

NAT Commands

- ip nat, on page 1
- ip nat inside source, on page 2
- ip nat inside source tcp static interface (loopback), on page 6
- ip nat log translations flow-export, on page 7
- ip nat outside source, on page 8
- ip nat pool, on page 10
- ip nat route vrf, on page 11
- ip nat service, on page 12
- ip nat settings preserve-sdwan-ports, on page 13
- ip nat translation (timeout), on page 14
- ip nat translation max-entries, on page 15
- nat64 provisioning, on page 16
- nat64 route, on page 18
- nat64 settings, on page 19
- nat64 settings mtu, on page 20
- nat64 translation timeout tcp, on page 21
- nat64 translation timeout udp, on page 21
- nat66 max vpn, on page 22
- nat66 outside, on page 23
- nat66 prefix, on page 23
- nat66 route vrf, on page 25

ip nat

To designate that traffic originating from the interface is subject to Network Address Translation (NAT), use the **ip nat** command in interface configuration mode. To designate that traffic originating from the interface is no longer subject to Network Address Translation (NAT), use the **no** form of this command.

ip nat outside
no ip nat outside

Syntax Description

outside	(Optional) Indicates that the interface is connected to the outside network.

Command Default

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

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Qualified for use in Cisco vManage CLI templates

Usage Guidelines

For the usage guidelines, see ip nat.

Examples

```
Device(config)# interface Ethernet 1
 Device(config-if)# ip nat outside
```

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* } **pool** *name* [**vrf** *name*] [**match-in-vrf** | **overload**] [**match-interface** | { *interface-name* }]
no ip nat inside source list { *access-list-number access-list-name* } **pool** *name* [**vrf** *name*] [**match-in-vrf** | **overload**] [**match-interface** | { *interface-name* }]

Static NAT

ip nat inside source static *local-ip global-ip* [**vrf** *name*] [**match-in-vrf** [**track** *track-id*] [**pool** *name*] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } | [**egress-interface** *type*] | [**extendable**] { [**match-in-vrf** [**pool** *name*]] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } }]
no ip nat inside source static *local-ip global-ip* [**vrf** *name*] [**match-in-vrf** [**track** *track-id*] [**pool** *name*] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } | [**egress-interface** *type*] | [**extendable**] { [**match-in-vrf** [**pool** *name*]] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } }]

Syntax Description

list *access-list-number*	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 *access-list-name*	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.
interface	Specifies an interface for the global address.
type	Interface type. For more information, use the question mark (?) to enable the online help function.

number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) to enable the online help function.
pool *name*	Specifies the name of the pool from which global IP addresses are allocated dynamically. From Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can use a NAT pool for static NAT.
overload	(Optional) Enables the device 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.
vrf *name*	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance.
egress-interface *type*	(Optional) Specifies the type of egress interface used for port forwarding with NAT DIA.
match-in-vrf	(Optional) Enables NAT inside and outside traffic in the same VRF.
match-interface *interface-name*	Specifies the interface name to apply the centralized data policy to for matching a NAT method with a NAT DIA egress interface.
track *track-id*	(Optional) Enables service-side NAT object tracking of LAN prefixes and LAN interfaces.
static	Sets up a single static translation.
local-ip	Local IP address assigned to a host on the inside network. The address could be randomly chosen, allocated from RFC 1918, or be an obsolete one.
global-ip	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.
tcp	Establishes the TCP protocol.
udp	Establishes the UDP protocol.
local-port	Local TCP or UDP port. The range is from 1 to 65535.
global-port	Global TCP or UDP port. The range is from 1 to 65535.

Command Default No NAT translation of inside source addresses occurs.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was modified. The **pool** *pool* keyword-argument pair is supported for static NAT.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was modified. Added the **track** keyword for service-side NAT object tracking.
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was modified. Added the **egress-interface** *type* keyword for port forwarding for NAT DIA.
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command was modified. Added the **match-interface** *interface-name* keyword fork mapping multiple NAT methods for NAT DIA.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip nat inside source` command.

