Configure NAT66

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Configure NAT66

Table 1: Feature History

Feature Name	Release Information	Description
Support for NAT66 DIA	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	The IPv6-to-IPv6 Network Address Translation (NAT66) Direct Internet Access (DIA) feature enables an IPv6 device to translate an inside source address prefix to an outside source address prefix in IPv6 packet headers. NAT66 DIA allows you to direct local IPv6 internet traffic to exit directly to the internet from the service-side VPN (VPN 1) through the transport VPN (VPN 0). You can configure NAT66 DIA using Cisco SD-WAN Manager, the CLI, or a device CLI template. This feature introduces new CLI commands. For more information on the new NAT commands, see the Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide.
Support for Multiple WAN Links for NAT66 DIA	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	You can configure NAT66 to use multiple WAN links to direct local IPv6 traffic to exit directly to the internet.
Automatically Configure IPv6 Address on a WAN Interface by Using SLAAC	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	You can configure the Stateless Address Autoconfiguration (SLAAC) by using the Router Advertisement (RA) prefix to automatically assign IPv6 addresses for NAT66 prefix translations.
Support for Flow Stickiness	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	Flow stickiness records the flow level state of the NAT path and ensures that the application flows don't get reset due to a change in the NAT path. When the first packet match fails in deep packet inspection (DPI), the edge router ensures the first flow for this unknown application to stick to the original path, bypassing the policy to change the path when it is recognized by the DPI engine a few packets later.

Feature Name	Release Information	Description
Support for Centralized Data Policy for NAT66 DIA	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	You can configure the centralized data policy by using the **nat use-vpn 0** command, which ensures that matching traffic is sent to VPN 0 after the source IP is translated, based on the policy match criteria. This feature is supported from service and from tunnel. The fallback option ensures that the traffic falls back to routing and takes the overlay path when the DIA route is not available.
Support for Redistribution of NAT66 DIA Routes	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	You can configure the redistribution of NAT66 DIA routes into BGP or OSPFv3 protocols.
Support for Point-to-Point Protocol (PPP) Dialer Interfaces with NAT66 DIA	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature adds support for two types of PPP dialer interfaces—PPP over Ethernet (PPPoE) and PPP over Asynchronous Transfer Mode (PPPoA). With this feature, you can configure PPP dialer interfaces for accessing IPv6 services and sites.

Information About NAT66 DIA

IPv6-IPv6 Network Prefix Translation (NPTv6) is a mechanism that converts an IPv6 address prefix to another IPv6 address prefix. The address translation method that is used is IPv6-IPv6 Network Address Translation (NAT66). A device that supports a NAT66 function is known as a NAT66 translator. A NAT66 translator provides source and destination address translation capability.

Note NPTv6 functionality was already available on Cisco IOS XE platforms before it was introduced in Cisco Catalyst SD-WAN in the Cisco IOS XE Catalyst SD-WAN Release 17.7.1a. For more information, see the *IP Addressing: NAT Configuration Guide*.

NAT66 DIA allows you to redirect or forward packets from one network to another in an IPv6 environment. NAT66 DIA provides an algorithmic translation function with a 1:1 relationship between addresses within the inside network and the outside network. You can interconnect different networks and support multihoming, load balancing, and peer-to-peer networking.

NAT66 DIA supports prefixes longer than 64 bits and static IPv6 host-to-host translations. Only the prefix portion of an IPv6 address is translated.

Note To access Cisco SD-WAN Manager using an IPv6 address, specify port number 8443 in the URL.

Example:

```
https://[cisco-vmanage IPv6-address]:8443/
```

NAT66 DIA Flow Stickiness

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a.

When NAT66 DIA is configured with centralized data policy with application match, the application flows subject to NAT66 DIA policy may get reset due to path change. For example, when you have a data policy matching an application list and the action is NAT66 DIA, the first few packets may not be identified by deep packet inspection (DPI). So, the packets not matching NAT66 DIA application policy follow routing to the Cisco Catalyst SD-WAN overlay path. When the flow is identified, the later packets of the flow take the NAT66 DIA path as defined by the data policy. This path change results in a flow reset as different paths means different client source or port combination towards the server and the server resets the unknown TCP flows.

The NAT66 DIA flow stickiness feature records the flow level state of the NAT66 path. If the first packet of the flow is non-NAT66, it keeps the rest of the packets of this flow to non-NAT66 paths. If the first packet flow is via the NAT66 DIA path, it keeps the rest of the packets of this flow to the NAT66 DIA path. It is enabled by default with the NAT66 DIA data policy.

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the NAT66 DIA flow stickiness feature is enabled by default. To disable flow stickiness, use the command **flow-stickiness-disable** under the localized policy using the CLI add-on template.

