
md5-authentication [md5-authentication-key]
```

Syntax Description

sip	Indicates Session Initiation Protocol (SIP) commands.
sdp-only	Establishes piggybacking in SDP only.
all-messages	Establishes piggybacking in all messages except SDP.
router <i>router-id</i>	Piggyback router ID number.
md5-authentication <i>md5-authentication key</i>	(Optional) MD5 authentication key.

Command Default

No messages are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Examples

The following example shows how to enable a NAT optimized message including MD5 authentication.

```
Router(config)#ip nat piggyback-support sip-alg sdp-only router 100 authentication md5-key
!
```

Related Commands

Command	Description
ip nat inside destination	Enables NAT of the inside destination address.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside source	Enables NAT of the inside destination address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Enables NAT of the outside source address.
ip nat service	Enables a port other than the default port.

Command	Description
show ip nat statistics	Displays NAT statistics.
show ip nat translations	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] [nopreservation]
```

```
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] [nopreservation]
```

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.
netmask <i>netmask</i>	Specifies the 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.
prefix-length <i>prefix-length</i>	Specifies the 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.
add-route	(Optional) Specifies that a route has been added to the NAT Virtual Interface (NVI) interface for the global address.
type	(Optional) Indicates the type of pool.
match-host	(Optional) Specifies that the host number is to remain the same after translation.
rotary	(Optional) Indicates that the range of addresses in the address pool identifies real, inside hosts among which TCP load distribution will occur.
accounting <i>list-name</i>	(Optional) Indicates the RADIUS profile name that matches the RADIUS configuration in the router.
arp-ping	(Optional) Determines static IP client instances and restarts the NAT entry timer.
nopreservation	(Optional) Enables all the IP addresses in the pool to be used for dynamic translation.

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 accounting 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 add-route keyword was added.

Release	Modification
12.4(6)T	The arp-ping keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	The nopreservation 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.

The **nopreservation** keyword is used after the **prefix-length** or **netmask** keywords. It turns off the default behavior, which is known as IP address reservation. The **no** form of the command with the **nopreservation** keyword enables the default behavior, and reserves the first IP address in the NAT pool, making it unavailable for dynamic translation.

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
clear ip nat translation	Clears dynamic NAT translations from the translation table.
debug ip nat	Displays information about IP packets translated by NAT.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside source	Enables NAT of the inside destination address.
ip nat outside source	Enables NAT of the outside source address.
ip nat service	Enables a port other than the default port.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	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 | allow-h323-even-rtp-ports | allow-h323-keepalive |
allow-sip-even-rtp-ports | allow-skinny-even-rtp-ports | fullrange { tcp | udp } port
port-number | list { access-list-number | access-list-name } { ESP spi-match | IKE
preserve-port | ftp tcp port port-number } | mgcp | nbar | ras | rtsp | sip { tcp | udp } port
port-number | skinny tcp port port-number | port-randomization | alg { tcp | udp } dns |
allow-multipart }
```