Examples

The following example shows how to translate between inside hosts addressed from one network to the globally unique network:

```
Device(config)# ip nat pool net-209 10.255.255.254 10.255.255.255 prefix-length 28
ip nat inside source list 1 pool net-209
!
interface ethernet 0
 ip address 10.0.0.1 255.255.255.224
 ip nat outside
!
interface ethernet 1
 ip address 10.255.255.254 10.255.255.255
 ip nat inside
!
access-list 1 permit 192.168.255.255 255.255.0.
access-list 1 permit 192.168.255.255 255.255.224.
```

The following example shows how to translate local traffic to an edge device that is using NAT (NAT-PE):

```
Device(config)# 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 0.0.0.0 0.0.0.0 192.168.255.254
ip route vrf vrf2 0.0.0.0 0.0.0.0 192.168.255.255
!
access-list 1 permit 0.0.0.0 255.0.0.0
!
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 0.0.0.0 0.0.0.0 192.168.0.0 global
ip route vrf vrf2 0.0.0.0 0.0.0.0 192.168.0.1 global
access-list 1 permit 0.0.0.0 255.0.0.0
```

The following example shows how to configure a NAT pool using static inside NAT.

```
Device(config)# ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
```

The following example shows how to configure a NAT pool using static inside and static outside NAT.

```
Device(config)# ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
ip nat outside source static 192.168.21.10 10.22.22.10 vrf 1 match-in-vrf pool natpool1
```

The following example shows how to configure an inside static NAT global pool with a tracker name and a tracker ID for tracking service-side NAT objects:

```
Device(config)# ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf
track 1
```

For more information on configuring the service-side NAT object tracker, see the *Cisco SD-WAN NAT Configuration Guide*.

The following example shows how to configure NAT DIA port forwarding:

```
Device(config)# interface GigabitEthernet1
ip address 10.1.2.1 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
end
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload
ip nat inside source static tcp 192.168.1.100 443 interface GigabitEthernet1 8443 vrf 1
ip nat inside source static tcp 192.168.1.100 80 10.1.2.10 80 vrf 1 egress-interface
GigabitEthernet1
ip nat inside source static tcp 192.168.1.100 22 10.1.2.20 2020 vrf 1 egress-interface
GigabitEthernet1
```

For more information on configuring NAT DIA port forwarding, see the *Cisco SD-WAN NAT Configuration Guide*.

The following is a sample configuration for configuring multiple NAT DIA where the default NAT method is using a NAT pool and the alternative or secondary NAT method is using interface overload with match-interface:

```
interface GigabitEthernet1
 ip address 10.1.1.1 255.255.255.0
 no ip redirects
 load-interval 30
 negotiation auto
 ip nat outside
 !
 ip nat inside source list dia-list 1 pool natpool1 overload egress-interface GigabitEthernet1

 ip nat inside source list dia-list 1 interface GigabitEthernet1 overload match-interface
GigabitEthernet1
```

For more information about configuring the multiple NAT methods for an interface using CLI, see the section "Configure Multiple NAT Types Using CLI" in Cisco SD-WAN NAT Configuration Guide.

ip nat inside source tcp static interface (loopback)

To enable the loopback interface of the inside source address, use the **ip nat inside source static tcp interface (loopback)** command in global configuration mode.

ip nat inside source static tcp *local-ip local-port* **interface** *interface-type interface-number* [**egress-interface** *interface-type interface-number* | **vrf** *vrf-name* **egress-interface** *interface-type interface-number*]

Syntax Description

local-ip	Local IP address assigned to a host on the inside network.
interface-type interface-number	Specifies the loopback interface type and the loopback interface number.
vrf *name*	(Optional) Associates the NAT translation rule with a particular VPN routing and forwarding (VRF) instance. The VRF keyword along with a VRF name. When you don't specify a value for the VRF number, port forwarding is configured on the transport VPN, which is VPN 0, by default.
egress-interface *interface-type interface-number*	(Optional) Specifies the egress interface type and the egress interface number that are used for port forwarding with NAT DIA with loopback interface.

Command Default

Loopback interface of the inside source address is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is introduced.

Usage Guidelines

Configure the WAN interface before you configure the loopback interface.

Optionally, you can provide the egress interface, for example, **GigabitEthernet1**, which is the internet-facing interface.

The following example shows how to configure port forwarding with NAT DIA by using a loopback interface:

Configure **ip nat outside** on the WAN interface:

```
interface GigabitEthernet1
 ip address 10.1.2.1 255.255.255.0
 ip nat outside
 negotiation auto
 no mop enabled
```

```
 no mop sysid
exit
```

Define the loopback interface:

```
interface Loopback3
 ip address 10.1.3.1 255.255.255.255
exit
```

Configure the loopback interface:

```
ip nat inside source static tcp 192.168.1.100 8080 interface Loopback3 8585 vrf 1
egress-interface GigabitEthernet1
ip nat inside source static tcp 192.168.1.100 80 interface Loopback3 5050 egress-interface
 GigabitEthernet1
```

For more information about configuring the loopback interface, see *Configure Port Forwarding with NAT DIA Using a CLI Template*.