How NAT66 DIA Works

1. An IPv6 client in a branch site attempts to access Cisco SD-WAN Manager in a data center on the transport side of the network (VPN 0).
2. The Cisco IOS XE Catalyst SD-WAN device routes the IPv6 address from the service VPN (VPN 1) to the next-hop transport VPN (VPN 0), which is the WAN side of the network.
3. A NAT66 translator performs an IPv6-to-IPv6 prefix translation. Dynamic Host Configuration Protocol version 6 (DHCPv6) requires a source IPv6 prefix in the IPv6 prefix range for prefix delegation.

   NAT66 conversion occurs in the transport VPN interface.

   DHCPv6 prefix delegation allows an ISP to automate the process of assigning prefixes to a customer for use within the customer's network. Prefix delegation occurs between a provider edge (PE) device and customer premises equipment (CPE) using the DHCPv6 prefix delegation option. After an ISP has delegated prefixes to a customer, the customer can further divide the network and assign prefixes to the links in the customer's network.
4. When traffic is returned from Cisco SD-WAN Manager, the Cisco IOS XE Catalyst SD-WAN device looks up the NAT66 entry in the DIA route table and forwards the packet to the client's IPv6 address.

Configure NAT66 DIA Using Stateless DHCP

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can autoconfigure an IPv6 address on a WAN interface by using Stateless Address Autoconfiguration (SLAAC) with a Router Advertisement (RA) prefix. Stateless DHCPv6 is a combination of SLAAC and DHCPv6. The device sends an RA with the O bit set but does not set the M bit. This is known as Stateless DHCPv6 because the DHCPv6 server does not have to track the client address bindings. The RA prefix is available for use with NAT66 for IPv6 DIA of the service side traffic. Once configured, the same source prefix can be matched with different outside interfaces.

Before you begin, ensure that you have configured DHCPv6 and SLAAC. For more information, see *Information About DHCPv6*.

Note Ensure that the RA prefix that are used in the SLAAC interface is different from the outside prefix that is used in the static NAT66 mapping rules.

When the mapping rule is configured and the flow match occurs, traffic flows from inside to outside. NAT66 maintains a bind table for sharing the RA prefix with service side hosts. When an IPv6 packet from the service side interface flows through the DIA path, a bind is created for the original source and the translated source address using the RA prefix. The same bind is used to translate back the packets. NAT66 maintains the bind entries for a specified time. The default timeout value is 5 minutes.

The prefix translation rule for an interface is effective only when the packet goes through that interface and there is no need to specify the egress interface when you've configured the prefix translation rule with RA.

When you configure the Translated Source Prefix as the system default, the SLAAC feature automatically provides the RA prefix (outside). Otherwise, you must configure the outside prefix in the translation rule.

You can configure NAT66 DIA Using Stateless DHCP by using the Cisco Catalyst SD-WAN Manager or the CLI:

- Configure NAT66 DIA Using Stateless DHCP Through Cisco Catalyst SD-WAN Manager
- Configure DIA Using Stateless DHCP using CLI

NAT66 DIA With Centralized Data Policy

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1

You can use the **nat use-vpn 0** command to configure a NAT66 DIA route using a centralized data policy on Cisco IOS XE Catalyst SD-WAN devices so that data traffic is NATed before entering the overlay tunnel that is located in the transport VPN. Based on the policy match criteria, matching IPv6 traffic is forwarded via DIA circuits after the source IP address is translated. The IPv6 traffic is forwarded after NAT66 on destination address via DIA circuits based on the centralized policy match criteria on source IPv6 prefix, prefix lists, or destination IPv6 prefix or Prefix-lists.

To configure NAT66 on the service-side of a device, you configure a NAT66 interface within a service VPN on the device, and then you configure a centralized data policy on the Cisco Catalyst SD-WAN Controller. The policy directs data traffic with the desired prefixes to the service-side NAT.

You can configure NAT for data that enters or exits the service-side of the network. The service-side NAT translates data traffic, of inside and outside host addresses, that match a configured centralized data policy.

If the DIA route is not available, traffic will drop if a fallback option is not configured. The NAT66 fallback feature provides a routing-based mechanism for all traffic that is sent to the DIA route to use an alternative route when required.This feature is supported this froms both service and from tunnel.

Configure NAT66 DIA Through Data Policy on Cisco SD-WAN Controller Using CLI

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Configure NAT66 DIA using CLI

Here is the complete configuration example to configure NAT66 DIA Through Data Policy on Cisco SD-WAN Controller:

```
Device# policy
 data-policy policy-name
 vpn-list vpn_list
 sequence number
 match
 source-ipv6 ipv6-address
 !
 action accept
 nat use-vpn 0
 nat fallback
 set
 local-tloc-color lte
```

Configure NAT66 DIA Through Data Policy Using Cisco Catalyst SD-WAN Manager

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1.

