



NAT Commands

application redundancy

To enter redundancy application configuration mode, use the **application redundancy** command in redundancy configuration mode.

application redundancy

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Redundancy configuration (config-red)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced.

Examples The following example shows how to enter redundancy application configuration mode:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)#
```

Related Commands	Command	Description
	group	Enters redundancy application group configuration mode.

authentication

To configure clear text authentication and MD5 authentication under a redundancy group protocol, use the **authentication** command in redundancy application protocol configuration mode. To disable the authentication settings in the redundancy group, use the **no** form of this command.

```
authentication {text string | md5 key-string [0 | 7] key | md5 key-chain key-chain-name}
```

```
no authentication {text string | md5 key-string [0 | 7] key | md5 key-chain key-chain-name}
```

Syntax Description

text <i>string</i>	Uses clear text authentication.
md5 key-string	Uses MD5 key authentication. The <i>key</i> argument can be up to 64 characters in length (at least 16 characters is recommended). Specifying 7 means the key will be encrypted.
0	(Optional) Specifies that the text following immediately is not encrypted.
7	(Optional) Specifies that the text is encrypted using a Cisco-defined encryption algorithm.
md5 key-chain <i>key-chain-name</i>	Uses MD5 key-chain authentication.

Command Default

The key is not encrypted.

Command Modes

Redundancy application group protocol configuration (config-red-app-protcl)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure clear text authentication for a redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-protcl)# authentication text name1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

Command	Description
protocol	Defines a protocol instance in a redundancy group.
timers hellotime	Configures timers for hellotime and holdtime messages for a redundancy group.

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) XND	The forced keyword was extended to support the removal of a half entry regardless of whether it has any child translations.
	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.
Cisco IOS XE Release 2.4.2	The forced keyword was extended for Cisco IOS XE Release 2.4.2 to support the removal of a half entry regardless of whether it has any child translations.
15.0(1)M2	The forced keyword was extended for Cisco IOS release 15.0(1)M2 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
```

clear nat64 ha statistics

To clear the Network Address Translation 64 (NAT64) high availability (HA) statistics, use the **clear nat64 ha statistics** command in privileged EXEC mode.

clear nat64 ha statistics

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines The HA statistics include the number of HA messages that are transmitted and received by the Route Processor (RP).

Examples The following example shows how to use the **clear nat64 ha statistics** command to clear the NAT64 HA statistics:

```
Router# clear nat64 ha statistics
```

Related Commands	Command	Description
	show nat64 ha status	Displays information about the NAT64 HA state.

clear nat64 statistics

To clear the Network Address Translation 64 (NAT64) statistics, use the **clear nat64 statistics** command in privileged EXEC mode.

clear nat64 statistics [**global** | **interface** *type number* | **prefix** *ipv6-prefix/prefix-length*]

Syntax Description		
global	(Optional)	Clears global NAT64 statistics.
interface	(Optional)	Clears interface statistics.
<i>type</i>	(Optional)	Interface type. For more information, use the question mark (?) online help function.
<i>number</i>	(Optional)	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
prefix	(Optional)	Clears statistics for a specified prefix.
<i>ipv6-prefix</i>	(Optional)	IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<i>/prefix-length</i>	(Optional)	Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines You can use the **clear nat64 statistics** command to clear the statistics of a specified interface or all the interfaces for a given stateless prefix.

Examples The following example shows how to clear NAT64 statistics:

```
Router# clear nat64 statistics
```

Related Commands	Command	Description
	show nat64 statistics	Displays statistics about NAT64 interfaces and the translated and dropped packet count.

control

To configure the control interface type and number for a redundancy group, use the **control** command in redundancy application group configuration mode. To remove control interface for the redundancy group, use the **no** form of this command.

```
control interface-name number protocol id
```

```
no control
```

Syntax Description

<i>interface-name</i>	Interface name.
<i>number</i>	Interface number.
protocol	Specifies redundancy group protocol media.
<i>id</i>	Redundancy group protocol instance. The range is from 1 to 8.

Command Default

Control interface is not configured

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure the redundancy group protocol media and instance for control Gigabit Ethernet interface:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# control GigabitEthernet 0/0/0 protocol 1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

data

To configure the data interface type and number for a redundancy group, use the **data** command in redundancy application group configuration mode. To remove the configuration, use the **no** form of this command.

data *interface-name* *number*

no data *interface-name* *number*

Syntax Description

<i>interface-name</i>	Interface name.
<i>number</i>	Interface number.

Command Default

No data interface is configured.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Use the **data** command to configure the data interface. Data interface can be the same physical interface as the control interface.

Examples

The following example shows how to configure the data Gigabit Ethernet interface for group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# data GigabitEthernet 0/0/0
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.

Command	Description
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

debug redundancy application group config

To display the redundancy application group configuration, use the **debug redundancy application group config** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug redundancy application group config {all | error | event | func}
```

```
no debug redundancy application group config {all | error | event | func}
```

Syntax Description

all	Displays debug information about configuration.
error	Displays information about the redundancy group's configuration errors.
event	Displays information about the redundancy group's configuration .
func	Displays information about the redundancy group's configuration functions entered.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following is sample output from the **debug redundancy application group config all** command:

```
Router# debug redundancy application group config all
```

```
RG config all debugging is on
```

Related Commands

Command	Description
debug redundancy application group media	Displays the redundancy application group media information.
debug redundancy application group protocol	Displays the redundancy application group protocol information.
debug redundancy application group RII	Displays the redundancy application group RII information.
debug redundancy application group transport	Displays the redundancy application group transport information.
debug redundancy application group VP	Displays the redundancy application group VP information.

debug redundancy application group faults

To display the redundancy application group faults, use the **debug redundancy application group faults** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug redundancy application group faults {all | error | event | fault | func}
```

```
no debug redundancy application group faults {all | error | event | fault | func}
```

Syntax Description

all	Displays fault information of a redundancy group.
error	Displays error information of a redundancy groups.
event	Displaysevent information of a redundancy group.
fault	Displays fault events information of a redundancy group.
func	Displays fault functions information of a redundancy group.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following is sample output from the **debug redundancy application group faults error** command:

```
Router# debug redundancy application group faults error
```

```
RG Faults error debugging is on
```

Related Commands

Command	Description
redundancy application group config	display the redundancy application group configuration.
debug redundancy application group media	Displays the redundancy application group media information.
debug redundancy application group protocol	Displays the redundancy application group protocol information.
debug redundancy application group rii	Displays the redundancy application group RII information.

Command	Description
debug redundancy application group transport	Displays the redundancy group application group transport information.
debug redundancy application group vp	Displays the redundancy group application group VP information.

debug redundancy application group media

To display the redundancy application group media information, use the **debug redundancy application group media** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug redundancy application group media {all | error | event | nbr | packet {rx | tx} | timer}
```

```
no debug redundancy application group media {all | error | event | nbr | packet {rx | tx} | timer}
```

Syntax Description

all	Displays media information of a redundancy group.
error	Displays media errors information of a redundancy group.
event	Displays media events information of a redundancy group.
nbr	Displays media neighbor (nbr) information of a redundancy group.
packet	Displays media packets information of a redundancy group.
rx	Displays the incoming packets information.
tx	Displays the outgoing packets information.
timer	Displays media timer events information about redundancy group media timer events.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following is sample output from the **debug redundancy application group media timer** command:

```
Router# debug redundancy application group media timer

RG Media timer debugging is on
```

Related Commands

Command	Description
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group protocol	Displays the redundancy group application group protocol information.
debug redundancy application group rii	Displays the redundancy group application group RII information.

Command	Description
debug redundancy application group transport	Displays the redundancy group application group transport information.
debug redundancy application group vp	Displays the redundancy application group VP information.
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group media	Displays the redundancy application group media information.
debug redundancy application group protocol	Displays the redundancy application group protocol information.

debug redundancy application group protocol

To display the redundancy application group protocol information, use the **debug redundancy application group protocol** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug redundancy application group protocol {all | detail | error | event | media | peer}
```

```
no debug redundancy application group protocol {all | detail | error | event | media | peer}
```

Syntax Description

all	Displays protocol information of a redundancy group.
detail	Displays event details of a redundancy group.
error	Displays protocol error information of a redundancy group.
event	Displays protocol events information of a redundancy group.
media	Displays protocol media events information of a redundancy group.
peer	Displays protocol peer information of a redundancy group.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following is sample output from the **debug redundancy application group protocol peer** command:

```
Router# debug redundancy application group protocol peer

RG Protocol peer debugging is on
```

Related Commands

Command	Description
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group protocol	Displays the redundancy application group protocol information.
debug redundancy application group rii	Displays the redundancy application group RII information.
debug redundancy application group transport	Displays the redundancy application group transport information.