Related Commands

Commands	Description
ip nat	Ensures that traffic originating from the interface is subject to Network Address Translation (NAT)
negotiation [auto]	Specifies enabling the autonegotiation protocol to configure the speed, duplex, and automatic flow control of the Gigabit Ethernet interface.
static	Sets up a single static translation.
tcp	Establishes the TCP protocol.
egress-interface	Specifies the type of egress interface used for port forwarding with NAT DIA using a loopback interface.

ip nat log translations flow-export

To enable the high-speed logging of translations by NAT, use the **ip nat log translations flow-export** command in global configuration mode. To disable the logging of NAT translations by using a flow exporter, use the **no** form of this command.

ip nat log translations flow-export v9 udp { **destination** *IPv4address port* } [**vrf** *vrf-name* | **source** *interface-name interface-number*]
no ip nat log translations flow-export

Syntax Description

v9	Specifies the flow exporter Version 9 format.
udp	Specifies the UDP.
destination	Specifies the destination IPv4 address. It can be IPv4 global (vpn0/transport vpn) or IPv4 vrf (service vpn).
ipv4 address	Specifies the IPv4 address of the destination.

local-udp-port	Specifies the local UDP port number. Valid values are from 1 to 65335.
source *interface-type interface-number*	(Optional) Specifies the source interface for which translations will be logged.
vrf *vrf-name*	(Optional) Specifies the destination VRF.

Command Default

Logging is disabled for all NAT translations.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco IOS XE Release 17.6.4 and later 17.6.x releases	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip nat log translations flow-export command.

Examples

The following example shows how to enable translation logging for a specific destination and source interface:

```
Device(config)# ip nat log translations flow-export v9 udp destination 10.10.0.1 1020 source
 gigabithethernet 0/0/1
```

Related Commands

Commands	Description
clear ip nat translations	Clears dynamic NAT translations from the translation table.
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* } } **pool** *pool-name* [**vrf** *name*]
no ip nat outside source { **list** { *access-list-number* *access-list-name* } } **pool** *pool-name* [**vrf** *name*]

Static NAT
ip nat outside source static *local-ip global-ip* [**vrf** *name*] [**match-in-vrf** [**pool** *name*] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } | [**extendable**] { [**match-in-vrf** [**pool** *name*]] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } }]

no ip nat outside source static *local-ip global-ip* [**vrf** *name*] [**match-in-vrf** [**pool** *name*] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } | [**extendable**] { [**match-in-vrf** [**pool** *name*]] | **pool** *name* | **no-payload** { **match-in-vrf** [**pool** *name*] | **pool** *name* } }]

Syntax Description

list *access-list-number*	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 *access-list-name*	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.
pool *pool-name*	Specifies the name of the pool from which global IP addresses are allocated. Starting Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, you can use a NAT pool for static NAT.
vrf *name*	(Optional) Associates the NAT rule with a particular VPN routing and forwarding (VRF) instance.
static	Sets up a single static translation.
global-ip	Globally unique IP address assigned to a host on the outside network by its owner. The address was allocated from the globally routable network space.
local-ip	Local IP address of an outside host as it appears to the inside network. The address was allocated from the address space routable on the inside (RFC 1918, *Address Allocation for Private Internets*).
match-in-vrf	(Optional) Matches the incoming VRF.
extendable	(Optional) Extends the transmission.

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.3.1a	The **match-in-vrf** keyword is added.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was modified. The **pool** *pool* keyword-argument pair is supported for Static NAT.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `ip nat outside source` command.

Examples

The following example shows how to translate between inside hosts addressed from the 10.0.0.1 network to the globally unique 10.0.0.0/28 network. Further, packets from outside hosts addressed from the 10.255.255.254 network are translated to appear to be from the 10.255.255.255/24 network.

```
ip nat pool net-208 10.255.255.254 10.255.255.255 prefix-length 28
```

```
ip nat pool net-10 10.255.255.254 10.255.255.255 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 10.0.0.1 255.255.255.224
 ip nat outside
!
interface ethernet 1
 ip address 10.0.0.1 255.255.255.224
 ip nat inside
!
access-list 1 permit 10.255.255.254 10.255.255.255
```

Static NAT Inside with NAT Pool

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
```

Static NAT Inside and Static NAT Outside with NAT Pool

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
ip nat outside source static 192.168.21.10 10.22.22.10 vrf 1 match-in-vrf pool natpool1
```

ip nat pool

To define a pool of IP addresses for Network Address Translation (NAT) translations, 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* [**prefix-length** *prefix-length*]
no ip nat pool *name*

Syntax Description

name	Name of the pool.
start-ip	Starting IP address that defines the range of addresses in the address pool.
end-ip	Ending IP address that defines the range of addresses in the address pool.
prefix-length *prefix-length*	Specifies the number that indicates how many bits of the address is dedicated for the network.