You can use the centralized data policy to configure IPv6 match and action conditions for NAT66 DIA along with fallback in Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. From the **Custom** options drop-down, under **Centralized Policy**, select **Traffic Data**.
3. From the **Add Policy** drop-down, click **Create New**.
4. Click **Sequence Type** and select **Custom**.
5. Click **(+) Sequence Rule** to create a new sequence rule.
6. Choose **IPv6** from the **Protocol** drop-down list.
7. After adding match conditions, click **Actions** and click **Accept**.
8. Click **NAT VPN** and select the **Fallback** checkbox.
9. Click **Save and Match Actions**.
10. Click **Save Data Policy**.

To enable NAT fallback using Cisco SD-WAN Manager, create and configure a data policy by doing the following:

- Edit the existing centralized policy and import the policy:
  1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
  2. From the **Custom** options drop-down, under **Centralized Policy**, select **Traffic Data**.
  3. From the **Add Policy** drop-down, click **Create New**.
  4. Click **Sequence Type** and select **Custom**.
  5. Click **(+) Sequence Rule** to create a new sequence rule.
  6. After adding match conditions, click **Actions** and click **Accept**.

7. Click **NAT VPN** and select the **Fallback** checkbox.
8. Click **Save and Match Actions**.
9. Click **Save Data Policy**.

Configure NAT66 DIA Through Data Policy Using Policy Groups

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can use configuration groups to configure NAT66 DIA by using stateless DHCP in Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups**.
2. Click **Application priority & SLA policy** to create a policy.

   To edit an existing policy, click the ellipsis icon (**...**) next to the application priority and SLA policy under **Action** and click **Edit**
3. Under **Internet Offload Traffic**, configure direct internet access by choosing an application from the **Application List** drop-down list and toggle on the **Fallback to Routing** option.
4. Under **Apply Policy**, configure the direction, VPN, and interface.
5. Click **Save**.

Benefits of NAT66 DIA

- Supports local IPv6 internet traffic to exit directly to the internet from the service-side VPN through the transport VPN
- Allows you to redirect or forward packets from one network to another in an IPv6 environment
- Enables good application performance
- Contributes to reduced bandwidth consumption and latency
- Contributes to lower bandwidth cost
- Enables improved branch office user experience by providing DIA at remote site locations
- Supports cellular and dialer interfaces from Cisco IOS XE Catalyst SD-WAN Release 17.14.x

Restrictions for NAT66 DIA

- Firewall, AppNav-XE, and multicast are not supported.

  From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, NAT66 supports the use of a firewall.
- Only NAT66 DIA traffic flows are supported. There is no support for service-side traffic flows.
- Centralized data policy is not supported for NAT66 DIA.

  From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Centralized data policy is supported for NAT66 DIA.
- Combined NAT64 and NAT66 is not supported on the same interface.

- Only one single prefix translation is supported for each VRF.

  From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, multiple prefix translations are supported for each VRF.

- Use of multiple WAN links for NAT66 DIA is not supported.

  From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, multiple WAN links are supported for NAT66 DIA.

- NAT66 DIA route redistribution using the service IPv6 routing protocol is not supported.

  From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can configure NAT66 DIA route redistribution into BGP or OSPFv3 protocols.

- Real-time operational application programming interface (APIs) are not supported.
- You must include a default route in VPN 0 for successful NAT66 DIA route operations.
- Only physical Ethernet subinterfaces are supported.
- Router Advertisement (RA) prefix is not supported in NAT66 prefix translations.
- Multitenancy resource limits are not supported.
- IPv6 TLOC extension with NAT66 is not supported.

Configure NAT66 DIA and a DIA Route

Workflow for Enabling NAT66 DIA and a NAT66 DIA Route

1. Enable NAT66 DIA using a **Cisco VPN Interface Ethernet** feature template for IPv6.

   A **Cisco VPN Interface Ethernet** template is used as a transport (WAN) interface.

   For more information on enabling NAT66 DIA using a **Cisco VPN Interface Ethernet** template, see Configure NAT66 DIA.

2. Configure a NAT66 DIA IPv6 route using a **Cisco VPN** feature template, which is a service-side VPN (VPNs other than VPN 0).

   For more information on configuring a NAT66 DIA IPv6 route, see Configure a NAT66 DIA Route.

Configure NAT66 DIA

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x release, **Feature Templates** is titled **Feature**.

3. Edit a **Cisco VPN Interface Ethernet** template by clicking **. . .** adjacent to it, and then choosing **Edit**.

4. Click **NAT** and choose **IPv6**.
5. In the **NAT** drop-down list, change the scope from **Default** to **Global**.

   Click **On** to enable NAT66.
6. In the **NAT Selection** field, choose **NAT66**.
7. Click **New Static NAT**.
8. In the **Source Prefix** field, specify the source IPv6 prefix.
9. In the **Translated Source Prefix** field, specify the translated source prefix.
10. In the **Source VPN ID** field, specify the source VPN ID.
11. Click **Update**.