Command	Description
debug redundancy application group vp	Displays the redundancy application group VP information.
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group media	Displays the redundancy application group media information.
redundancy application group config	Displays the redundancy application configuration.
debug redundancy application group protocol	Displays the redundancy application group protocol information.

debug redundancy application group rii

To display the redundancy application group RII information, use the **debug redundancy application group rii** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug redundancy application group rii {error | event}
```

```
no debug redundancy application group rii {error | event }
```

Syntax Description

error	Displays RII errors information about the redundancy group's .
event	Dispalys information about the redundancy group's RII events.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following is sample output from the **debug redundancy application group rii event** command:

```
Router# debug redundancy application group rii event

RG RII events debugging is on
```

Related Commands

Command	Description
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group protocol	Displays the redundancy group application group protocol information.
debug redundancy application group rii	Displays the redundancy group application group RII information.
debug redundancy application group vp	Displays the redundancy group application group VP information.
redundancy application group config	Displays the redundancy group application configuration.

Command	Description
debug redundancy application group media	Displays the redundancy application group media information.
debug redundancy application group protocol	Displays the redundancy application group protocol information.

debug redundancy application group transport

To display the redundancy application group transport information, use the **debug redundancy application group transport** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug redundancy application group transport {db | error | event | packet | timer | trace}
```

```
no debug redundancy application group transport {db | error | event | packet | timer | trace}
```

Syntax Description

db	Displays transport information of a redundancy group.
error	Displays transport error information of a redundancy group.
event	Displays transport event information of a redundancy group.
packet	Displays transport packet information of a redundancy group.
timer	Displays transport timer information of a redundancy group.
trace	Displays transport trace information of a redundancy group.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following is sample output from the **debug redundancy application group transport trace** command:

```
Router# debug redundancy application group transport trace
```

```
RG Transport trace debugging is on
```

Related Commands

Command	Description
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group protocol	Displays the redundancy application group protocol information.
debug redundancy application group rii	Displays the redundancy application group RII information.
debug redundancy application group transport	Displays the redundancy application group transport information.

Command	Description
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group media	Displays the redundancy application group media information.
debug redundancy application group protocol	Displays the redundancy application group protocol information.

debug redundancy application group vp

To display the redundancy application group virtual platform (VP) information, use the **debug redundancy application group VP** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug redundancy application group vp {error | event}
```

```
no debug redundancy application group vp {error | event}
```

Syntax Description

error	Displays VP errors information of a redundancy group.
event	Displays VP event information of a redundancy group.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following is sample output from the **debug redundancy application group vp event** command:

```
Router# debug redundancy application group vp event

RG VP events debugging is on
```

Related Commands

Command	Description
redundancy application group config	Displays the redundancy group application configuration.
debug redundancy application group protocol	Displays the redundancy application group protocol information.
debug redundancy application group rii	Displays the redundancy application group RII information.
debug redundancy application group transport	Displays the redundancy application group transport information.
redundancy application group config	Displays the redundancy application configuration.
debug redundancy application group media	Displays the redundancy application group media information.

Command	Description
debug redundancy application group protocol	Displays the redundancy application group protocol information.
redundancy application group config	Displays the redundancy application configuration.

group

To enter redundancy application group configuration mode, use the **group** command in redundancy application configuration mode. To remove the group configuration, use the **no** form of this command.

group *id*

no group *id*

Syntax Description	<i>id</i>	Redundancy group group ID. Valid values are 1 and 2.
--------------------	-----------	--

Command Default	No group is configured.
-----------------	-------------------------

Command Modes	Redundancy application configuration (config-red-app)
---------------	---

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced.

Examples	The following example shows how to configure a redundancy group with group ID 1:
----------	--

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)#
```

Related Commands	Command	Description
	application redundancy	Enters redundancy application configuration mode.

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 the Network Address Translation (NAT) of a globally unique outside host address to multiple inside host addresses, use the **ip nat inside destination** command in global configuration mode. This command is primarily used to implement TCP load balancing by performing destination address rotary translation. 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

To implement TCP load balancing, you must configure NAT to use rotary pools as specified with the **ip nat pool** command and the **rotary** keyword.

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.

For more information about implementing TCP load balancing, see the [Cisco IOS IP Addressing Services Configuration Guide](#).

Examples

The following example shows how to define a virtual address with connections that are distributed among a set of real hosts. The rotary pool defines the addresses of the real hosts. The access list defines the virtual address. If a translation does not already exist, TCP packets from serial interface 0 (the outside interface) whose destination matches the access list are translated to an address from the rotary pool.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0/0/0
 ip address 192.168.15.129 255.255.255.240
 ip nat outside
!
interface GigabitEthernet 0/0/1
 ip address 192.168.15.17 255.255.255.240
 ip nat inside
!
access-list 2 permit 192.168.15.1
```

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 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} [no-payload] [overload] [reversible] [vrf name [match-in-vrf]]
[oer] [portmap name]
```

```
no ip nat inside source {list {access-list-number | access-list-name} | route-map name} {interface
type number | pool name} [no-payload] [overload] [reversible] [vrf name [match-in-vrf]]
[oer] [portmap name]
```

Static NAT

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

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

Port Static NAT

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

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

Network Static NAT

```
ip nat inside source static network local-network global-network mask [extendable] [forced]
[mapping-id map-id] [no-alias] [no-payload] [redundancy group-name] [vrf name
[match-in-vrf]]
```

```
no ip nat inside source static network local-network global-network mask [extendable] [forced]
[mapping-id map-id] [no-alias] [no-payload] [redundancy group-name] [vrf name
[match-in-vrf]]
```

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	Specifies an interface for the global address.
<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>number</i>	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
pool <i>name</i>	Specifies the name of the pool from which global IP addresses are allocated dynamically.
no-payload	(Optional) Prohibits the translation of an embedded address or port in the payload.
overload	(Optional) Enables the router to use one global address for many local addresses. When overloading is configured, the TCP or 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.
portmap <i>name</i>	(Optional) Specifies the portmap to be associated for NAT.
static	Sets up a single static translation.
esp <i>local-ip</i>	Establishes the IPsec Encapsulating Security Payload (ESP) (tunnel mode) support.
<i>local-ip</i>	Local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or obsolete.
<i>global-ip</i>	Globally unique IP address of an inside host as it appears to the outside network.
extendable	(Optional) Extends the translation.
forced	(Optional) Forcefully deletes an entry and its children from the configuration.
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.
no-alias	(Optional) Prohibits an alias from being created for the global address.
redundancy <i>group-name</i>	(Optional) Establishes NAT redundancy.
tcp	Establishes the TCP protocol.
udp	Establishes the UDP protocol.
<i>local-port</i>	Local TCP or UDP port in a range from 1 to 65535.
<i>global-port</i>	Global TCP or UDP port in a range from 1 to 65535.
network <i>local-network</i>	Specifies the local subnet translation.
<i>global-network</i>	Global subnet translation.
<i>mask</i>	IP network mask to be used with subnet translations.

Command Default 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	This command was modified. The interface keyword was added for static translations. The vrf <i>name</i> keyword and argument combination was added.
	12.3(7)T	This command was modified. The static mapping-id <i>map-id</i> keyword and argument combination was added.
	12.4(3)T	This command was modified. 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	This command was modified. 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.
	12.2(33)SRE	This command was modified. The vrf <i>name</i> keyword and argument pair was removed from Cisco 7600 series routers.
	Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines The optional keywords of the **ip nat inside source** command can be entered in any order.