Command Default

No pool of addresses is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE, see ip nat pool command.

Examples

The following example shows how to translate between inside hosts addressed from one network to a globally unique network:

```
ip nat pool net-208 10.0.0.0 10.255.255.254 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
 ip address 10.0.0.1 255.255.255.224
 ip nat outside
!
interface ethernet 1
 ip address 192.168.255.255 255.255.0.0
 ip nat inside
!
access-list 1 permit 192.168.0.0 255.240.0.0
access-list 1 permit 192.168.0.1 255.255.0.0
```

ip nat route vrf

To configure an IP NAT route, use the **ip nat route vrf** command in global configuration mode. To remove the IP NAT route, use the **no** form of this command.

ip nat route vrf { *vrf* | *route-prefix* | *prefix-mask* | **global** }

no ip nat route vrf { *vrf* | *route-prefix* | *prefix-mask* | **global** }

Syntax Description

vrf	Specifies the service VRF.
route-prefix	Specifies the route prefix.
prefix-mask	Specifies the route mask.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.3.1	Command qualified for use in Cisco SD-WAN Manager C

Usage Guidelines

This command can be used to configure an IP NAT route using device templates to route traffic from the service-side to the transport-side (VPN 0) interface that has NAT enabled.

This command can be used for DIA solution.

Example

The following example shows how to configure an IP NAT default route to route traffic from service-side to the transport-side (VPN 0) NAT-enabled interface.

```
Device(config)# ip nat route vrf 65529 0.0.0.0 0.0.0.0 global
```

ip nat service

To enable an application-level gateway (ALG) for NAT translations of embedded IP addresses and port numbers in the payload of a packet, use the **ip nat service** command in global configuration mode. To disable ALG processing of NAT translations of embedded IP addresses and port numbers in the payload of a packet, use the **no** form of this command.

ip nat service { **all-algs** | **dns** { **tcp** | **udp** } | **ftp** | **sip** { **tcp** | **udp** } **port** *port-number* }

no ip nat service

Syntax Description

all-algs	Enables global NAT ALG for translation of IP address and port information inside the payload of an application packet.
dns	Enables Domain Name System (DNS) processing with an ALG for either TCP or UPD.
tcp	Specifies the TCP protocol.
udp	Specifies the UDP protocol.
ftp	Enables FTP processing with an ALG.
sip	Enables Session Initiation Protocol (SIP) processing with an ALG for either TCP or UDP.
port *port-number*	Specifies the port other than the default port in the range from 1 to 65533.

Command Default

NAT ALG translation support is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

Enable NAT ALG globally prior to enabling NAT ALG per protocol.

Examples

The following example shows how to enable global NAT ALG globally:

```
Device(config)# ip nat service all-algs
```

The following examples show how to enable NAT ALG for DNS for either TCP or UDP protocols:

```
Device(config)# ip nat service dns tcp
```

```
Device(config)# ip nat service dns udp
```

The following example shows how to enable NAT ALG for FTP:

```
Device(config)# ip nat service ftp
```

The following example shows how to enable NAT ALG for SIP for either TCP or UDP with port 5060:

```
Device(config)# ip nat service sip tcp port 5060
```

```
Device(config)# ip nat service sip udp port 5060
```

Related Commands

Commands	Description
clear ip nat translations	Clears dynamic NAT translations from the translation table.
show ip nat translations	Displays active NAT translations.
show platform hardware qfp active feature nat datapath summary	Displays configured and operational data specific to NAT.

ip nat settings preserve-sdwan-ports

To configure source ports preservation for the known SD-WAN port range during NAT, use the **ip nat settings preserve-sdwan-ports** command in global configuration mode. To remove the port preservation, use the **no** form of the command.

ip nat settings preserve-sdwan-ports

no ip nat settings preserve-sdwan-ports

Syntax Description

This command has no arguments or keywords.

