NAT64 on Cisco IOS XE SD-WAN Devices

Table 1: Feature History

Feature Name	Release Information	Description
Service-Side NAT64 for Cisco IOS XE SD-WAN Devices	Cisco IOS XE SD-WAN Release 16.12.1b Cisco vManage Release 19.2.1	The service-side Network Address Translation (NAT) 64 feature translates a source IPv6 address to available IPv4 addresses in a NAT pool. The destination IPv6 address is translated to the server's actual IPv4 address since the destination IPv6 address is an IPv4 embedded IPv6 address. Service-side NAT64 allows IPv4 servers to communicate with IPv6 clients.
NAT64 DIA for Cisco IOS XE SD-WAN Devices	Cisco IOS XE SD-WAN Release 16.12.1b Cisco vManage Release 19.2.1	The NAT64 Direct Internet Access (DIA) feature supports routing of traffic from branch sites directly to the internet instead of tunneling the internet traffic to a central site or data center for internet access.

- Prerequisites for NAT64, on page 2
- Restrictions for NAT64 , on page 2
- Restrictions for IPv4 Addresses for NAT64, on page 2
- Information About NAT64, on page 2
- Configure NAT64, on page 4
- Configure a NAT64 Pool, on page 5
- Configure NAT64 Using the CLI, on page 6
- Verify Configuration of NAT64, on page 6
- Configuration Examples for NAT64, on page 8
- NAT64 Direct Internet Access, on page 8
- Restrictions for NAT64 DIA, on page 8
- Information About NAT64 Direct Internet Access, on page 9
- Configure NAT64 DIA, on page 9
- Configure a NAT64 DIA Route, on page 10
- Configure a NAT64 DIA Route Using the CLI, on page 11
- Verify NAT64 DIA Route Configuration, on page 11
- Configuration Example for NAT64, on page 12

• Advertise NAT64 Routes Through OMP, on page 12

Prerequisites for NAT64

- For Domain Name System (DNS) traffic to work, you must have a separate working installation of DNS64.

Restrictions for NAT64

- Traffic must always originate on the remote branch site and go to the IPv4 server on the local LAN within the local site.
- Traffic cannot originate from the IPv4 application server to any IPv6 client in the data center or to a remote branch site.
- Traffic flow is from the transport-side (WAN) to the service-side (LAN).

Restrictions for IPv4 Addresses for NAT64

- For more information on the usable IPv4 destination IP addresses, see the Deployment Guidelines, RFC 6052, Section 3.1.
- The well-known prefix (WKP) must not be used to represent non-global IPv4 addresses, such as those listed in the Deployment Guidelines, Section 3 of RFC 5735.

  For example, the following IPv4 prefixes are not allowed:

  - 0.0.0.0/8
  - 10.0.0.0/8
  - 127.0.0.0/8
  - 169.254.0.0/16

- You cannot use a private IPv4 address range on the service-side (LAN).

Information About NAT64

With the dwindling IPv4 public address space and the growing need for more routable addresses, service providers and enterprises continue to build and roll out IPv6 networks. As the IPv4 internet is going to stay for a while, communication between IPv4 and IPv6 networks is an important requirement for a seamless end-user experience.

Network Address Translation IPv6 to IPv4, or NAT64, technology facilitates communication between IPv6 and IPv4 networks.

The service-side NAT64 feature translates a source IPv6 address to available IPv4 addresses in a NAT44 pool. The destination IPv6 address is translated to the server's actual IPv4 address since the destination IPv6 address is an IPv4-embedded IPv6 address.

Cisco IOS XE SD-WAN devices use stateful NAT64 for translating IPv6 addresses to IPv4 addresses and IPv4 addresses to IPv6 addresses. Stateful NAT64 with NAT44 overload provides a 1:*n* mapping between IPv4 and IPv6 addresses.

How Service-Side NAT64 Works

1. An IPv6 client attempts to connect to an IPv4 server.
2. The IPv6 client makes an IPv6 AAAA record Domain Name System (DNS) query, which is an IPv6 query for an IPv4 address.

   The DNS64 server responds with an IPv4-embedded IPv6 address.

   Example:

   ```
   64:ff9b::c000:0201
   ```

   which uses the NAT64 well-known prefix (WKP), `64:FF9B::/96`. The WKP is used for algorithmic mapping between address families.