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

This command has two forms: the dynamic and the static address translation. The form with an access list establishes the 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 192.0.2.0 or the 198.51.100.0 network to the globally unique 203.0.113.209/28 network:

```
ip nat pool net-209 203.0.113.209 203.0.113.222 prefix-length 28
ip nat inside source list 1 pool net-209
!
interface ethernet 0
 ip address 203.0.113.113 255.255.255.240
 ip nat outside
!
interface ethernet 1
 ip address 192.0.2.1 255.255.255.0
 ip nat inside
!
access-list 1 permit 192.0.2.1 255.255.255.0
access-list 1 permit 198.51.100.253 255.255.255.0
```

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

```
ip nat inside source list 1 interface ethernet 0 vrf vrf1 overload
ip nat inside source list 1 interface ethernet 0 vrf vrf2 overload
!
ip route vrf vrf1 10.0.0.1 10.0.0.1 192.0.2.1
ip route vrf vrf2 10.0.0.1 10.0.0.1 192.0.2.1
!
access-list 1 permit 10.1.1.1 0.0.0.255
!
ip nat inside source list 1 interface ethernet 1 vrf vrf1 overload
ip nat inside source list 1 interface ethernet 1 vrf vrf2 overload
!
ip route vrf vrf1 10.0.0.1 10.0.0.1 198.51.100.1 global
ip route vrf vrf2 10.0.0.1 10.0.0.1 198.51.100.1 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
!
route-map 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 the 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 forwarding1
 ip address 192.0.2.11 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet0/0
 ip vrf forwarding forwarding2
 ip address 192.0.2.22 255.255.255.0
 ip nat outside
 ip virtual-reassembly

ip nat pool MYPPOOL 192.0.2.5 192.0.2.5 prefix-length 24
ip nat inside source list acl-nat pool MYPPOOL vrf vrf1 overload
!
!
ip access-list extended acl-nat
 permit ip 192.0.2.0 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 translations flow-export

To enable high speed logging for all or some a Network Address Translation (NAT) translations, use the **ip nat log translations flow-export** 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 flow-export v9 { udp destination addr port source interface
interface-number | { vrf-name | global-on } }
```

```
no ip nat log translations flow-export v9 { udp destination addr port source interface
interface-number | { vrf-name | global-on } }
```

Syntax Description

destination <i>addr</i> <i>port</i>	Specifies the destination address for which translations will be logged.
source <i>interface</i> <i>interface-number</i>	Specifies the source interface for which translations will be logged.
<i>vrf-name</i>	Specifies the Virtual Private Network (VPN) for which translations will be logged. The VPN is identified by the VPN Routing and Forwarding (VRF) network name.
global-on	Enables high speed logging for all Virtual Private Networks (VPNs).

Command Default

Logging is disabled for all translations

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release XE 3.1S	This command was introduced.

Usage Guidelines

You must first use the **ip nat log translations flow-export v9 udp destination** command to enable high speed logging for all VPN and non-VPN translations. VPN translations are also known as VPN Routing and Forwarding (VRF) translations.

After you enable high speed logging for all NAT translations, you can then use the **ip nat log translations flow-export v9 vrf-name** command to enable or disable translations for specific VPNs. When you use this command, high speed logging is disabled for all VPNs except for the ones where it is explicitly enabled.

Examples

The following example shows how to enable logging for a specific VPN.

```
Router(config)# ip nat log translations flow-export v9 udp destination 10.10.0.1 1020
source Ethernet 0/0
Router(config)# ip nat log translations flow-export v9 VPN-18
```

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 log translations syslog

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]
```

Dynamic NAT for inter-chassis redundancy

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

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

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]
```

Static NAT for inter-chassis redundancy

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

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

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]
```

Port Static NAT for inter-chassis redundancy

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

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

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**]

Network Static NAT for inter-chassis redundancy

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

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

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 name	(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.
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.
Cisco IOS XE Release 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 10.4.4.254 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 Network Address Translation (NAT) optimized Session Initiation Protocol (SIP) media path, use the **ip nat piggyback-support** command in global configuration mode.

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

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

Syntax Description

sip	SIP protocol algorithm.
all-messages	Establishes piggybacking in all messages except Session Description Protocol (SDP).
sdp-only	Establishes piggybacking in SDP only.
router <i>router-id</i>	Piggyback router ID number.
authentication <i>authentication-key</i>	(Optional) Specifies the MD5 authentication key.

Command Modes

Global configuration (config)

Command History

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

Examples

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

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

Related Commands

Command	Description
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 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 } | alg { tcp | udp } dns | allow-multipart | mgcp |
enable-mib | nbar | port-randomization | ras | rtsp | sip { tcp | udp } port port-number |
skinny tcp port port-number }
```

```
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 } | alg { tcp | udp } dns | allow-multipart | mgcp |
enable-mib | nbar | port-randomization | ras | rtsp | sip { tcp | udp } port port-number |
skinny tcp port port-number }
```

Syntax Description

H225	Specifies the H.323 to H.225 protocol.
allow-h323-even-rtp-ports	Specifies the even-numbered Real-time Transport Protocol (RTP) ports for the H.323 protocol.
allow-h323-keepalive	Specifies the H.323 keepalive.
allow-sip-even-rtp-ports	Specifies the even-numbered RTP ports for the Session Initiation Protocol (SIP).
allow-skinny-even-rtp-ports	Specifies the even-numbered RTP ports for the skinny protocol.
fullrange	Specifies all the available ports. The range is from 1 to 65535.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.
port <i>port-number</i>	Specifies the port other than the default port in the range from 1 to 65533.
list <i>access-list-number</i>	Specifies the standard access list number in the range from 1 to 199.
<i>access-list-name</i>	Name of a standard IP access list.
ESP	Specifies the Security Parameter Index (SPI) matching IPsec pass-through.
spi-match	Specifies the SPI matching IPsec pass-through. The ESP endpoints must also have SPI matching enabled.
IKE	Preserves the Internet Key Exchange (IKE) port, as required by some IPsec servers.
preserve-port	Preserves the UDP port in IKE packets.
ftp	Specifies FTP.
alg { tcp udp } dns	Enables Domain Name System (DNS) processing with an Application-Level Gateway (ALG) for either TCP or UDP.
allow-multipart	Enables SIP multipart processing.
mgcp	Specifies the Media Gateway Control Protocol (MGCP).
enable-mib	Enables NAT MIB support.

nbar	Enables network-based application recognition (NBAR).
port-randomization	Specifies that ports are allocated randomly for Network Address Translation (NAT), instead of sequentially.
ras	Specifies the H.323-Registration, Admission, and Status (RAS) protocol.
rtsp	Specifies the Real Time Streaming Protocol (RTSP). This protocol is enabled by default on port 554 and requires NBAR.
sip	Specifies SIP. This protocol is enabled by default on port 5060.
skinny	Specifies the skinny protocol.

Command Default

DNS ALG processing is enabled for TCP and UDP.
H.323 even-numbered RTP port allocation is enabled.
Port randomization is disabled.
RTSP is enabled and requires NBAR.
Skinny even-numbered RTP port allocation is enabled.
UDP SIP even-numbered RTP port allocation is enabled.
UDP SIP is enabled on port 5060.
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	This command was modified. The skinny keyword was added.
12.2(8)T	This command was modified. The sip keyword was added.
12.2(15)T	This command was modified. The ESP and spi-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	This command was modified. The rtsp and mgcp keywords were added.
12.3(11)T	This command was modified. 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	This command was modified. The nbar keyword was added.
12.4(24)T	This command was modified. The port-randomization keyword was added.
15.0(1)M	This command was modified. The alg , dns , and allow-multipart keywords were added.
15.0(1)M2	This command was modified. The enable-mib keyword was added.
15.1(1)T2	This command was modified. The tcp keyword used along with the sip keyword was removed.

Release	Modification
15.0(1)M3	This command was modified. The enable-mib keyword was removed.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

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 Cisco 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 H.323.

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.

By default SIP is enabled on port 5060; therefore NAT-enabled devices interpret all packets on this port as SIP call messages. If other applications in the system use port 5060 to send packets, the NAT service may corrupt the packet as it attempts to interpret the packet as a SIP call message.

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 Cisco IOS 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 features, including port map, full-range, and Secure Network Address Translation (SNAT).
- It is supported only for the port in the Layer 4 header of the packet.

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

NAT MIB support is turned off by default to avoid breakpoint exception crashes. To enable NAT MIB support, use the **enable-mib** keyword.

Examples

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

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

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

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

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

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

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

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

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

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

Related Commands

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

ip nat service dns-reset-ttl

To reset the time-to-live (TTL) value for Domain Name System (DNS) resource records (RRs) going through Network Address Translation (NAT) to zero (0), use the **ip nat service dns-reset-ttl** command in global configuration mode. To prevent the TTL value for a DNS RR from being set to 0, use the **no** form of this command.

ip nat service dns-reset-ttl

no ip nat service dns-reset-ttl

Syntax Description This command has no arguments or keywords.

Command Default The TTL value is set to 0 for DNS RRs going through NAT.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.4(20)T	This command was introduced.

Usage Guidelines RFC 2694, *DNS extensions to Network Address Translators (DNS_ALG)*, states that the TTL value supplied in the original RRs for static address assignments is left unchanged. For dynamic address assignments, DNS_ALG will modify the TTL to be 0, so the RRs are used just for the transaction in progress, and not cached. RFC 2181, *Clarifications to the DNS Specification*, requires all RRs in an RRset (RRs with the same name, class, and type, but with different RDATA) to have the same TTL. So if the TTL of an RR is set to 0, all other RRs within the same RRset will also be adjusted by the DNS_ALG to be 0.