Enable DHCPv6 Prefix Delegation Using a CLI Add-On Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Click **Add Template**.
4. Under **Select Devices**, choose the device for which you are creating the template.
5. Under **Select Template**, scroll down to the **OTHER TEMPLATES** section, and click **CLI Add-On Template**.
6. In the **Template Name** field, enter a name for the feature template.
7. In the **Description** field, enter a description for the feature template.
8. In the **CLI CONFIGURATION** area, enter the DHCPv6 configuration.

   ```
   interface GigabitEthernet1
   ipv6 dhcp client pd prefix-from-provider
   ipv6 dhcp client request vendor
   ```
9. Click **Save**.

   The CLI add-on template is displayed in the **CLI CONFIGURATION** table.
10. To use the CLI add-on feature template, edit the device template as follows:
    a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
    b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

    c. Click **...** adjacent to the device template for which you want to add the CLI add-on feature template, and choose **Edit**.
    d. Scroll down to **Additional Templates**, and from the **CLI Add-On Template** drop-down list, choose the CLI add-on feature template that you previously created.

e. Click **Update**.

Configure a NAT66 DIA Route

Enable an IPv6 route with NAT66 DIA in a **Cisco VPN** template.

Every service VPN, for example, VPN 1, routes packets into the transport VPN (VPN 0) for DIA traffic.

Configure a NAT66 DIA Route Using a Cisco VPN Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x release, **Feature Templates** is titled **Feature**.

3. Edit a **Cisco VPN** template by clicking **. . .** adjacent to it, and then choosing **Edit**.
4. Click **IPv6 Route**.
5. Click **New IPv6 Route**.
6. In the **Prefix** field, enter an IPv6 prefix for NAT66 translation.

   Global inside and outside prefixes should be unique per virtual routing and forwarding (VRF).

   IPv6-prefix delegation (PD) prefix length should be equal to or less than /56.

   A global outside prefix should be unique per VRF.

   The inside prefix length and an outside prefix length should be the same.

   Up to 250 VRFs are supported with a PD prefix of /56.
7. In the **Gateway** field, click **VPN**.
8. In the **Enable VPN** drop-down list, change the scope from **Default** to **Global**, and click **On** to enable VPN.
9. In the **NAT** drop-down list, change the scope from **Default** to **Global**, and click **On** to enable NAT66.
10. Click **Update**.

Configure NAT66 DIA Using Stateless DHCP Through Cisco Catalyst SD-WAN Manager

From Cisco Catalyst SD-WAN Manager Release 20.13.1, you can use configuration groups to configure NAT66 DIA by using stateless DHCP in Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **Add Configuration Group** to create a new configuration group or click **Edit** under **Actions** to edit an existing configuration group.

3. To edit a configuration group, click **. . .** adjacent to it, and then choose **Edit**.
4. Click **Transport Profile**.
5. Click **. . .** adjacent to the VPN feature and choose **Add Sub-Feature**.
6. Select Ethernet Interface from the drop-down list.
7. Click **NAT** > **IPv6 Settings**.
8. In the **NAT** drop-down list, change the scope from **Default** to **Global**, and toggle on NAT66.
9. Under the **NAT66** option, click **Add Nat66** and configure the **Source Prefix** and **Source VPN ID**.
10. Leave the system default value in the **Translated Source** field.
11. In the **Egress Interface** drop-down list, change the scope from **Default** to **Global**, and toggle on egress interface.
12. Click **Add**.
13. Click **Save**.

Configure NAT66 DIA Using Stateless DHCP Through a Feature Template

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can use feature templates to configure NAT66 DIA by using stateless DHCP in Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Click **Add Template**.
4. Under **Select Devices**, choose the device for which you are creating the template.
5. Under **Select Template**, scroll down to the **VPN** section, and click **Cisco VPN Interface Ethernet**
6. In the **Template Name** field, enter a name for the feature template.
7. In the **Description** field, enter a description for the feature template.
8. Click **NAT** > **IPv6**.
9. In the **NAT** drop-down list, change the scope from **Default** to **Global**.
10. Click **ON** to enable NAT.
11. In the **NAT Selection** drop-down list, change the scope from **Default** to **Global** and choose **NAT66**.
12. Click **New Static NAT**.
13. Configure the **Source Prefix** and **Source VPN ID**.
14. Leave the system default value in the **Translated Source Prefix** field.
15. In the **Egress Interface** drop-down list, change the scope from **Default** to **Global**, and click **Yes**.
16. Click **Add**.