Command Default

NAT port preservation for the known SD-WAN ports is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

You may remove all NAT mapping configuration before configuring port-preservation command to allow port-preservation to take effect (avoiding reboot).

If there are existing NAT mapping configurations, ensure that you reboot the device after configuring the **ip nat settings preserve-sdwan-ports** command to achieve the expected behavior. If not, add NAT mapping configurations after configuring the **ip nat settings preserve-sdwan-ports** command.

Use the **ip nat settings preserve-sdwan-ports** command to enable port preservation for the control traffic using SD-WAN known ports. This is enabled during the following conditions:

- Interface overload
- Loopback overload

Examples

The following example shows how to configure NAT port preservation capability:

```
Device(config)# ip nat settings preserve-sdwan-ports
```

ip nat translation (timeout)

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

ip nat translation { **dns-timeout** | **syn-timeout** | **icmp-timeout** *max-entries* | **port-timeout** **tcp-timeout timeout udp-timeout** }
no ip nat translation { **dns-timeout** | **syn-timeout** | **icmp-timeout** *max-entries* | **port-timeout** **tcp-timeout timeout udp-timeout** }

Syntax Description

dns-timeout	Specifies that the timeout value applies to connections to the Domain Name System (DNS). The default is 60 seconds.
syn-timeout	Specifies that the timeout value applies to 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.
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-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 UDP port. The default is 300 seconds (5 minutes).

Command Default

NAT translation timeouts are enabled by default.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines When port translation is configured, each entry contains more information about the traffic that is using the translation, 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 a TCP Reset (RST) or a Finish (FIN) bit is seen on the stream, in which case they will time out in 1 minute.

For usage guidelines, see the Cisco IOS XE ip nat translation (timeout) command.

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

```
Device# configure terminal
Device(config)# ip nat translation udp-timeout 600
```

ip nat translation max-entries

To specify the maximum number of network address translation entries stored by the router, use the **ip nat translation max-entries** command in global configuration mode. To restore the default number of NAT entries, use the **no** form of this command.

ip nat translation max-entries *max-entries*
no ip nat translation max-entries *max-entries*

Syntax Description

max-entries *max-entries*	(Optional) Specifies the maximum number (1-2147483647) of NAT-PT translation entries. Default is unlimited.

Command Default No maximum size is specified for the NAT table.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco vManage CLI templates.

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 ACL, or a VRF instance is generating an unexpectedly high number of NAT requests, the host may be the source of a virus or worm attack.

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

Example

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

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

nat64 provisioning

To configure the Network Address Translation 64 (NAT64) Mapping and Port Address Encapsulation (MAP-E) domain and MAP-E parameters, use the **nat64 provisioning** command in global configuration mode and NAT64 provisioning configuration mode. To disable NAT64 provisioning, use the **no** form of the command.

nat64 provisioning { **mode jp01** | **address-resolution-server** { **2** | **6** *address-resolution-server-url password username* } **api-key** { **2** | **6** *api-key-id* } | **hostname** *hostname* | **rule-server** { *rule-server-url* | **2** | **6** | **request wait-time** *wait-time-value* | **service-prefix** *ipv6-prefix* | **tunnel** { **interface** *interface-type* | **source** *interface-type* } } | **version draft-ietf-softwire-map-03** }

no nat64 provisioning

Syntax Description

mode	Specifies the NAT64 MAP-E domain and enters the NAT64 provisioning configuration mode.
jp01	Specifies the NAT64 provisioning mode.
address-resolution-server 2 6 *address-resolution-server-url username password*	Specifies the URL of the address resolution server. Allows you to configure the username and password of the address resolution server. Specifies an encryption type (2 or 6) for encrypting the username and password of the address resolution server.
api-key 2 6 *api-key-id*	Specifies the NAT64 API key ID. Specifies an encryption type (2 or 6) for encrypting the API key ID.
hostname *hostname*	Specifies the hostname of the Domain Name System (DDNS). The hostname comes from the MAP-E rule server. **Note** In case you overwrite the hostname, you can specify a new hostname.

rule-server 2 6 request wait-time *wait-time-value*	Specifies the URL of the MAP-E rule server. Specifies an encryption type (2 or 6) for encrypting the rule server URL. You enter the rule server URL in clear text. The rule server URL is later encrypted in the output of the **show running-config** command. (Optional) Specifies the wait time in seconds after the MAP-E CE device receives the Dynamic Domain Name System (DDNS) response. The wait time is before the DDNS response is sent to the MAP-E rule server.
service-prefix *ipv6-prefix*	Specifies the IPv6 prefix of the address resolution server. **Note** The service prefix needs to match the IPv6 prefix of the MAP-E rule returned by the border router.
tunnel interface *interface-name interface-number*	Specifies the NAT64 provisioning tunnel.
source *interface-type interface-number*	Specifies the NAT64 tunnel source.
version draft-ietf-softwire-map-03	Specifies the version of the MAP-E specification.