The **ip nat service dns-reset-ttl** command allows you to modify this behavior. The TTL values on all DNS RRs passing through NAT are set to 0 by default. This means that DNS servers or clients do not cache temporarily assigned RRs. Use the **no ip nat service dns-reset-ttl** command to disable the TTL value from being set to 0, and use the **ip nat service dns-reset-ttl** command to allow the TTL value to be reset to 0 again.

You may want to have a TTL value of 0 to prevent nonauthoritative servers from caching DNS RRs, perhaps in advance of changing a server's IP address. Allowing a nonzero value for DNS RRs enables remote name servers to cache the DNS RR information for a longer period of time, reducing the number of queries for the RR, while having the effect of lengthening the amount of time required to proliferate RR changes simultaneously.

Examples The following example shows how to prevent DNS RRs that pass through NAT from having their TTL values set to 0:

```
Router(config)# no ip nat service dns-reset-ttl
```

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 dns primary	Configures router authority parameters for the DNS name server.
ip dns server	Enables the DNS server on the router.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
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 dns primary	Displays the authoritative name server configuration for the router.
show ip nat statistics	Displays NAT statistics.
show ip nat translation	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 disable		(Optional) Disables the use of queuing with asymmetric routing in HSRP mode.
as-queuing enable		(Optional) Enables the use of queuing with asymmetric routing 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.
	15.0(1)M2	The as-queuing keyword was removed.

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 { arp-ping-timeout | dns-timeout | finrst-timeout | icmp-timeout |
port-timeout { tcp port-number | udp port-number } | pptp-timeout | routemap-entry-timeout
| syn-timeout | tcp-timeout | timeout | udp-timeout } { seconds | never }
```

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

Syntax Description

arp-ping-timeout	Specifies that the timeout value applies to the Address Resolution Protocol (ARP) ping.
dns-timeout	Specifies that the timeout value applies to connections to the Domain Name System (DNS). The default is 60 seconds.
finrst-timeout	Specifies that the timeout value applies to Finish and Reset TCP packets, which terminate a connection. The default is 60 seconds.
icmp-timeout	Specifies the timeout value for Internet Control Message Protocol (ICMP) flows. The default is 60 seconds.
port-timeout	Specifies that the timeout value applies to the TCP/UDP port.
tcp	Specifies Transport Control Protocol (TCP).
udp	Specifies User Datagram Protocol (UDP).
<i>port-number</i>	Port number. The range is from 1 to 65535.
pptp-timeout	Specifies the timeout value for NAT Point-to-Point Tunneling Protocol (PPTP) flows. The default is 86,400 seconds (24 hours).
routemap-entry-timeout	Specifies that the timeout applies for routemap created half entry.
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.
tcp-timeout	Specifies that the timeout value applies to the TCP port. Default is 86,400 seconds (24 hours).
timeout	Specifies that the timeout value applies to dynamic translations except for overload translations. The default is 86,400 seconds (24 hours).
udp-timeout	Specifies that the timeout value applies to the User Datagram Protocol (UDP) port. The default is 300 seconds (5 minutes).
<i>seconds</i>	Number of seconds after which the specified port translation times out.
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)

Command Modes Global configuration (config)

Command History	Release	Modification
	11.2	This command was introduced.
	12.4(6)T	This command was modified. 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.
	15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The routemap-entry-timeout , tcp , udp , and <i>port-number</i> keywords and arguments were added.

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

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

```
Router# configure terminal
Router(config)# 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 [all-host | all-vrf | host ip-address | list {listname | listnumber} | vrf name] number
```

```
no ip nat translation max-entries [all-host | all-vrf | host ip-address | list {listname | listnumber} | vrf name] number
```

Syntax Description

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

Command Default

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The vrf name keyword and argument pair was removed from Cisco 7600 series routers.

Usage Guidelines

Before you configure a NAT rate limit, you must first classify the current NAT usage and determine the sources of requests for NAT translations. If a specific host, an access control list, or a VRF instance is generating an unexpectedly high number of NAT requests, it may be the source of a 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 the **ip nat translation max-entries** command, you must specify the type of NAT rate limit you want to remove and its current value. For more information about how to display the current NAT rate limit settings, see the **show ip nat statistics** command.

Examples

The following examples show how to configure the 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.

Command	Description
ip nat translation (timeout)	Changes the NAT timeout value.
show ip nat statistics	Displays NAT statistics.
show ip nat translations	Displays active NAT translations.

name

To configure the redundancy group with a name, use the **name** command in redundancy application group configuration mode. To remove the name of a redundancy group, use the **no** form of this command.

name *group-name*

no name *group-name*

Syntax Description

<i>group-name</i>	Name of the redundancy group.
-------------------	-------------------------------

Command Default

The redundancy group is not configured with a name.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure the redundancy group name as group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# name group1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group	Enters redundancy application group configuration mode.
shutdown	Shuts down a group manually.

nat64 enable

To enable stateless Network Address Translation 64 (NAT64) on an interface, use the **nat64 enable** command in interface configuration mode. To disable the NAT64 configuration on an interface, use the **no** form of this command.

nat64 enable

no nat64 enable

Syntax Description This command has no arguments or keywords.

Command Default NAT64 is not enabled on an interface.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Examples

The following example shows how to enable stateless NAT64 on a Gigabit Ethernet interface:

```
Router# configure terminal
Router(config)# interface gigabitethernet0/0/0
Router(config-if)# nat64 enable
Router(config-if)# end
```

Related Commands

Command	Description
show nat64 adjacency	Displays information about the NAT64-managed adjacencies.
show nat64 ha status	Displays information about the NAT64 HA status.
show nat64 statistics	Displays statistics about a NAT64 interface and the transmitted and dropped packet count.

nat64 prefix

To assign a global or interface-specific Network Address Translation 64 (NAT64) stateless prefix, use the **nat64 prefix** command in global configuration or interface configuration mode. To disable the configuration, use the **no** form of this command.

```
nat64 prefix stateless ipv6-prefix/prefix-length
```

```
no nat64 prefix stateless
```

Syntax Description

stateless	Specifies the stateless prefix.
<i>ipv6-prefix</i>	IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<i>/prefix-length</i>	Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default

No NAT64 translation is performed.

Command Modes

Global configuration (config)
Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **nat64 prefix stateless** command uses a prefix and prefix length for IPv4-translatable IPv6 addresses. Use the **nat64 prefix stateless** command in global configuration mode to assign a global NAT64 stateless prefix or in interface configuration mode to assign an unique NAT64 stateless prefix for each interface. In interface configuration mode, a stateless prefix should be configured on an IPv6-facing interface.

All packets coming to an IPv6 interface are matched against the configured prefix, and the matched packets are translated to IPv4. Similarly, the packets that the IPv6 interface sends use the stateless prefix to construct the source and destination IPv6 address.



Note

A maximum of one global stateless prefix and one stateless prefix per interface is supported.

If NAT64 is enabled on an interface that does not have a stateless prefix configured, then the global stateless prefix is used. However, if a global prefix and an interface prefix are configured, then the interface prefix is used for stateless NAT64 translation. The use of a stateless prefix on an interface has priority over the configured global stateless prefix.

Examples

The following example shows how to configure a global NAT64 stateless prefix:

```
Router# configure terminal  
Router(config)# nat64 prefix stateless 2001::7001:10A/96  
Router(config)# end
```

The following example shows how to assign a NAT64 stateless prefix for a Gigabit Ethernet interface:

```
Router# configure terminal  
Router(config)# interface gigabitethernet0/0/0  
Router(config-if)# nat64 prefix stateless 2001:0DB8:0:1::/96  
Router(config-if)# end
```

Related Commands

Command	Description
nat64 route	Specifies the NAT64 stateless prefix to which an IPv4 prefix should be translated.
show nat64 prefix stateless	Displays information about the configured NAT64 stateless prefixes.

nat64 route

To specify the Network Address Translation 64 (NAT64) stateless prefix to which an IPv4 prefix should be translated, use the **nat64 route** command in global configuration mode. To disable the configuration, use the **no** form of this command.