```
no ip nat service { H225 | allow-h323-even-rtp-ports | allow-h323-keepalive |
allow-sip-even-rtp-ports | allow-skinny-even-rtp-ports | fullrange { tcp | udp } port
port-number | list { access-list-number | access-list-name } { ESP spi-match | IKE
preserve-port | ftp tcp port port-number } | mgcp | nbar | ras | rtsp | sip { tcp | udp } port
port-number | skinny tcp port port-number | port-randomization | alg { tcp | udp } dns |
allow-multipart }
```

Syntax Description

H225	H323-H225 protocol.
allow-h323-even-rtp-ports	Even-numbered RTP ports for the H323 protocol.
allow-h323-keepalive	H323 keepalive.
allow-sip-even-rtp-ports	Even-numbered RTP ports for the Session Initiation Protocol (SIP).
allow-skinny-even-rtp-ports	Even-numbered RTP ports for the skinny protocol.
fullrange	All available ports. The range is from 1 to 65535.
tcp	TCP.
udp	User Datagram Protocol (UDP).
port <i>port-number</i>	Port other than the default port in the range from 1 to 65533.
list <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.
ESP	Security Parameter Index (SPI) matching IPsec pass-through.
spi-match	SPI matching IPsec pass-through. The ESP endpoints must also have SPI matching enabled.
IKE	Preserve Internet Key Exchange (IKE) port, as required by some IPsec servers.
preserve-port	Preserve the UDP port in IKE packets.
ftp	FTP.
mgcp	Media gateway control protocol (MGCP).
nbar	Network-Based Application Recognition.
ras	H323-RAS (Registration, Admission, and Status) protocol.
rtsp	Real Time Streaming Protocol. This protocol is enabled by default on port 554 and requires NBAR.
sip	SIP.
skinny	Skinny protocol.
port-randomization	Ports are allocated randomly for NAT, instead of sequentially.

alg {tcp udp} dns	Enables Domain Name Service (DNS) processing with an Application-Level Gateway (ALG) for either TCP or UDP.
allow-multipart	SIP multipart processing.

Command Default

RTSP is enabled and requires NBAR
H323 even-numbered RTP port allocation is enabled
SIP even-numbered RTP port allocation is enabled
Skinny even-numbered RTP port allocation is enabled
Port randomization is disabled
DNS ALG processing is enabled for TCP and UDP
SIP multipart processing is disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.
12.1(5)T	The skinny keyword was added.
12.2(8)T	The sip keyword was added.
12.2(15)T	The ESP and sip-match keywords were added to enable SPI matching on outside IPsec gateways. The ike and preserve-port keywords were added to enable outside IPsec gateways that require IKE source port 500.
12.3(7)T	The rtsp and mgcp keywords were added.
12.3(11)T	The allow-sip-even-rtp-ports keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4	The nbar keyword was added.
12.4(24)T	The port-randomization keyword was added.
15.0(1)M	The alg , dns , and allow-multipart keywords were 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 allow-h323-even-rtp-ports** command to force odd-numbered RTP port allocation for H323.

Use the **no ip nat service allow-sip-even-rtp-ports** command to force odd-numbered RTP port allocation for SIP.

Use the **no ip nat service allow-skinny-even-rtp-ports** command to force odd-numbered RTP port allocation for the skinny protocol.

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

A NAT-enabled Cisco device that is running Cisco IOS Release 12.3(7)T or a later release may experience an increase in CPU usage when upgrading from a previous release. RTSP and MGCP NAT ALG support was added in Release 12.3(7)T, which requires NBAR. You can use the **no ip nat service nbar** command to disable NBAR processing, which can decrease the CPU utilization rate.

The **port-randomization** keyword can be used to prevent a security threat caused by the possibility of predicting the next port number that NAT will allocate. This security threat is described in the Cisco Security Advisory titled [Multiple Cisco Products Vulnerable to DNS Cache Poisoning Attacks](#). Port randomization has the following limitations:

- It cannot be used with certain other NAT feature, including portmap, full-range, and SNAT.
- It is supported only for the port in the L4 header of the packet.

Use the **ip nat service allow-multipart** command to enable the processing of SIP multipart Session Description Protocol (SDP) packets.

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
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.

Command	Description
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

ip nat service enable-sym-port

To enable the endpoint agnostic port allocation, use the **ip nat service enable-sym-port** command in global configuration mode. To disable the endpoint agnostic port allocation, use the **no** form of this command.

ip nat service enable-sym-port

no ip nat service enable-sym-port

Syntax Description

This command has no arguments or keywords.

Command Default

If you do not issue this command, the *endpoint agnostic port allocation* is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

Use the **ip nat service enable-sym-port** command to enable the endpoint agnostic port allocation, which is also known as symmetric port allocation.



Note

Use this command before you enable Network Address Translation (NAT). If you enable the symmetric port database after creating entries in the NAT database, then corresponding entries are not added to the symmetric port database.

Examples

In the following example, an access list is created and the inside source address is translated using NAT. The endpoint agnostic port allocation is enabled after the inside source address is translated.

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# access list 1 permit 172.18.192.0 0.0.0.255
Router(config)# ip nat inside source list 1 interface Ethernet 0/0
Router(config)# ip nat service enable-sym-port
Router(config)# end
```