Command Default

NAT64 provisioning is not enabled.

Command Modes

Global configuration (config) mode and NAT64 provisioning configuration mode (config-nat64-provisioning)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

Use this command to configure a MAP-E domain and parameters for transporting IPv4 packets over an IPv6 network using IP encapsulation.

Example

The following example shows how to enable NAT64 provisioning and configure the MAP-E domain and parameters:

```
Device(config)# nat64 settings fragmentation header disable
Device(config)# nat64 route 0.0.0.0/0 GigabitEthernet1
Device(config)# nat64 settings v4 tos ignore
Device(config)# interface GigabitEthernet1
Device(config-if)# nat64 settings mtu minimum 1500
Device(config-if)# nat64 provisioning mode jp01
Device(config-nat64-provisioning)# address-resolution-server
http://2001:db8:b000:0:fe7f:6ee7:33db:5013/nic/update
Device(config-nat64-provisioning)# address-resolution-server password encypted-password
Device(config-nat64-provisioning)# address-resolution-server username encypted-username
Device(config-nat64-provisioning)# rule-server
http://admin:admin@2001:DB8:A000::1//mape-rule.json
```

```
Device(config-nat64-provisioning)# rule-server request wait-time 180
Device(config-nat64-provisioning)# hostname hostname
Device(config-nat64-provisioning)# tunnel interface Tunnel1
Device(config-nat64-provisioning)# tunnel source GigabitEthernet2
Device(config-nat64-provisioning)# service-prefix 2001:DB8:b800::/48
```

Related Commands

Commands	Description
nat64 route	Specify NAT64 prefix to which an IPv4 prefix should be translated.
nat64 settings	Configure NAT64 settings.
nat64 settings mtu	Configure the path maximum transmission unit (MTU) size for preventing fragmentation of IPv4 packets for translation to IPv6.

nat64 route

To specify the Network Address Translation 64 (NAT64) 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

ipv4-prefix / *mask*	Length of the IPv4 prefix and the mask.
interface-type	Interface type. For more information, use the question mark (?) online help.
interface-number	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 Catalyst SD-WAN Release 17.10.1a	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.

For usage guidelines, see the Cisco IOS XE nat64 route command.

Example

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

```
Device(config)# nat64 route 0.0.0.0/0 GigabitEthernet1
```

Related Commands

Commands	Description
nat64 provisioning	Configure the Mapping and Port Address Encapsulation (MAP-E) domain and parameters.
nat64 settings	Configure NAT64 settings.
nat64 settings mtu	Configure MTU size for preventing fragmentation of IPv4 packets for translation to IPv6 using NAT64.

nat64 settings

To configure Network Address Translation 64 (NAT64) settings, use the **nat64 settings** command in global configuration mode. To disable NAT64 settings, use the **no** form of this command.

nat64 settings { **fragmentation header disable** | **v4 tos ignore** }
no nat64 settings { **fragmentation header disable** | **v4 tos ignore** }

Syntax Description

fragmentation header disable	Disables the NAT64 fragmentation header.
v4 tos ignore	Specifies not to copy the IPv4 type-of-service (ToS) header.

Command Default

NAT64 settings are disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

By default, NAT64 adds a fragmentation header for all IPv4-to-IPv6 packets that do not have the Do Not Fragment (DF) bits set. Configure the **nat64 settings fragmentation header disable** command to disable the adding of a fragmentation header for packets that are not fragmented.

By default, NAT64 copies ToS bits from an IPv4 header to an IPv6 header. Configure the **nat64 settings v4 tos ignore** command to disable the copying of ToS bits from an IPv4 header to an IPv6 header.