```
nat64 route ipv4-prefix/mask interface-type interface-number
```

```
no nat64 route ipv4-prefix/mask
```

Syntax Description		
	<i>ipv4-prefix/mask</i>	Length of the IPv4 prefix and the mask.
	<i>interface-type</i>	Interface type. For more information, use the question mark (?) online help function.
	<i>interface-number</i>	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default No NAT64 routing is performed.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines A prefix that is configured on an interface is used as the stateless prefix on that interface. If no interface-specific prefix is configured, the configured global prefix is used for NAT64 translation.

Examples The following example shows how to assign an IPv4 prefix and mask to an interface:

```
Router# configure terminal
Router(config)# nat64 route 192.168.0.0/24 gigabitethernet0/0/1
Router(config)# exit
```

Related Commands	Command	Description
	nat64 prefix stateless	Assigns a global or interface-specific NAT64 stateless prefix.
	show nat64 routes	Displays information about the configured NAT64 routes.

preempt

To enable preemption on the redundancy group, use the **preempt** command in redundancy application group configuration mode. To disable the group's preemption, use the **no** form of this command.

preempt

no preempt

Syntax Description This command has no arguments or keywords.

Command Default Preemption is disabled on the redundancy group.

Command Modes Redundancy application group configuration (config-red-app-grp)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines When the preemption is enabled, it means that a standby redundancy group should preempt an active redundancy group if its priority is higher than the active redundancy group.

Examples The following example shows how to enable preemption on the redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp) preempt
```

Related Commands	Command	Description
	application redundancy	Enters redundancy application configuration mode.
	group	Enters redundancy application group configuration mode.
	name	Configures the redundancy group with a name.
	protocol	Defines a protocol instance in a redundancy group.

priority

To specify a group priority and failover threshold value in a redundancy group, use the **priority** command in redundancy application group configuration mode. To disable the priority value of a group, use the **no** form of this command.

priority *value* [**failover-threshold** *value*]

no priority *value* [**failover-threshold** *value*]

Syntax Description

<i>value</i>	The priority value. The range is from 1 to 255.
failover-threshold <i>value</i>	(Optional) Specifies the failover threshold value. The range is from 1 to 255.

Command Default

The default priority value is 100.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The priority of the redundancy group is used to determine a redundancy group's active or standby role on the configured node. The failover threshold is used to determine when a switchover must occur. After the priority is set under threshold, the active redundancy group gives up its role.

Examples

The following example shows how to configure the priority value and threshold value for the redundancy group named group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp) priority 100 failover-threshold 90
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.

protocol

To define a protocol instance in a redundancy group, use the **protocol** command in redundancy application group configuration mode. To remove the protocol instance from the redundancy group, use the **no** form of this command.

protocol *id*

no protocol *id*

Syntax Description

id Redundancy group protocol ID. The range is from 1 to 8.

Command Default

Protocol instance is not defined in a redundancy group.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Protocol configuration is used to configure timers and authentication method for a control interface. Thus, a protocol instance is attached to the control interface.

Examples

The following example shows how to configure a protocol named protocol 1 to a redundancy group:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
timers hellotime	Configures timers for hellotime and holdtime messages for a redundancy group.

redundancy application reload group

To manually force a state switchover for the redundancy group, use the **redundancy application reload group** command in user EXEC or privileged EXEC mode. To remove virtual IP address from the redundancy group, use the **no** form of this command.

redundancy application reload group *id* [**peer** | **self**]

Syntax Description		
	<i>id</i>	Redundancy group ID.
	peer	Force the peer in the redundancy group to reload.
	self	Force this member of the redundancy group to reload.

Command Default Forces this member of the redundancy group to reload.

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

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines You can use this command to reload the peer only on the active member of the redundancy group to reload the standby member of the redundancy group.

Examples The following example shows how to reload the standby peer in a redundancy group:

```
Router# redundancy application reload group 2 peer
```

Related Commands	Command	Description
	show redundancy application group	Displays redundancy group information.

redundancy group

To configure the virtual IP address for the redundancy group, use the **redundancy group** command in interface configuration mode. To remove virtual IP address from the redundancy group, use the **no** form of this command.

redundancy group *id* **ip** *address* **exclusive** [**decrement** *value*]

no redundancy group *id* **ip** *address* **exclusive** [**decrement** *value*]

Syntax Description

<i>id</i>	Redundancy group ID.
ip <i>address</i>	Specifies the IP address of the interface.
exclusive	Specifies whether the interface is not shared with another redundancy group.
decrement <i>value</i>	(Optional) Amount decremented from the priority when the L1 state of the interface goes down. This overrides the default amount for the redundancy group. The range is from 1 to 255.

Command Default

Virtual IP address is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The virtual IP address and the physical address must in the same subnet.

Examples

The following example shows how to configure the redundancy group redundancy traffic interface:

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1/1
Router(config-if)# redundancy group 2 ip 1.2.3.4 exclusive
```

Related Commands

Command	Description
application	Enters redundancy application configuration mode.
redundancy	
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.

Command	Description
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.
redundancy rii	Configures the RII for the redundancy group.

redundancy rii

To configure the redundancy interface identifier (RII) for the redundancy group protected traffic interfaces, use the **redundancy rii** command in interface configuration mode. To remove the control interface from the redundancy group, use the **no** form of this command.

redundancy rii *id*

no redundancy rii *id*

Syntax Description

id Redundancy interface identifier. The range is from 1 to 65535.

Command Default

RII is not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Every interface associated with one or more Redundancy Groups must have a unique RII assigned to it. RII allows interfaces to have a one-to-one mapping between peers.

Examples

The following example shows how to configure the RII for the Gigabit Ethernet interface:

```
Router# configure terminal
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# redundancy rii 100
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

Command	Description
protocol	Defines a protocol instance in a redundancy group.
redundancy group	Configures the virtual IP address for a redundancy group.

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.
	Cisco IOS XE Release 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
192.168.22.20:28726CD9
esp 192.168.22.40:0    192.168.122.20:2E59EEF5 192.168.22.20:0 192.168.22.20:0
```

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

```
Router# show ip nat translation esp verbose
```

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

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
```

show nat64 adjacency

To display information about the stateless Network Address Translation 64 (NAT64) managed adjacencies, use the **show nat64 adjacency** command in user EXEC or privileged EXEC mode.

```
show nat64 adjacency {all | count | ipv4 | ipv6}
```

Syntax Description	all	Displays all adjacencies.
	count	Displays the adjacency count.
	ipv4	Displays IPv4 adjacencies.
	ipv6	Displays IPv6 adjacencies.

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

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines An adjacency is a node that can be reached by one Layer 2 hop. The stateless NAT64 adjacencies include adjacency addresses and the total number of adjacencies.

Examples The following is sample output from the **show nat64 adjacency all** command:

```
Router# show nat64 adjacency all

Adjacency Counts
  IPv4 Adjacencies: 2
  IPv6 Adjacencies: 1
  Stateless Prefix Adjacency Ref Count: 1

Adjacencies
  IPv6 Adjacencies
    ::42
  IPv4 Adjacencies
    0.0.19.137 (5001)
    0.0.19.140 (5004)
```

[Table 40](#) describes the significant fields shown in the display.

Table 40 *show nat64 adjacency all Field Descriptions*

Field	Description
Adjacency Counts	Count of all adjacencies.
Adjacencies	Types of adjacencies.

Related Commands

Command	Description
nat64 enable	Enables stateless NAT64 on an interface.

show nat64 ha status

To display information about the stateless Network Address Translation 64 (NAT64) high availability (HA) status, use the **show nat64 ha status** command in user EXEC or privileged EXEC mode.

show nat64 ha status

Syntax Description This command has no arguments or keywords.

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

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced.

Examples The following is sample output from the **show nat64 ha status** command:

```
Router# show nat64 ha status

NAT64 HA Status

Role: active
Peer is ready: TRUE
Peer is compatible: TRUE
Synchronization enabled: TRUE
Is hot (standby): FALSE
Bulk sync PID: NO_PROCESS
ISSU negotiation status: IPC, CF
ISSU context IDs: IPC(198), CF(197)
Synchronization capabilities: 0x00000001
Adjacency mappings: TRUE
CF info: handle(0x0000011B), peer ready(TRUE),
flow control(TRUE) (FALSE) (0x0)
Initialized: HA(TRUE) ISSU(TRUE)

Message stats:
Adjacency mapping: rx(0) tx(5001) tx err(0)
Bulk sync done: rx(0) tx(1) tx err(0)
Errors:
Bulk sync: 0
CF tx: 0
```

Table 41 describes the significant fields shown in the display.

Table 41 *show nat64 ha status Field Descriptions*

Field	Description
NAT64 HA Status	Status of stateless NAT64 HA.
Message stats	Status of the messages.
Errors	Types of errors.