Following are the list of entries which are made to the SymmetricPort (Sym Port) table, debugs, and Symmetric DB (Sym DB) when the command is issued and when the command is not entered:

```
NAT Symmetric Port Database: 1 entries
public ipaddr:port [tableid] | port# [refcount][syscount] | localaddr:localport [flags]
172.18.192.69:1024 [0] | 1025 [1] [0] | 172.18.192.69:1024 [0]
```

Sample SymPort Debugs:

If SymDB is not enabled or initiated:

NAT-SymDB: DB is either not enabled or not initiated.

If an entry needs to be inserted into SymDB:

NAT-SymDB: insert 172.18.192.69 1024 0

172.18.192.69 is the local address, 1024 is the local port, and 0 is the tableid

If SymDB lookup found an entry:

NAT-SymDB: [0] Entry was found for 172.18.192.69 -> 10.10.10.1: wanted 1024 got 1025

172.18.192.69 is the local address, 10.10.10.1 is the global address, 1024 is the requested port, and 1025 is the allocated port

If entry was deleted from SymDB:

NAT-SymDB: deleting entry 172.18.192.69:1024

172.18.192.69 is the local address, 1024 is the local port.

Related Commands

Command	Description
show ip nat translations	Displays the list of translations entries.
show ip nat statistics	Displays the entries in the symmetric port database