   An IPv4-embedded IPv6 address is comprised of a variable length prefix, an embedded IPv4 address, and a variable length suffix. The last 32 bits are the hexadecimal representation of the original IPv4 address, which is 192.0.2.1 in this example.
3. The IPv6 client now tries to connect to the IPv4 server.
4. An IPv6 to IPv4 translation is performed.

   A source IPv6 address is translated to one of the available IPv4 addresses in the pool.

   A destination IPv6 address is translated to the server's actual IPv4 address since the destination IPv6 address is an IPv4-embedded IPv6 address.

Benefits of NAT64

- Provides translation of IPv6 to IPv4 addresses for maintaining dual access to IPv6 and IPv4 networks
- Requires little or no changes to existing IPv4 network infrastructures when using stateful NAT64
- Seamless internet experience for IPv6 users accessing IPv4 internet services, thus maintaining IPv4 business continuity
- Supports configuration of NAT64 without having to configure a data policy

Use Cases for NAT64

Supported traffic flow is from the IPv6 client on the remote site, in the data center, or in another branch site, to the IPv4 client or server on the local LAN behind VM5, as shown in the diagram.

Note Traffic origination is always from the transport-side (WAN) to the service-side (LAN) in the overlay network.

Configure NAT64

Use the procedures in the following sections for enabling and configuring NAT64.

Enable NAT64 Using a Device Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device**.
3. Click **Create Template**.
4. From the **Create Template** drop-down list, choose **From Feature Template**.
5. Choose a Cisco IOS XE SD-WAN device.
6. Choose a **Device Role**.
7. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
8. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
9. To create a template for VPN 0 or VPN 512:
   a. Click **Transport & Management VPN** located directly beneath the **Description** field, or scroll to the **Transport & Management VPN** section.
   b. From the **Cisco VPN 0** or **Cisco VPN 512** drop-down list, click **Create Template**.

      The **Cisco VPN** template form appears. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN parameters.
   c. In the **Cisco VPN Interface Ethernet** template, click **NAT**, and choose **IPv6**.
   d. Change the scope from **Default** to **Global**.
   e. Click **On** to enable NAT64.

      The correct set of parameters appears.
   f. Enter the parameter values.
   g. To save the feature template, click **Save**.
10. To create a template for VPNs 1 through 511, and 513 through 65527:
    a. Click **Service VPN**.
    b. Click **Add VPN**.
    c. From the **Add VPN** window, click **Create Template**.

       The **Cisco VPN** template form displays. The top of the form contains fields for naming the template, and the bottom contains fields for defining VPN parameters.

11. To save the feature template, click **Save**.

Enable NAT64 Using a Feature Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature**.
3. Click **Add Template**.
4. Choose a Cisco IOS XE SD-WAN device.
5. Click the **Cisco VPN Interface Ethernet** template.

Note The **Cisco VPN Interface Ethernet** template is a transport-side interface.

6. In the **Template Name** field, enter a name for the template.
   The name can be up to 128 characters and can contain only alphanumeric characters.
7. In the **Template Description** field, enter a description of the template.
   The description can be up to 2048 characters and can contain only alphanumeric characters.
8. Click **Basic Configuration** and choose an interface.
9. Click **NAT** and choose **IPv6** for NAT64.
10. Change the scope from **Default** to **Global**.
11. Click **On** to enable NAT64.
12. To save the feature template, click **Save**.

Configure a NAT64 Pool

Before You Begin

1. You must have enabled NAT64 prior to configuring a NAT64 IPv4 pool.
2. Configure a feature template.

Configure a NAT64 Pool

1. Click **Cisco VPN**.
2. In the **Template Name** field, enter a name for the template.
   The name can be up to 128 characters and can contain only alphanumeric characters.
3. In the **Template Description** field, enter a description of the template.
   The description can be up to 2048 characters and can contain only alphanumeric characters.

4. Click **NAT64 v4 Pool**.
5. Click **New NAT64 v4 Pool**.
6. In the **NAT64 Pool name** field, specify the pool name.

Note You have to specify a number for the pool name.

7. In the **NAT 64 v4 Pool Range Start** field, specify the IPv4 address for the start of the pool range.
8. In the **NAT 64 v4 Pool End Start** field, specify the IPv4 address for the end of the pool range.
9. From the drop-down list, choose **Global**.
10. Click **On** to enable **NAT 64 Overload**.

Note **NAT 64 Overload** is set to **Off** by default.