17. Click **Save**.

Configure NAT66 DIA Using the CLI

Configure Static NAT Prefix Translation for NAT66 DIA

```
interface GigabitEthernet1
 ip address 10.1.15.15 255.0.0.0
 no ip redirects
 load-interval 30
 negotiation auto
 nat66 outside
 ipv6 address 2001:DB8:A1:F::F/64
 no ipv6 redirects
 service-policy output shape_GigabitEthernet1
!
nat66 prefix inside 2001:DB8:380:1::/80 outside 2001:DB8:A1:F:0:1::/80 vrf 1
nat66 prefix inside 2001:DB8:A14:18::/80 outside 2001:DB8:A1:F::/80 vrf 1
nat66 route vrf 1 2001:DB8:A14:19::/64 global
nat66 route vrf 1 2001:DB8:3D0:1::/64 global
```

Configure DIA Using Stateless DHCP using CLI

```
interface GigabitEthernet1
 nat66 outside
 ip address 10.1.15.15 255.0.0.0
 ipv6 address autoconfig
 ipv6 enable
 ipv6 nd autoconfig default-route
 no ip redirects
 load-interval 30
 negotiation auto
 no ipv6 redirects
 service-policy output shape_GigabitEthernet1
!
nat66 prefix inside 2001:a14:18::/64 outside interface GigabitEthernet1 vrf 1
nat66 prefix inside 2001:a14:18::/64 outside interface GigabitEthernet1
```

Configure multiple links for NAT66 DIA

From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, you can configure multiple egress interfaces for NAT66 DIA.

Here is an example of configuring 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
```

For more information, see the nat66 prefix command in the Cisco IOS XE SD-WAN Qualified Command Reference Guide.

Configure DHCPv6 Prefix Delegation for NAT66 DIA

```
interface GigabitEthernet1
ip address 10.1.15.15 255.0.0.0
no ip redirects
load-interval 30
negotiation auto
nat66 outside
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
ipv6 nd autoconfig default-route
ipv6 dhcp client pd prefix-from-provider
ipv6 dhcp client request vendor
arp timeout 1200
no mop enabled
no mop sysid
service-policy output shape_GigabitEthernet1
!
nat66 prefix inside 2001:DB8:10:1::/64 outside prefix-from-provider vrf 1
nat66 prefix inside 2001:DB8:100:1::/64 outside prefix-from-provider vrf 100
nat66 prefix inside 2001:DB8:101:1::/64 outside prefix-from-provider vrf 101
nat66 route vrf 1 2001:DB8:A14:19::/64 global
nat66 route vrf 1 2001:DB8:3D0:1::/64 global
nat66 route vrf 100 ::/0 global
nat66 route vrf 101 ::/0 global
```

Verify NAT66 DIA and DIA Route Configuration

Display NAT66 Prefix Translation Entries

```
Device# show nat66 prefix
Prefixes configured: 2
NAT66 Prefixes
Id: 1 Inside 2001:DB8:380:1::/80 Outside 2001:DB8:A1:F:0:1::/80
Id: 2 Inside 22001:DB8:A14:18::/80 Outside 2001:DB8:A1:F::/80
```

Verify NAT66 DIA Routes

```
Device# show nat66 route-dia
Total interface NAT66 DIA enabled count [1]
route add [1] addr [2001:DB8:A14:19::] vrfid [2] prefix len [64]
route add [1] addr [2001:DB8:3D0:1::] vrfid [2] prefix len [64]
```

Display NAT66 Neighbor Discovery

```
Device# show nat66 nd
NAT66 Neighbor Discovery

ND prefix DB:
  2001:DB8:A1:F::/80
  2001:DB8:A1:F:0:1::/80
  2001:DB8:A1:F:1::/64
  2001:DB8:A1:F:2::/64
  2001:DB8:A1:F:3::/64

ipv6 ND entries:
  2001:DB8:A1:F::F
  2001:DB8:A1:F::11
```

Verify NAT66 Global Statistics for Translated Packets

```
Device# show nat66 statistics
NAT66 Statistics

Global Stats:
   Packets translated (In -> Out)
      : 7
   Packets translated (Out -> In)
      : 7
```

Verify NAT66 DIA Using Stateless DHCP

To view the binding entry:

```
Device# show platform hardware qfp active feature nat66 datapath bind-dump
bind 0xdf612cc0 v6outaddr 2001:A1:F::96 v6addr 2001:A14:18::96 vrfid 3 domain 0 create time
 513092 refcnt 0 flags 0x0 mapping 0xdf54ba40 last_use_ts 513186 output_ifhandle 0x1b
```

Display NAT66 Platform for Each Prefix Counter for Inside and Outside Translations