Related Commands

Command	Description
clear nat64 ha statistics	Clears stateless NAT64 HA statistics.
nat64 enable	Enables stateless NAT64 on an interface.

show nat64 prefix stateless

To display information about the configured Network Address Translation 64 (NAT64) stateless prefixes, use the **show nat64 prefix stateless** command in user EXEC or privileged EXEC mode.

```
show nat64 prefix stateless {global | {interfaces | static-routes} [prefix
                             ipv6-prefix/prefix-length]}
```

Syntax Description

global	Displays the global stateless prefixes.
interfaces	Displays the interfaces and the stateless prefixes used by the interfaces.
prefix	(Optional) Displays the interfaces that are using a specific stateless prefix.
static-routes	Displays the static routes that are using the stateless prefix.
<i>ipv6-prefix</i>	(Optional) IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<i>/prefix-length</i>	(Optional) Length of the IPv6 prefix. Prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. Valid values are from 0 to 128.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The output of the **show nat64 prefix stateless** command displays the interfaces that use a specific prefix and the number of prefixes that use a static route.

Examples

The following is sample output from the **show nat64 prefix stateless global** command:

```
Router# show nat64 prefix stateless global

Global Prefix: is valid, 2001::/96

IFs Using Global Prefix

  Fa0/3/4
  Fa0/3/5
```

Table 42 describes the significant fields shown in the display.

Table 42 show nat64 prefix stateless global Field Descriptions

Field	Description
Global Prefix	IPv6 stateless prefix configured at the global level.
IFs Using Global Prefix	Lists the interfaces that are using the specified global prefix.

The following is sample output from the **show nat64 prefix stateless interfaces** command.

```
Router# show nat64 prefix stateless interfaces

Interface          NAT64 Enabled   Global   Stateless Prefix
FastEthernet0/3/4  TRUE            FALSE   2001::/96
```

Table 41 describes the significant fields shown in the display.

Table 43 show nat64 prefix stateless interfaces Field Descriptions

Field	Description
Interface	Interface name and number.
NAT64 Enabled	Information on whether NAT64 is enabled on a route. TRUE if enabled and FALSE if not enabled.
Global	Information on whether a global prefix is used. TRUE if the global prefix is used and FALSE if the interface prefix is used.
Stateless Prefix	Stateless prefix used for NAT64 translation.

The following is sample output from the **show nat64 prefix stateless static-routes** command. The output fields are self-explanatory.

```
Router# show nat64 prefix stateless static-routes

Stateless          Prefix Static Route Ref Count
2001::/96          1
```

Related Commands

Command	Description
nat64 prefix	Assigns a global or interface-specific NAT64 stateless prefix.

show nat64 routes

To display information about the configured Network Address Translation 64 (NAT64) routes, use the **show nat64 routes** command in privileged EXEC mode.

```
show nat64 routes [adjacency address | interface type number | prefix prefix-length]
```

Syntax Description		
adjacency	(Optional)	Displays the route for an adjacency address.
<i>address</i>	(Optional)	Adjacency address for lookup.
interface	(Optional)	Displays routes pointing to an interface.
<i>type</i>	(Optional)	Interface type. For more information, use the question mark (?) online help function.
<i>number</i>	(Optional)	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
prefix	(Optional)	Displays the route of an IPv4 prefix.
<i>prefix-length</i>	(Optional)	Length of the IPv4 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

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

Command History	Release	Modification
	Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines The output of the **show nat64 routes** command displays the stateless prefix and adjacency used by the routes and information on whether the routes are enabled.

Examples The following is sample output from the **show nat64 routes** command:

```
Router# show nat64 routes
```

IPv4 Prefix	Adj. Address	Enabled	Output IF	Global	IPv6 Prefix
192.0.2.1/24	0.0.19.137	FALSE	Fa0/3/4		
198.51.100.253/24	0.0.19.140	TRUE	Fa0/3/0	FALSE	3001::/96

Table 41 describes the significant fields shown in the display.

Table 44 *show nat64 routes Field Descriptions*

Field	Description
IPv4 Prefix	Prefix used by IPv4 address.
Adj. Address	Adjacency address.
Enabled	Information on whether NAT64 is enabled on a route. TRUE if enabled and FALSE if not enabled.
Output IF	Output interfaces.
Global	Information on whether a global prefix is used. TRUE if the global prefix is used and FALSE if the interface prefix is used.

Related Commands

Command	Description
nat64 route	Specifies the NAT64 stateless prefix to which an IPv4 prefix should be translated.

show nat64 statistics

To display Network Address Translation 64 (NAT64) packet count statistics, use the **show nat64 statistics** command in user EXEC or privileged EXEC mode.

```
show nat64 statistics [global | interface type number | prefix ipv6-prefix/prefix-length]
```

Syntax Description

global	(Optional) Displays global NAT64 statistics.
interface	(Optional) Displays statistics for an interface.
<i>type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>number</i>	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
prefix	(Optional) Displays statistics for a specified prefix.
<i>ipv6-prefix</i>	(Optional) IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<i>/prefix-length</i>	(Optional) Length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value. The valid values are from 0 to 128.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The output of the **show nat64 statistics** command displays the interfaces configured for stateless NAT64 and the packets that were translated or dropped.

Examples

The following is sample output from the **show nat64 statistics** command:

```
Router# show nat64 statistics

NAT64 Statistics

Global Stats:
  Packets translated (IPv4 -> IPv6): 21
  Packets translated (IPv6 -> IPv4): 15

GigabitEthernet0/0/1 (IPv4 configured, IPv6 configured):
  Packets translated (IPv4 -> IPv6): 5
```

```

Packets translated (IPv6 -> IPv4): 0
Packets dropped: 0
GigabitEthernet1/2/0 (IPv4 configured, IPv6 configured):
Packets translated (IPv4 -> IPv6): 0
Packets translated (IPv6 -> IPv4): 5
Packets dropped: 0

```

Table 45 describes the significant fields shown in the display.

Table 45 *show nat64 statistics Field Descriptions*

Field	Description
Global Stats	Statistics of all the NAT64 interfaces.
Packets translated	Number of packets translated from IPv4 to IPv6 and vice versa.
Packets dropped	Number of packets dropped. The packets that are not translated are dropped.

Related Commands

Command	Description
nat64 enable	Enables stateless NAT64 on an interface.

show platform hardware qfp feature

To display feature specific information in the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature** command in privileged EXEC mode.

```
show platform hardware qfp {active | standby} feature alg {memory | statistics [protocol
[clear]]
```

Syntax Description

active	Displays the active instance of the processor.
standby	Displays the standby instance of the processor.
alg	Displays the Application Level Gateway (ALG) information of the processor.
memory	Displays ALG memory usage information of the processor.
statistics	Displays ALG common statistics information of the processor.
<i>protocol</i>	One of the following protocols: <ul style="list-style-type: none"> • dns • exec • ftp • h323 • http • ldap • login • netbios • rtsp • shell • sip • skinny • smtp • tftp
clear	Clears the ALG counters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced.
Cisco IOS XE Release 3.1S	This command was modified. Support for the Network Basic Input Output System (NetBIOS) protocol and the following keywords were added: netbios-dgm , netbios-ns , and netbios-ssn .

Usage Guidelines

The **show platform hardware qfp feature** command when used with the **netbios** keyword displays the NetBIOS ALG memory usage and statistics information of the processor.

Examples

The following example displays the NetBIOS ALG statistics information of the processor:

```
Router# show platform hardware qfp active feature alg statistics netbios
```

```
NetBIOS ALG Statistics:
  No. of allocated chunk elements in L7 data pool:0
  No. of times L7 data is allocated:0 No. of times L7 data is freed:0
  Datagram Service statistics
    Total packets          :0
    Direct unique packets  :0
    Direct group packets   :0
    Broadcast packets      :0
    DGM Error packets      :0
    Query request packets  :0
    Positive Qry response packets :0
    Netgative Qry response packets:0
    Unknown packets        :0
    Total error packets     :0
  Name Service statistics
    Total packets          :0
    Query request packets  :0
    Query response packets :0
    Registration req packets :0
    Registration resp packets:0
    Release request packets :0
    Release response packets :0
    WACK packets           :0
    Refresh packets        :0
    Unknown packets        :0
    Total error packets     :0
  Session Service statistics
    Total packets          :0
    Message packets        :0
    Request packets        :0
    Positive response packets:0
    Negative response packets:0
    Retarget response packets:0
    Keepalive packets      :0
    Unknown packets        :0
    Total error packets     :0
```

Table 46 describes the significant fields shown in the display.

Table 46 *show platform hardware qfp feature Field Descriptions*

Field	Description
No. of allocated chunk elements in L7 data pool	Counter tracking number of memory chunks allocated for processing NetBIOS packets.
No. of times L7 data is allocated:0 No. of times L7 data is freed	Counters tracking number of times memory is allocated and freed for processing NetBIOS packets.
Direct unique packets	Counter tracking number of direct unique NetBIOS packets processed.
Direct group packets	Counter tracking number of direct group NetBIOS packets processed.