11. Click **Add**.
12. Click **Update** to push the configuration to the device.

Configure NAT64 Using the CLI

Enable NAT64 Using the CLI

This section provides an example CLI configuration for enabling NAT64.

Enable NAT64 on the LAN interface, which is equivalent to the **Service VPN** template on Cisco vManage.

The IPv4 application server is on the local LAN site and the IPv6 client is in the data center or on the remote site of the LAN.

```
Device# interface GigabitEthernet 5.104
nat64 enable
```

Configure a NAT64 Pool Using the CLI

This section provides an example CLI configuration for configuring a service-side NAT64 pool.

```
Device# nat64 v4 pool pool10 10.1.1.10 10.1.1.100
nat64 v6v4 list global-list_nat64 pool pool10 vrf 4 overload
```

Verify Configuration of NAT64

Example - What Displays in the Routing Table for the Specified Device

The following is a sample output from the **show ipv6 route vrf** command:

```
Device# show ipv6 route vrf 4
IPv6 Routing Table - 4 - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP, Nd - Nat-Route DIA
S   64:FF9B::/96 [1/0]
     via ::10.1.1.2%default, NVI0%default
```

In this example, the NAT64 well-known prefix, `64:FF9B::/96`, displays in the IPv6 routing table of a service VPN.

The following is a sample output from the **show ip route vrf 4** command:

```
Device# show ip route vrf 4

Routing Table: 4
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set
```

The NAT64 IPv4 pool address is installed in the routing table as `nat inside route` in the IPv4 routing table of a service VPN.

Example - What Displays in the Routing Table on OMP

The following is a sample output from the **show ipv6 route vrf** command:

```
Device# show ipv6 route vrf 4
IPv6 Routing Table - 4 - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP
m   64:FF9B::/96 [251/0]
     via 172.16.255.15%default, Sdwan-system-intf%default
```

In this example, the NAT64 well-known prefix, `64:FF9B::/96`, is received as an OMP route.

The NAT64 IPv4 pool addresses are received as an OMP route.

Configuration Examples for NAT64

This example shows the configuration of NAT64.

```
nat64 v4 pool 1-4 10.1.1.1 10.1.1.10
nat64 v6v4 list nat64-list pool 1-4 vrf 4 overload
!
interface GigabitEthernet5.104
 encapsulation dot1Q 104
 vrf forwarding 4
 ip address 10.1.19.15 10.255.255.255
 ip mtu 1496
 ip ospf network broadcast
 ip ospf 4 area 0
 nat64 enable
end
```

This example shows the configuration of a NAT64 pool.

```
nat64 v4 pool 1-4 10.1.1.1 10.1.1.10
nat64 v6v4 list nat64-list pool 1-4 vrf 4 overload
!
interface GigabitEthernet5.104
 encapsulation dot1Q 104
 vrf forwarding 4
 ip address 10.1.19.15 10.255.255.255
 ip mtu 1496
 ip ospf network broadcast
 ip ospf 4 area 0
 nat64 enable
end
```

NAT64 Direct Internet Access

Restrictions for NAT64 DIA

- NAT64 DIA uses interface overload only and works only with NAT DIA interface overload.
- NAT DIA pool or loopback is not supported for NAT64.
- NAT DIA is not supported for NAT64.
- You can use the following NAT64 DIA routes for installing routes in the routing table:
  - Example of a NAT64 DIA route for a /128 prefix:

    ```
    nat64 route vrf 4 64:FF9B::1E00:102/128 global
    ```

  - Example of a NAT64 DIA route for a /96 NAT64 prefix:

    ```
    nat64 route vrf 4 64:FF9B::/96 global
    ```

- You cannot use the following NAT64 DIA route configurations for installing routes in the routing table:
  - `nat64 route vrf 4 64:ff9b::/64 global`

- `nat64 route vrf 4 ::0/0 global`

Information About NAT64 Direct Internet Access

Cisco SD-WAN NAT64 Direct Internet Access (DIA) supports routing of traffic from branch sites directly to the internet instead of tunneling the internet traffic to a central site or data center for internet access.

The traffic flow for NAT64 DIA is from the LAN to DIA.

Workflow for Enabling NAT64 DIA

1. Enable NAT64 using a **Cisco VPN Interface Ethernet** template for both IPv4 and IPv6.

Note NAT64 IPv4 DIA uses interface overload by default.

A **Cisco VPN Interface Ethernet** template is a transport interface.