Example

The following example shows how to disable the NAT64 fragmentation header:

```
Router(config)# nat64 settings fragmentation header disable
```

Related Commands

Commands	Description
nat64 provisioning	Configure the Mapping and Port Address Encapsulation (MAP-E) domain and parameters.
nat64 settings mtu	Configure MTU size for preventing fragmentation of IPv4 packets for translation to IPv6 using NAT64.

nat64 settings mtu

To configure the path maximum transmission unit (MTU) size for preventing fragmentation of IPv4 packets for translation to IPv6 using Network Address Translation (NAT64), use the **nat64 settings mtu** command in interface configuration mode. To disable the MTU size for NAT64, use the **no** form of this command.

nat64 settings mtu minimum *mtu-value*
no nat64 settings mtu

Syntax Description

minimum *mtu-value*	MTU size in bytes.

Command Default

NAT64 MTU size is not set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Additional parameter qualified: **mtu**.

Usage Guidelines

Path maximum transmission unit (MTU) discovery prevents fragmentation in the path between endpoints. Path MTU discovery is used to dynamically determine the lowest MTU along the path from a packet's source to its destination. Path MTU discovery is supported only by TCP and UDP. Path MTU discovery is mandatory in IPv6, but it is optional in IPv4. IPv6 devices never fragment a packet—only the sender can fragment packets.

Example

The following example shows how to set the MTU size for NAT64:

```
Router(config)# interface GigabitEthernet1
Router(config-if)# nat64 settings mtu minimum 1500
```

Related Commands

Commands	Description
nat64 settings	Configure NAT64 settings.

nat64 translation timeout tcp

To configure a NAT64 translation timeout value for TCP traffic, use **nat64 translation timeout tcp** command in global configuration mode. To remove the configuration, use the **no** form of this command.

nat64 translation timeout tcp { *time* | **never** }

no nat64 translation timeout tcp { *time* | **never** }

Syntax Description

time	Specifies the timeout value. Range: 0 to 536870 seconds.
never	Specifies that TCP translation never expires.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.3.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to configure a NAT64 translation timeout value for TCP traffic.

Example

The following example shows how to configure a NAT64 translation timeout value for TCP traffic to 30 seconds.

```
Device(config)# nat64 translation timeout tcp 30
```

nat64 translation timeout udp

To configure a NAT64 translation timeout value for UDP traffic, use the **nat64 translation timeout udp** command in global configuration mode. To remove the configuration, use the **no** form of this command.

nat64 translation timeout udp { *time* | **never** }

no nat64 translation timeout udp { *time* | **never** }

Syntax Description

time	Specifies the timeout value. Range: 0–536870 seconds.
never	UDP translation never expires.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.3.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to configure a NAT64 translation timeout value for UDP traffic.

Example

The following example shows how to configure a NAT64 translation timeout value for UDP traffic to two seconds.

```
Device(config)# nat64 translation timeout udp 2
```

nat66 max vpn

To configure the maximum number of virtual routing and forwarding (VRF) connections allowed for prefix translation, use the **nat66 max-vpn** command in global configuration mode. To remove the maximum number of VRFs allowed for prefix translation, use the **no** form of this command.

nat66 max-vpn *number*

no nat66 max-vpn

Syntax Description

max-vpn *number*	Specifies the maximum number of VRF connections allowed for prefix translation. The maximum number of VRFs allowed is 250.

Command Default

The maximum number of VRF connections are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

When using prefix delegation (PD) with NAT66, an outside prefix is extended by adding a VRF ID to the prefix translation. An inside prefix length of /64 and a PD prefix length of /56 results in /56 + 8 bits of a VRF ID for an outside prefix length.

Examples

The following example shows how to configure the maximum number of VRFs allowed for prefix translation:

```
Device(config)# nat66 max-vpn number
```

nat66 outside

To configure a NAT66 outside network interface for prefix translation, use the **nat66 outside** command in interface configuration mode. To remove the NAT66 outside network address prefix, use the **no** form of this command.

nat66 outside

no nat66 outside

Syntax Description

This command has no arguments or keywords.

Command Default

No NAT66 outside network interface is configured for prefix translation.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE nat66 outside command.