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 {tcp | udp}
[call-id-pool pool-name] [override {address | none | port}] [mode allow-flow-around]
[mode allow-flow-through pool-name] [session-timeout {seconds | nat-default}]
[registration-throttle inside-timeout seconds outside-timeout seconds] [vrf-list vrf-name
vrf-name | no | exit]
```

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

Syntax Description

proxy	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.
<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.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.
call-id-pool <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.
override address	(Optional) Specifies the default override address mode.
override none	(Optional) Specifies that no override will be configured.
override port	(Optional) Specifies override port mode.
mode allow-flow-around	(Optional) Configures Real-Time Transport Protocol (RTP) for flow around for traffic between phones in the inside domain.
mode allow-flow-through <i>pool-name</i>	(Optional) Configures Real-Time Transport Protocol (RTP) for flow through for traffic between phones in the inside domain.
session-timeout <i>seconds</i>	(Optional) Configures the timeout duration for NAT entries pertaining to SIP signaling flows.
session-timeout nat-default	(Optional) Allows the default timeout to return to the NAT default timeout value of 5 minutes.
none	(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.
vrf-list vrf-name	(Optional) Defines SIP SBC VPN Routing and Forwarding (VRF) list names.

no	(Optional) Removes a name from the VRF list.
registration-throttle	(Optional) Defines the registration throttling parameter.
inside-timeout <i>seconds</i>	Timeout in seconds in the range of 1-536870.
outside-timeout <i>seconds</i>	Timeout in seconds in the range of 1-536870.
exit	(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.
	12.4(15)T	The allow-flow-through and registration-throttle sub commands were added.

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

list <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.
list <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.
interface <i>type</i>	Specifies the interface type for the global address.
interface <i>number</i>	Specifies the interface number for the global address.
pool <i>name</i>	Name of the pool from which global IP addresses are allocated dynamically.
overload	(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.

vrf <i>name</i>	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
static <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.
static <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.
extendable	(Optional) Extends the translation.
no-alias	(Optional) Prohibits as alias from being created for the global address.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
esp <i>local-ip</i>	Establishes IPSec-ESP (tunnel mode) support.
tcp	Establishes the Transmission Control Protocol.
udp	Establishes the User Datagram Protocol.
network <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
ip nat enable	Configures an interface connecting VPNs and the Internet for NAT translation.
ip nat pool	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.
redundancy <i>name</i>		Establishes Hot Standby Routing Protocol (HSRP) as the method of redundancy.
mapping-id <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.
protocol		(Optional) Enables the HSRP UDP default to be changed to TCP.
tcp		(Optional) Establishes the Transmission Control Protocol.
udp		(Optional) Establishes the User Datagram Protocol.
as-queuing		(Optional) Enables asymmetric routing during queuing for HSRP to be disabled.
disable		(Optional) Disables asymmetric routing during queuing in HSRP mode.
enable		(Optional) Enables asymmetric routing during queuing in HSRP mode.
primary <i>ip-address-primary</i>		Manually establishes redundancy for the primary router.
backup <i>ip-address-backup</i>		Manually establishes redundancy for the backup router.
peer <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 protocol and as-queuing 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 delay minimum 30 reload 60
standby 1 ip 10.1.1.1
standby 1 name SNATHSRP
standby 1 preempt delay minimum 60 reload 60 sync 60
!
ip nat Stateful id 1
redundancy SNATHSRP
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
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	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		
timeout	Specifies that the timeout value applies to dynamic translations except for overload translations. Default is 86,400 seconds (24 hours).	
udp-timeout	Specifies that the timeout value applies to the User Datagram Protocol (UDP) port. Default is 300 seconds (5 minutes).	
dns-timeout	Specifies that the timeout value applies to connections to the Domain Name System (DNS). Default is 60 seconds.	
tcp-timeout	Specifies that the timeout value applies to the TCP port. Default is 86,400 seconds (24 hours).	
finrst-timeout	Specifies that the timeout value applies to Finish and Reset TCP packets, which terminate a connection. Default is 60 seconds.	
icmp-timeout	Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. Default is 60 seconds.	
pptp-timeout	Specifies the timeout value for NAT Point-to-Point Tunneling Protocol (PPTP) flows. Default is 86,400 seconds (24 hours).	
syn-timeout	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.	
port-timeout	Specifies that the timeout value applies to the TCP/UDP port.	
arp-ping-timeout	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.	
never	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 ip nat translation command were documented under the command name ip nat translation (timeout) .
	12.4(6)T	The arp-ping-timeout keyword was added.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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
	clear ip nat translation	Clears dynamic NAT translations from the translation table.
	ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
	ip nat inside destination	Enables NAT of the inside destination address.
	ip nat inside source	Enables NAT of the inside source address.
	ip nat outside source	Enables NAT of the outside source address.
	ip nat pool	Defines a pool of IP addresses for NAT.
	ip nat service	Enables a port other than the default port.
	ip nat translation max-entries	Limits the maximum number of NAT entries.
	show ip nat statistics	Displays NAT statistics.
	show ip nat translations	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.
all-host	Constrains each host by the specified number of NAT entries.
all-vrf	Constrains each VPN routing and forwarding (VRF) instance by the specified NAT limit.
host	Constrains an IP address by the specified NAT limit.
<i>ip-address</i>	The IP address subject to the NAT limit.
list	Constrains an access control list (ACL) by the specified NAT limit.
<i>listname</i>	The ACL name subject to the NAT limit.
vrf	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
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Enables a port other than the default port.
ip nat translation (timeout)	Changes the NAT timeout value.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

show ip nat nvi statistics

To display NAT virtual interface (NVI) statistics, use the **show ip nat nvi statistics** command in user EXEC or privileged EXEC mode.

show ip nat nvi statistics

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC (>)
Privileged EXEC (#)

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

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