2. Configure a NAT64 DIA IPv6 route using a **Cisco VPN** template.

Benefits of NAT64 DIA

- Better application performance
- Reduced bandwidth consumption and latency
- Lower bandwidth cost
- Improved branch office user experience by providing DIA at remote site locations

Configure NAT64 DIA

Before You Begin

Configure a feature template.

Configure NAT64 DIA with Interface Overload

1. Click **Cisco VPN Interface Ethernet**.

Note The **Cisco VPN Interface Ethernet** template is a transport-side interface.

2. In the **Template Name** field, enter a name for the template.

   The name can be up to 128 characters and can contain only alphanumeric characters.

3. In the **Template Description** field, enter a description of the template.

   The description can be up to 2048 characters and can contain only alphanumeric characters.

4. Click **Basic Configuration** and choose an interface.
5. Click **NAT** and choose **IPv4**.
6. Change the scope from **Default** to **Global**.
7. Click **On** to enable NAT64 for IPv4.
8. Repeat the process for IPv6.

Note Configure both IPv4 and IPv6 for NAT64 DIA.

9. In the **NAT Type** field, click **Interface** for interface overload.

   Table 2: NAT Interface Overload Parameters

Parameter Name	Description
NAT	Specify if NAT translation is used. The default is **Off**.
NAT Type	Specify the NAT translation type. The default is the **Interface** option. The **Interface** option is supported for NAT64.
UDP Timeout	Specify when NAT translations over UDP sessions time out. Range: 1 through 65536 minutes Default: 1 minutes
TCP Timeout	Specify when NAT translations over TCP sessions time out. Range: 1 through 65536 minutes Default: 60 minutes (1 hour)

10. Click **Save** if you are creating a new template or **Update** if you are editing an existing template.

Configure a NAT64 DIA Route

Before You Begin

Configure a feature template using a Cisco IOS XE SD-WAN device.

Configure a NAT64 DIA Route Using a Cisco VPN Template

1. Click **Cisco VPN** as the template.

Note You configure an IPv6 DIA route in a **Cisco VPN** template, which is the service VPN.

2. Click **IPv6 Route**.
3. Click **New IPv6 Route**.
4. In the **Prefix** field, enter the well-known prefix, `64:FF9B::/96`.
5. In the **Gateway** field, click **VPN**.
6. In the **Enable VPN** field, change the scope from **Default** to **Global**, and click **On** to enable VPN.
7. Click **Add**.

Configure a NAT64 DIA Route Using the CLI

Example: Configure a NAT64 DIA Route

```
nat64 route vrf 4 64:FF9B::1E00:102/128 global
```

Verify NAT64 DIA Route Configuration

Example 1

The following is a sample output from the **show ipv6 route vrf** command:

```
Device# show ipv6 route vrf 4
IPv6 Routing Table - 4 - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP
m   64:FF9B::/96 [251/0]
     via 172.16.255.15%default, Sdwan-system-intf%default
```

In this example, `64:FF9B::/96`, is the NAT64 well-known prefix for translating IPv6 to IPv4 addresses.

Example 2

Because NAT64 DIA is configured in the transport VPN, the routing table in the transport VPN appears as the following:

```
Device# show ipv6 route
IPv6 Routing Table - default - 2 entries
```

```
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP, Nd - Nat-Route DIA
S   64:FF9B::/96 [1/0]
```

Configuration Example for NAT64

This example shows the end-to-end configuration for NAT64 DIA.

```
interface GigabitEthernet1
          no shutdown
          arp timeout 1200
          ip address 10.1.15.15 10.255.255.255
          no ip redirects
          ip mtu    1500
          ip nat outside
          load-interval 30
          mtu           1500
          negotiation auto
          nat64 enable
          !
          nat64 v6v4 list nat64-global-list interface GigabitEthernet1 overload
          !
          ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1
 overload
```

GigabitEthernet 1 and 4 are transport VPN interfaces.

Advertise NAT64 Routes Through OMP

When NAT64 DIA advertisement is configured on any designated Cisco SD-WAN site on the network, Overlay Management Protocol (OMP) advertises the NAT64 default route to the branches. The branches receive the default route and use it to reach the hub for all DIA traffic. The Cisco SD-WAN site acts as the internet gateway for all DIA traffic.

For more information, see the *NAT on Cisco IOS XE SD-WAN Devices* chapter.

Note By default, NAT64 IPv4 pool addresses and the NAT64 well-known prefix are received as an OMP route.