```
Device# show platform hardware qfp active feature nat66 datapath prefix
prefix hasht 0x89628400 max 2048 chunk 0x8c392bb0 hash_salt 719885386
NAT66 hash[1] id(1) len(64) vrf(0) in: 2001:db8:ab01:0000:0000:0000:0000:0000 out:
2001:db8:ab02:0000:0000:0000:0000:0000 in2out: 7 out2in: 7
```

Verify NAT66 Platform Global Counters

```
Device# show platform software nat66 fp active statistics
QFP Stats:
Interface:
    Add: 2, Ack: 2, Err: 0
    Mod: 0, Ack: 0, Err: 0
    Del: 0, Ack: 0, Err: 0
Prefix Trans:
    Add: 5, Ack: 5, Err: 0
    Mod: 0, Ack: 0, Err: 0
    Del: 0, Ack: 0, Err: 0
AOM Stats:
Interface:
    Add: 2, Err: 0
    Mod: 0, Err: 0
    Del: 0, Err: 0
    Free: 0, Err: 0
Prefix Translation:
    Add: 5, Err: 0
    Mod: 0, Err: 0
```

```
    Del: 0, Err: 0
    Free: 0, Err: 0
DB Stats:
  Interface:
    Add: 2, Err: 0
    Mod: 0, Err: 0
    Del: 0, Err: 0
  Prefix Translations:
    Add: 5, Err: 0
    Mod: 0, Err: 0
    Del: 0, Err: 0
Message RX Stats:
  Interface:
    Add: 2
```

Configuration Example for NAT66 DIA

The following is an end-to-end configuration example for NAT66 DIA:

```
interface GigabitEthernet1
ip address 10.1.15.15 255.0.0.0
no ip redirects
load-interval 30
negotiation auto
nat66 outside
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
ipv6 nd autoconfig default-route
ipv6 dhcp client pd prefix-from-provider
ipv6 dhcp client request vendor
arp timeout 1200
no mop enabled
no mop sysid
service-policy output shape_GigabitEthernet1
!
nat66 prefix inside 2001:DB8:380:1::/80 outside 2001:DB8:A1:F:1::/80 vrf 1
nat66 prefix inside 2001:DB8:A14:18::/80 outside 2001:DB8:A1:F::/80 vrf 1
nat66 prefix inside 2001:DB8:10:1::/64 outside prefix-from-provider vrf 1
nat66 prefix inside 2001:DB8:100:1::/64 outside prefix-from-provider vrf 100
nat66 prefix inside 2001:DB8:101:1::/64 outside prefix-from-provider vrf 101
nat66 route vrf 1 2001:DB8:A14:19::/64 global
nat66 route vrf 1 2001:DB8:3D0:1::/64 global
nat66 route vrf 100 ::/0 global
nat66 route vrf 101 ::/0 global
```

The following is an end-to-end configuration example with multiple links for NAT66 DIA:

```
interface GigabitEthernet3
 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
GigabitEthernet3
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
```

NAT66 DIA Route Redistribution

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

Route redistribution shares routing information between multiple domains running different routing protocols. When you configure NAT66 DIA route redistribution, you enable redistribution of the translated IPv6 addresses into Open Shortest Path First (OSPFv3) or the Border Gateway Protocol (BGP).

When the traffic from a remote site traverses the overlay network or tunnels, the NAT66 outside address translation service translates the remote host source IP address (outside host). The translation occurs before the traffic is sent to the LAN (VPN1) side of the network. If route redistribution is configured, the NAT outside pool address or routes are redistributed to the LAN side of the network through OSPFv3 or BGP protocols. Thus, the inside host from one network is aware of the path to reach remote hosts in another network running a different routing protocol.

NAT66 route redistribution applies to the following types of routes that it learns either locally or from its routing peers:

- BGP
- OSPFv3

You can configure NAT66 DIA route redistribution using CLI-based configuration groups or feature templates.

Configure NAT66 DIA Route Redistribution Using a Feature Template

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can use feature templates in Cisco SD-WAN Manager to configure NAT66 DIA route redistribution into BGP or OSPFv3 protocols.

Configure NAT66 DIA Route Redistribution into BGP Using a Feature Template

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Click **Add Template**.
4. Under **Select Devices**, choose the device for which you are creating the template.
5. Under **Select Template**, scroll down to the **OTHER TEMPLATES** section, and click **Cisco BGP**.

6. In the **Template Name** field, enter a name for the feature template.
7. In the **Description** field, enter a description for the feature template.
8. Click **UNICAST ADDRESS FAMILY**.
9. Click **IPv6**.
10. Click **New Redistribute**.
11. In the **Protocol** drop-down list, choose **NAT**.
12. Click **Add**.
13. Click **Save**.

Configure NAT66 DIA Route Redistribution into OSPFv3 Using a Feature Template

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Click **Add Template**.
4. Under **Select Devices**, choose the device for which you are creating the template.
5. Under **Select Template**, scroll down to the **OTHER TEMPLATES** section, and click **Cisco OSPFv3**.
6. In the **Template Name** field, enter a name for the feature template.
7. In the **Description** field, enter a description for the feature template.
8. Click **IPv6**.
9. In the **Redistribute** tab, click **New Redistribute**.
10. In the **Protocol** drop-down list, choose **nat-route**.
11. Click **Add**.
12. Click **Save**.

Configure NAT66 DIA Route Redistribution Using CLI Based Configuration Groups

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, you can use a CLI based configuration group in Cisco SD-WAN Manager to configure NAT66 DIA route redistribution into BGP or OSPFv3 protocols.

Configure NAT66 DIA Route Redistribution into BGP

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **Add CLI based Configuration Group**.

3. Enter a name for the CLI based configuration group.
4. In the **Solution** drop-down list, choose **sdwan**.
5. In the **Description** field, enter a description for the CLI based configuration group.
6. Click **Next**.
7. Enter the CLI based configuration in the field.