```
Router# show ip nat nvi statistics

Total active translations: 0 (0 static, 0 dynamic; 0 extended) NAT Enabled interfaces:
Hits: 0 Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0 Expired translations: 0 Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool pool1 refcount 1213 pool pool1: netmask 255.255.255.0
      start 192.168.1.10 end 192.168.1.253
      start 192.168.2.10 end 192.168.2.253
      start 192.168.3.10 end 192.168.3.253
      start 192.168.4.10 end 192.168.4.253
      type generic, total addresses 976, allocated 222 (22%), misses 0
[Id: 2] access-list 5 pool pool2 refcount 0 pool pool2: netmask 255.255.255.0
      start 192.168.5.2 end 192.168.5.254
      type generic, total addresses 253, allocated 0 (0%), misses 0
[Id: 3] access-list 6 pool pool3 refcount 3 pool pool3: netmask 255.255.255.0
      start 192.168.6.2 end 192.168.6.254
      type generic, total addresses 253, allocated 2 (0%), misses 0
[Id: 4] access-list 7 pool pool4 refcount 0 pool pool4 netmask 255.255.255.0
      start 192.168.7.30 end 192.168.7.200
      type generic, total addresses 171, allocated 0 (0%), misses 0
[Id: 5] access-list 8 pool pool5 refcount 109195 pool pool5: netmask 255.255.255.0
      start 192.168.10.1 end 192.168.10.253
      start 192.168.11.1 end 192.168.11.253
      start 192.168.12.1 end 192.168.12.253
      start 192.168.13.1 end 192.168.13.253
      start 192.168.14.1 end 192.168.14.253
      start 192.168.15.1 end 192.168.15.253
      start 192.168.16.1 end 192.168.16.253
      start 192.168.17.1 end 192.168.17.253
      start 192.168.18.1 end 192.168.18.253
      start 192.168.19.1 end 192.168.19.253
      start 192.168.20.1 end 192.168.20.253
      start 192.168.21.1 end 192.168.21.253
      start 192.168.22.1 end 192.168.22.253
      start 192.168.23.1 end 192.168.23.253
```

```

start 192.168.24.1 end 192.168.24.253
start 192.168.25.1 end 192.168.25.253
start 192.168.26.1 end 192.168.26.253
type generic, total addresses 4301, allocated 3707 (86%),misses 0 Queued
Packets:0

```

Table 36 describes the fields shown in the display.

Table 36 *show ip nat nvi statistics Field Descriptions*

Field	Description
Total active 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 timed out.
NAT enabled interfaces	List of interfaces marked as NAT enabled with the ip nat enable 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.
CEF Translated packets	Number of packets switched via Cisco Express Forwarding (CEF).
CEF Punted packets	Number of packets punted to the process switched level.
Expired translations	Cumulative count of translations that have expired since the router was booted.
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.
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.
Queued Packets	Number of packets in the queue.

Related Commands

Command	Description
show ip nat nvi translations	Displays active NAT virtual interface translations.

show ip nat nvi translations

To display active NAT virtual interface (NVI) translations, use the **show ip nat nvi translations** command in user EXEC or privileged EXEC mode.

```
show ip nat nvi translations [protocol [global | vrf vrf-name] | vrf vrf-name | global] [verbose]
```

Syntax Description

<i>protocol</i>	(Optional) Displays protocol entries. The protocol argument must be replaced with one of the following keywords: <ul style="list-style-type: none"> esp—Encapsulating Security Payload (ESP) protocol entries. icmp—Internet Control Message Protocol (ICMP) entries. pptp—Point-to-Point Tunneling Protocol (PPTP) entries. tcp—TCP protocol entries. udp—User Datagram Protocol (UDP) entries.
global	(Optional) Displays entries in the global destination table.
vrf <i>vrf-name</i>	(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show ip nat nvi translations** command:

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

```
Pro      Source global      Source local      Destin local      Destin global
icmp    172.20.0.254:25    172.20.0.130:25    172.20.1.1:25     10.199.199.100:25
icmp    172.20.0.254:26    172.20.0.130:26    172.20.1.1:26     10.199.199.100:26
icmp    172.20.0.254:27    172.20.0.130:27    172.20.1.1:27     10.199.199.100:27
icmp    172.20.0.254:28    172.20.0.130:28    172.20.1.1:28     10.199.199.100:28
```

[Table 37](#) describes the fields shown in the display.

Table 37 show ip nat nvi translations Field Descriptions

Field	Description
Pro	Protocol of the port identifying the address.
Source global	Source global address.
Source local	Source local address.

Table 37 *show ip nat nvi translations Field Descriptions (continued)*

Field	Description
Destin local	Destination local address.
Destin global	Destination global address.

Related Commands

Command	Description
show ip nat nvi statistics	Displays NAT virtual interface statistics.

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.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 172.16.233.208 end 172.16.233.221
   type generic, total addresses 14, allocated 2 (14%), misses 0
```

[Table 38](#) describes the significant fields shown in the display.