Table 46 *show platform hardware qfp feature Field Descriptions (continued)*

Field	Description
Broadcast packets	Counter tracking number of BROADCAST NetBIOS packets processed.
DGM Error packets	Counter tracking number of Datagram Error NetBIOS packets processed.
Query request packets	Counter tracking number of query request NetBIOS packets processed.
Positive Qry response packets	Counter tracking number of positive query response NetBIOS packets processed.
Negative Qry response packets	Counter tracking number of negative query response NetBIOS packets processed.
Unknown packets	Counter tracking number of unknown packets.
Total error packets	Counter tracking number of error packets.

Related Commands

Command	Description
debug platform hardware qfp feature	Debugs features in QFP.

show platform software trace message

To display trace messages for a module, enter the **show platform software trace message** command in privileged EXEC mode or diagnostic mode.

show platform software trace message *process hardware-module slot*

Syntax Description		
<i>process</i>	The process in which the tracing level is being set. The following keywords are available:	<ul style="list-style-type: none"> • chassis-manager—The Chassis Manager process. • cpp-control-process—The Cisco packet processor (CPP) Control process. • cpp-driver—The CPP driver process. • cpp-ha-server—The CPP high availability (HA) server process. • cpp-service-process—The CPP service process. • forwarding-manager—The Forwarding Manager process. • host-manager—The Host Manager process. • interface-manager—The Interface Manager process. • ios—The Cisco IOS process. • logger—The logging manager process. • pluggable-services—The pluggable services process. • shell-manager—The Shell Manager process.
<i>hardware-module</i>	The hardware module where the process whose trace level is being set is running. The following keywords are available:	<ul style="list-style-type: none"> • carrier-card—The process is on an SPA Interface Processor (SIP). • forwarding-processor—The process is on an embedded services processor (ESP). • route-processor—The process is on an route processor (RP).
<i>slot</i>	The slot of the hardware module. Options are as follows:	<ul style="list-style-type: none"> • number—The number of the SIP slot of the hardware module where the trace level is being set. For instance, if you want to specify the SIP in SIP slot 2 of the router, enter 2. • SIP-slot/SPA-bay—The number of the SIP router slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in router slot 3, enter 3/2. • cpp active—The CPP in the active ESP. • cpp standby—The CPP in the standby ESP. • f0—The ESP in ESP slot 0. • f1—The ESP in ESP slot 1 • fp active—The active ESP. • fp standby—The standby ESP.

- **r0**—The RP in RP slot 0.
- **r1**—The RP in RP slot 1.
- **rp active**—The active RP.
- **rp standby**—The standby RP.
- **qfp active**—The active Quantum Flow Processor (QFP)

Command Modes

Privileged EXEC (#)
Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
12.2(33)XND	This command was modified. The command output displays the truncated traceback message also.
Cisco IOS XE Release XE 3.1S	The qfp active keywords were added.

Usage Guidelines

The **show platform software trace message** command is used to display trace messages from an in-memory message ring of a module's process that keeps a condensed historical record of all messages. Although all messages are saved in a trace log file unmodified, only the first 128 bytes of a message are saved in the message ring. The size limitation does not apply to the traceback portion of a message.

Examples

The following example shows how to display the trace messages for the Host Manager process in RP slot 0 using the **show platform software trace message** command:

```
Router# show platform software trace message host-manager R0

08/23 12:09:14.408 [uipeer]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipeer]: (info): Start of request handling for con 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Received new connection 0x100a61c8 on descriptor 14
08/23 12:09:14.398 [uipeer]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipeer]: (info): Going to send a status update to the shell manager in
slot 0
08/23 11:53:47.417 [uipeer]: (info): Going to send a status update to the shell manager in
slot 0
```

The following example shows a truncated message that has a traceback. The truncated portion of the message is indicated by an ellipsis (...):

```
03/02 15:47:44.002 [errmsg]: (ERR): %EVENTLIB-3-TIMEHOG: read asyncon 0x100a9260: 60618ms,
Traceback=1#862f8780825f93a618ecd9 ...Traceback=1#862f8780825f93a618ecd9dd48b3be96
evlib:FCAF000+CC00 evlib:FCAF000+A6A8 evutil:FFCA000+ADD0 evutil:FFCA000+5A80
evutil:FFCA000+A68C uipeer:FF49000+10AFC evlib:FCAF000+D28C evlib:FCAF000+F4C4
:10000000+1B24C c:EF44000+1D078 c:EF44000+1D220
```

Related Commands

Command	Description
set platform software trace	Sets the trace level for a specific module.
show platform software trace levels	Displays trace levels for a module.

show redundancy application group

To display the redundancy group information, use the **show redundancy application group** command in privileged EXEC mode.

show redundancy application group [*group-id* | **all**]

Syntax Description

<i>group-id</i>	(Optional) redundancy group group is. Valid values are 1 and 2.
all	(Optional) Display the redundancy group information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

Use the **show redundancy application group** command to display the current state of each interbox redundancy group on the device and the peer device.

Examples

The following is sample output from the **show redundancy application group all** command:

```
Router# show redundancy application group all

Faults states Group 1 info:
  Runtime priority: [200]
  RG Faults RG State: Up.
  Total # of switchovers due to faults:      3
  Total # of down/up state changes due to faults: 2

Group ID:1
Group Name:grp2

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No

RF Domain: btob-one
  RF state: ACTIVE
  Peer RF state: DISABLED

RG Protocol RG 1
-----
  Role: Active
  Negotiation: Enabled
```

```

Priority: 200
Protocol state: Active
Ctrl Intf(s) state: Down
Active Peer: Local
Standby Peer: Not exist
Log counters:
    role change to active: 2
    role change to standby: 0
    disable events: rg down state 1, rg shut 0
    ctrl intf events: up 0, down 2, admin_down 1
    reload events: local request 3, peer request 0

```

RG Media Context for RG 1

```

-----
Ctx State: Active
Protocol ID: 1
Media type: Default
Control Interface: GigabitEthernet0/1/0
Hello timer: 5000
Effective Hello timer: 5000, Effective Hold timer: 15000
  LAPT values: 0, 0
Stats:
    Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
    Authentication not configured
    Authentication Failure: 0
    Reload Peer: TX 0, RX 0
    Resign: TX 1, RX 0
Standby Peer: Not Present.

```

Faults states Group 2 info:

```

Runtime priority: [150]
RG Faults RG State: Up.
    Total # of switchovers due to faults:      2
    Total # of down/up state changes due to faults: 2

```

Group ID:2
Group Name:name1

```

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No

```

```

RF Domain: btob-two
RF state: ACTIVE
Peer RF state: DISABLED

```

RG Protocol RG 2

```

-----
Role: Active
Negotiation: Enabled
Priority: 150
Protocol state: Active
Ctrl Intf(s) state: Down
Active Peer: Local
Standby Peer: Not exist
Log counters:
    role change to active: 1
    role change to standby: 0
    disable events: rg down state 1, rg shut 0

```

show redundancy application group

```
ctrl intf events: up 0, down 2, admin_down 1
reload events: local request 2, peer request 0
```

```
RG Media Context for RG 2
```

```
-----
Ctx State: Active
Protocol ID: 2
Media type: Default
Control Interface: GigabitEthernet0/1/0
Hello timer: 5000
Effective Hello timer: 5000, Effective Hold timer: 15000
  LAPT values: 0, 0
Stats:
  Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
  Authentication not configured
  Authentication Failure: 0
  Reload Peer: TX 0, RX 0
  Resign: TX 0, RX 0
  Standby Peer: Not Present.
```

Table 47 describes the significant fields shown in the display.

Table 47 show redundancy application group all Field Descriptions

Field	Description
Faults states Group 1 info	Redundancy group faults information for Group 1.
Runtime priority	Current redundancy group priority of the group.
RG Faults RG State	Redundancy group state returned by redundancy group faults.
Total # of switchovers due to faults	Number of switchovers triggered by redundancy group fault events.
Total # of down/up state changes due to faults	Number of down and up state changes triggered by redundancy group fault events.
Group ID	Redundancy group ID.
Group Name	Redundancy group name.
Administrative State	The redundancy group state configured by users.
Aggregate operational state	Current redundancy group state.
My Role	The current role of the device.
Peer Role	The current role of the peer device.
Peer Presence	Indicates if the peer device is detected or not.
Peer Comm	Indicates the communication state with the peer device.
Peer Progression Started	Indicates if the peer box has started RF progression.
RF Domain	The name of RF domain for the redundancy group.