```
router bgp 15
bgp bestpath as-path multipath-relax
bgp log-neighbor-changes
bgp router-id 10.1.1.1
address-family ipv4 unicast vrf 1
  neighbor 10.2.2.2 remote-as 2
  neighbor 10.2.2.2 activate
  redistribute nat-route dia
  exit-address-family
!

address-family ipv6 unicast vrf 1
  bgp router-id 10.1.1.1
  neighbor 2001:a14:18::64 remote-as 2
  neighbor 2001:a14:18::64 activate
  redistribute nat-route
  exit-address-family
!
```

8. Click **Save**.

A new keyword, nat-route is added for redistributing NAT66 DIA routes into BGP protocol. For more information, see the **redistribute (IP)** section in Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide.

Configure NAT66 DIA Route Redistribution into OSPFv3

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Click **Add CLI based Configuration Group**.
3. Enter a name for the CLI based configuration group.
4. In the **Solution** drop-down list, choose **sdwan**.
5. In the **Description** field, enter a description for the CLI based configuration group.
6. Click **Next**.
7. Enter the CLI based configuration in the field.

```
interface GigabitEthernet5
ospfv3 1 network point-to-point
ospfv3 1 ipv4 area 0
ospfv3 1 ipv6 area 0

router ospfv3 1
max-lsa 50000
router-id 10.1.1.1
address-family ipv4 unicast vrf 1
  log-adjacency-changes
  redistribute connected
  exit-address-family
```

```
!