Table 38 *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 ip nat outside command.
Inside interfaces	List of interfaces marked as inside with the ip nat inside command.
Hits	Number of times the software does a translations table lookup and finds an entry.

Table 38 *show ip nat statistics Field Descriptions (continued)*

Field	Description
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.
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
clear ip nat translation	Clears dynamic NAT translations from the translation table.
ip nat	Designates that traffic originating from or destined for the interface is subject to NAT.
ip nat inside destination	Enables NAT of the inside destination address.
ip nat inside source	Enables NAT of the inside source address.
ip nat outside source	Enables NAT of the outside source address.
ip nat pool	Defines a pool of IP addresses for NAT.
ip nat service	Changes the amount of time after which NAT translations time out.
show ip nat translations	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 [inside global-ip] [outside local-ip] [esp] [icmp] [pptp] [tcp] [udp]
[verbose] [vrf vrf-name]
```

Syntax Description		
esp	(Optional)	Displays Encapsulating Security Payload (ESP) entries.
icmp	(Optional)	Displays Internet Control Message Protocol (ICMP) entries.
inside <i>global-ip</i>	(Optional)	Displays entries for only a specific inside global IP address.
outside <i>local-ip</i>	(Optional)	Displays entries for only a specific outside local IP address.
pptp	(Optional)	Displays Point-to-Point Tunneling Protocol (PPTP) entries.
tcp	(Optional)	Displays TCP protocol entries.
udp	(Optional)	Displays User Datagram Protocol (UDP) entries.
verbose	(Optional)	Displays additional information for each translation table entry, including how long ago the entry was created and used.
vrf <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 vrf <i>vrf-name</i> keyword and argument combination was added.
	12.2(15)T	The esp keyword was added.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	XE 2.4.2	The inside and outside keywords were 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	172.16.2.132:53	172.16.2.132:53
tcp	10.69.233.209:11012	192.168.1.89:11012	172.16.1.220:23	172.16.1.220:23
tcp	10.69.233.209:1067	192.168.1.95:1067	172.16.1.161:23	172.16.1.161:23

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	172.16.233.209:1220	192.168.1.95:1220	172.16.2.132:53	172.16.2.132:53
				create 00:00:02, use 00:00:00, flags: extended
tcp	172.16.233.209:11012	192.168.1.89:11012	172.16.1.220:23	172.16.1.220:23
				create 00:01:13, use 00:00:50, flags: extended
tcp	172.16.233.209:1067	192.168.1.95:1067	172.16.1.161:23	172.16.1.161:23
				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
---	10.2.2.1	192.168.121.113	---	---
---	10.2.2.2	192.168.122.49	---	---
---	10.2.2.11	192.168.11.1	---	---
---	10.2.2.12	192.168.11.3	---	---
---	10.2.2.13	172.16.5.20	---	---
Pro	Inside global	Inside local	Outside local	Outside global
---	10.2.2.3	192.168.121.113	---	---
---	10.2.2.4	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

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

Router# **show ip nat translations inside 10.69.233.209**

Pro	Inside global	Inside local	Outside local	Outside global
udp	10.69.233.209:1220	192.168.1.95:1220	172.16.2.132:53	172.16.2.132:53

Table 39 describes the significant fields shown in the display.

Table 39 *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.
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"> • extended—Extended translation • static—Static translation • destination—Rotary translation • outside—Outside translation • timing out—Translation will no longer be used, due to a TCP finish (FIN) or reset (RST) flag.

Related Commands

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

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

Command Modes EXEC

Command History	Release	Modification
	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
```