Related Commands

Command	Description
show redundancy application group	Displays redundancy group information.
show redundancy application control-interface	Displays control-interface information for a redundancy group.

Command	Description
show redundancy application faults	Displays faults specific information for a redundancy group.
show redundancy application protocol	Displays protocol specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

show redundancy application transport

To display transport specific information for a redundancy group, use the **show redundancy application transport** command in privileged EXEC mode.

```
show redundancy application transport { client | group [group-id ]}
```

Syntax Description

client	Displays transport client specific information.
<i>group-id</i>	(Optional) Redundancy group group is. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application transport** command shows information for redundancy group transport.

Examples

The following is sample output from the **show redundancy application transport group** command:

```
Router# show redundancy application transport group 1

Transport Information for RG (1)
```

Related Commands

Command	Description
show redundancy application group	Displays redundancy group information.
show redundancy application control-interface	Displays control-interface information for a redundancy group.
show redundancy application faults	Displays faults specific information for a redundancy group.
show redundancy application protocol	Displays protocol specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

show redundancy application control-interface

To display control-interface information for a redundancy group, use the **show redundancy application control-interface** command in privileged EXEC mode.

show redundancy application control-interface group [*group-id*]

Syntax Description

group	Redundancy group.
<i>group-id</i>	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application control-interface** command shows information of the redundancy group control interfaces

Examples

The following is sample output from the **show redundancy application control-interface** command:

```
Router# show redundancy application control-interface group 2
```

```
The control interface for rg[2] is GigabitEthernet0/1/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
```

Related Commands

Command	Description
show redundancy application group	Displays redundancy group information.
show redundancy application faults	Displays faults specific information for a redundancy group.
show redundancy application protocol	Displays protocol specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

show redundancy application faults

To display faults specific information for a redundancy group, use the **show redundancy application faults** command in privileged EXEC mode.

```
show redundancy application faults group [group-id]
```

Syntax Description

group	Redundancy group.
<i>group-id</i>	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application faults** command shows information returned by redundancy group faults.

Examples

The following is sample output from the **show redundancy application faults** command:

```
Router# show redundancy application faults group 2

Faults states Group 2 info:
  Runtime priority: [150]
  RG Faults RG State: Up.
    Total # of switchovers due to faults:          2
    Total # of down/up state changes due to faults: 2
```

[Table 48](#) describes the significant fields shown in the display.

Table 48 show redundancy application group all Field Descriptions

Field	Description
Faults states Group 1 info	Redundancy group faults information for Group 1.
Runtime priority	Current redundancy group priority of the group. This field is important when monitoring redundancy group switchover and when configuring interface tracking.
RG Faults RG State	Redundancy group state returned by redundancy group faults.
Total # of switchovers due to faults	Number of switchovers triggered by redundancy group fault events.
Total # of down/up state changes due to faults	Number of down and up state changes triggered by redundancy group fault events.

Related Commands

Command	Description
show redundancy application group	Displays redundancy group information.
show redundancy application control-interface	Displays control-interface information for a redundancy group.
show redundancy application protocol	Displays protocol specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

show redundancy application protocol

To display protocol specific information for a redundancy group, use the **show redundancy application protocol** command in privileged EXEC mode.

show redundancy application protocol {*protocol-id* | **group** [*group-id*]}

Syntax Description		
	<i>protocol-id</i>	Protocol ID. The range is from 1 to 8.
	group	Redundancy group.
	<i>group-id</i>	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines The **show redundancy application protocol** command shows information returned by redundancy group protocol.

Examples The following is sample output from the **show redundancy application protocol** command:

```
Router# show redundancy application protocol 3

Protocol id: 3, name:
  BFD: ENABLE
  Hello timer in msec: 0
  Hold timer in msec: 0
```

[Table 49](#) describes the significant fields shown in the display.

Table 49 *show redundancy application protocol Field Descriptions*

Field	Description
Protocol id	Redundancy group protocol ID.
BFD	Indicates whether the BFD protocol is enabled for the redundancy group protocol.
Hello timer in msec	Redundancy group hello timer, in milliseconds, for the redundancy group protocol. The default is 3000 msec.
Hold timer in msec	Redundancy group hold timer, in milliseconds, for the redundancy group protocol. The default is 10000 msec.

Related Commands

Command	Description
show redundancy application group	Displays redundancy group information.
show redundancy application control-interface	Displays control-interface information for a redundancy group.
show redundancy application faults	Displays faults specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

show redundancy application if-mgr

To display interface manager information for a redundancy group, use the **show redundancy application if-mgr** command in privileged EXEC mode.

```
show redundancy application if-mgr group [group-id]
```

Syntax Description

group	(Optional) Specifies the redundancy group.
<i>group-id</i>	(Optional) Redundancy group ID. The range is from 1 to 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application if-mgr** command shows information of traffic interfaces protected by Redundancy Groups. When a traffic interface is functioning with the redundancy group, the state is no shut on the active device, and shut on the standby device. On the other hand, it is always shut on the standby device.

Examples

The following is sample output from the **show redundancy application if-mgr** command:

```
Router# show redundancy application if-mgr group 2

RG ID: 2
Interface      VIP          VMAC          Shut   Decrement
=====
GigabitEthernet0/1/7 10.1.1.3 0007.b422.0016 no shut    50
GigabitEthernet0/3/1 11.1.1.3 0007.b422.0017 no shut    50
```

[Table 50](#) describes the significant fields shown in the display.

Table 50 show redundancy application if-mgr Field Descriptions

Field	Description
RG ID	Redundancy group ID.
Interface	Interface name.
VIP	Virtual IP address for this traffic interface.
VMAC	Virtual MAC address for this traffic interface.

Table 50 *show redundancy application if-mgr Field Descriptions (continued)*

Field	Description
Shut	The state of this interface. Note It is always “shut” on the standby box.
Decrement	The decrement value for this interface. When this interface goes down, the runtime priority of its redundancy group decreases.

Related Commands

Command	Description
show redundancy application group	Displays redundancy group information.
show redundancy application control-interface	Displays control-interface information for a redundancy group.
show redundancy application faults	Displays faults specific information for a redundancy group.
show redundancy application protocol	Displays protocol specific information for a redundancy group
show redundancy application group	Displays redundancy group information.

show redundancy application data-interface

To display data interface specific information, use the **show redundancy application data-interface** command in privileged EXEC mode.

```
show redundancy application data-interface group [group-id]
```

Syntax Description

group	Specifies the redundancy group.
<i>group-id</i>	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application data-interface** command displays information about the redundancy group data interfaces.

Examples

The following is sample output from the **show redundancy application data-interface** command:

```
Router# show redundancy application data-interface group 1
```

```
The data interface for rg[1] is GigabitEthernet0/1/1
```

Related Commands

Command	Description
show redundancy application group	Displays redundancy group information.
show redundancy application control-interface	Displays control-interface information for a redundancy group.
show redundancy application faults	Displays faults specific information for a redundancy group.
show redundancy application protocol	Displays protocol specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application group	Displays redundancy group information.

shutdown

To shut down a group manually, use the **shutdown** command in redundancy application group configuration mode. To enable a redundancy group, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The group is active.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

When a group is shutdown, it does not participate in the role negotiation. The group remains in the shutdown state until you execute the **no shutdown** command.

Examples

The following example shows how to shut down a group named group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# shutdown
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

timers hellotime

To configure timers for hellotime and holdtime messages for a redundancy group, use the **timers hellotime** command in redundancy application protocol configuration mode. To disable the timers in the redundancy group, use the **no** form of this command.

timers hellotime [**msec**] *seconds* **holdtime** [**msec**] *seconds*

no timers hellotime [**msec**] *seconds* **holdtime** [**msec**] *seconds*

Syntax Description

msec	(Optional) Specifies the interval, in milliseconds, for hello messages. The range is from 250 to 1000.
<i>seconds</i>	Interval time, in seconds, for hello messages. The range is from 1 to 254.
holdtime	Specifies the hold timer.
msec	Specifies the interval, in milliseconds, for hold time messages. The range is from 750 to 3000.
<i>seconds</i>	Specifies the interval time, in milliseconds, for hold time messages. The range is from 6 to 255.

Command Default

The default value for the hellotime interval is 3 seconds and for the holdtime interval is 10 seconds.

Command Modes

Redundancy application group protocol configuration (config-red-app-protc)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The hello time is an interval in which hello messages are sent. The holdtime is the time before the active or the standby device is declared to be in down state. Use the **msec** keyword to configure the timers in milliseconds.

Examples

The following example shows how to configure the hellotime and holdtime messages:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-protcl)# timers hellotime 100 holdtime 100
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.