Examples

The following example shows how to configure a NAT66 outside network interface:

```
Device(config-if)# nat66 outside
```

nat66 prefix

To configure translation of an inside and an outside IPv6 source address prefix for NAT66 translation, use the **nat66 prefix** command in global configuration mode. To remove the IPv6 prefix from the IPv6 prefix translation, use the **no** form of this command.

nat66 prefix inside *prefix/prefix-length* **outside** *prefix/prefix-length* **interface** *interface-type interface-number* **vrf** *vrf-id* **egress-interface** *interface-type interface-number*

no nat66 prefix inside *prefix/prefix-length* **outside** *prefix/prefix-length* **interface** *interface-type interface-number* **vrf** *vrf-id* **egress-interface** *interface-type interface-number*

Syntax Description

inside	Specifies the IPv6 inside network.
outside	Specifies the IPv6 outside network.
prefix	The IPv6 network prefix.
prefix-length	The length of the IPv6 address prefix.

interface *interface-type interface-number*	Specifies the outside interface type and interface number that are automatically assigned global IPv6 addresses by Stateless Address Autoconfiguration (SLAAC) for forwarding packets.
vrf *vrf-id*	Specifies the VRF and VRF ID used for prefix translation.
egress-interface *interface-type interface-number*	(Optional) Specifies the egress interface type and the egress interface number that are used for forwarding packets to the internet-facing or WAN interface.

Command Default

No prefix translations are configured for an inside or an outside IPv6 source address.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command was modified. Added the **egress-interface** type keyword to configure multiple WAN links for NAT66 DIA.
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command was modified. Added the **interface** keyword to configure the outside interface type and interface-number for NAT66 DIA translations by Stateless Address Autoconfiguration (SLAAC).

Usage Guidelines

For usage guidelines, see the Cisco IOS XE nat66 prefix command.

Examples

The following example shows how to configure IPv6-to-IPv6 address prefix translation:

```
Device(config)# nat66 prefix inside 2001:DB8:A14:18::/80 outside 2001:DB8:A1:F::/80 vrf 1
```

The following example shows how to configure NAT66 DIA with two interfaces, GigabitEthernet1 and GigabitEthernet4:

```
interface GigabitEthernet1
 no shutdown
 ipv6 address 2001:a1:f::f/64
 ipv6 nd ra suppress all
 no mop enabled
 no mop sysid
 negotiation auto
 nat66 outside
!
interface GigabitEthernet4
 no shutdown
 ipv6 address 2001:a0:14::f/64
 ipv6 enable
 ipv6 nd ra suppress all
 no mop enabled
 no mop sysid
 negotiation auto
 nat66 outside
!
```

```
nat66 prefix inside 2001:a14:18:0::/64 outside 2001:a1:f::/64 vrf 1 egress-interface
GigabitEthernet1
nat66 prefix inside 2001:a14:18:0::/64 outside 2001:a0:14::/64 vrf 1 egress-interface
GigabitEthernet4
nat66 prefix inside FC00:1:2:3::/80 outside 3001:a1:5::/80 vrf 100
nat66 route vrf 1 2001:a0:5::/64 global
nat66 route vrf 100 ::/0 global
```

The following example shows how to configure Stateless Address Autoconfiguration (SLAAC) to automatically assign IPv6 addresses for NAT66 prefix translations:

Enable NAT66 outside network interface on the NAT66 DIA WAN interface:

```
interface GigabitEthernet1
  nat66 outside
```

Enable automatic configuration of IPv6 address on the NAT66 DIA WAN interface:

```
interface GigabitEthernet1
 ipv6 address autoconfig
 ipv6 enable
 ipv6 nd autoconfig default-route
```

Create SLAAC mapping translation rules with the NAT66 DIA WAN interface:

```
nat66 prefix inside 2001:a0:5::/64 outside interface GigabitEthernet1 vrf 1
nat66 prefix inside 2001:a0:5::/64 outside interface GigabitEthernet1
```

For more information about configuring SLAAC to automatically assign IPv6 addresses for NAT66 prefix translations, see the section *Configure NAT66 DIA Using Stateless DHCP* in *How NAT66 DIA Works*.

nat66 route vrf

To configure a NAT66 VRF route, use the **nat66 route vrf** command in global configuration mode. To disable the configuration of a NAT66 VRF route, use the **no** form of this command.

nat66 route vrf *vrf-name ipv6-dest-prefix* **global**

no nat66 route vrf *vrf-name ipv6-dest-prefix* **global**

Syntax Description

vrf	Specifies all the virtual private network (VPN) VRF tables or a specific VRF table for IPv6 addresses.
vrf-name	The name of a specific VRF table for an IPv6 address.
ipv6-dest-prefix	The IPv6 destination prefix.
global	Specifies the globally routable prefix.

Command Default

No NAT66 VRF route is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following example shows how to configure the NAT66 VRF route:

```
Device(config)# nat66 route vrf 1 2001:DB8:A14:19::/64 global
Device(config)# nat66 route vrf 1 2001:DB8:3D0:1::/64 global
```