address-family ipv6 unicast
  log-adjacency-changes
  redistribute connected
  redistribute nat-route
  redistribute maximum-prefix 10240
  exit-address-family
!
```

8. Click **Save**.

A new keyword, nat-route is added for redistributing NAT66 DIA routes into OSPFv3 protocol.

Dialer Interfaces with NAT66 DIA

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

Information About Dialer Interface with NAT66 DIA

A dialer interface specifies how to handle dialer traffic from clients, including default routing information, the encapsulation protocol, and the dialer pool to use. Dialer interfaces provide an abstraction layer from the physical interfaces that actually perform the dial-up. This feature provides support for Point-to-Point Protocol (PPP) dialer interfaces for the NAT66 DIA. Use dialer interfaces to access IPv6 internet services and sites.

The following dialer interfaces are supported:

- Point-to-Point Protocol over Ethernet (PPPoE)
- Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA)
- Point-to-Point Protocol over Ethernet over Asynchronous Transfer Mode (PPPoEoA)

PPP connects multiple users over an ethernet local area network to a remote site through common customer premises equipment. PPP is commonly used in a broadband aggregation, such as by digital subscriber line (DSL). PPP provides authentication with the Challenge Handshake Authentication Protocol (CHAP) or password authentication protocol (PAP) while physical interfaces don't perform authentication.

For more information about configuring PPPoE, see the Configuring PPPoE section in the *Cisco Catalyst SD-WAN Systems and Interfaces Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

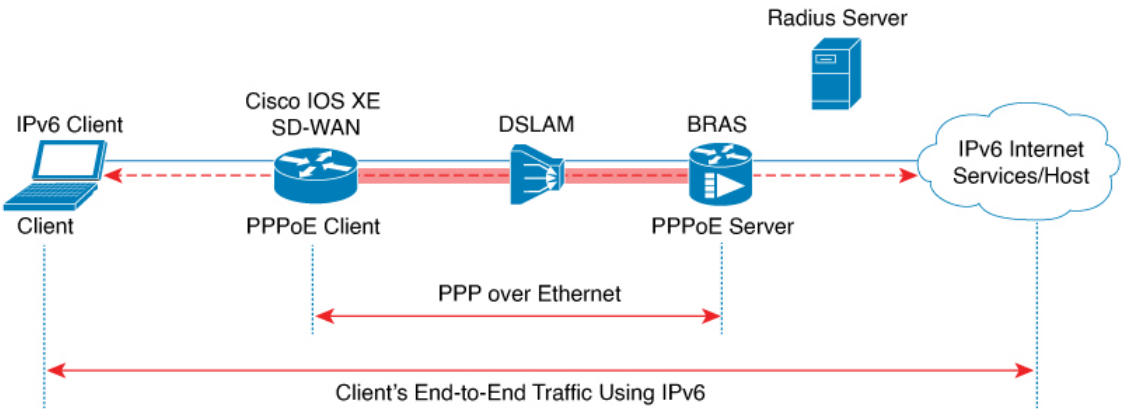
Benefits of Using a Dialer Interface with NAT66 DIA

- Allows physical interfaces to take on different characteristics based on incoming or outgoing call requirements
- Supports route-based as well as data-policy-based configuration with NAT66 DIA

Flow for IPv6 traffic through a NAT DIA Dialer Interface

The following diagram describes how IPv6 client traffic gets routed over a dialer interface for reaching IPv6 internet sites and services.

Figure 1: Workflow for NAT66 DIA Dialer Interface Support



Restrictions for Using a Dialer Interface with NAT66 DIA

- DIA support:

  Only NAT66 DIA is supported with dialer interfaces.

- Service-side NAT66:

  No support for service-side NAT66 with dialer interfaces.

- PPPoE jumbo frames:

  PPPoE jumbo frames are limited to 1800 bytes when using a CLI add-on template.

- PPPoA dialer interface encapsulations:

  There is no support for configuring the following PPPoA dialer interface encapsulations: AAL5MUX, AAL5SNAP, AAL5NLPID, or bridge-dot1q using Cisco SD-WAN Manager feature templates. If you want to configure these PPPoA encapsulations, you need to configure the encapsulations using a CLI template.

- DIA tracker:

  NAT66 DIA tracker is not supported for a dialer interface with an IP unnumbered interface.

- DIA path preference:

  NAT66 DIA path preference is not supported with loopback on a WAN interface.

Configure a Dialer Interface with NAT66 DIA

Minimum support release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

You can configure a dialer interface with NAT66 DIA using configuration groups or by using a CLI template.

Configure a Dialer Interface with NAT66 DIA Using Configuration Groups

Minimum support release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

   For more information about creating a configuration group, see Configuration Group Workflows.

2. Under **Transport and Management Profile**, click **…** adjacent to an interface under the VPN 0 feature.
3. Click **Add Sub Feature** and select the one of the following dialer interfaces from the drop-down list:
   - DSL PPPoE
   - DSL PPPoA
4. Configure the options for DSL PPPoE or DSL PPPoA.

   For more information, see the sections DSL PPPoE or DSL PPPoA in Transport and Management Profile.
5. Click **Save**.

Configure a Dialer Interface with NAT66 DIA Using a CLI Template

Minimum support release: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1

For more information on using CLI templates, see CLI Templates and CLI Add-On Feature Templates.

1. Configure a PPPoE dialer interface with NAT66 DIA enabled.

```
interface interface-type-number
 pppoe enable group global
 pppoe-client dial-pool-number dialer-pool-number
!
interface Dialer dialer-number
 mtu bytes
 ipv6 address negotiated
 ipv6 mtu bytes
 nat66 outside
 encapsulation encapsulation-type
 ipv6 tcp adjust-mss bytes
 dialer pool dialer-pool-number
 dialer down-with-vInterface
 ppp chap hostname hostname
 ppp chap password password
 ppp authentication chap callin
 ppp ipcp route default
 service-policy output shape_Dialer dialer-number
```

2. Enable **nat66 outside** over a dialer interface.

```
nat66 outside
nat66 prefix inside ipv6-address outside interface Dialer interface name vrf Sevice VPN
 number
nat66 prefix inside ipv6-address outside interface Dialer interface name
```

3. Configure a NAT66 DIA route for a service-side VPN.

For more information on configuring a NAT DIA route for a service-side VPN, see Configure a NAT DIA Route.

or

Configure a NAT66 DIA route for a service-side VPN using a centralized data policy.

nat66 route vrf *vrf-id route-prefix prefix-mask* global

Note Deleting the dialer interface in the same transaction as NAT66 Mapping with Pool-overload-config, generates an extra no NAT66 configuration. Remove each NAT66 configuration separately using different transactions as folllows:

```
Device(config)# no nat66 inside source list global-list pool natpool-Dialer100-0 overload
egress-interface Dialer100
Device(config)# commit

Device(config)# no interface Dialer100
Device(config)# commit
```

Here's an example of configuring a PPPoE dialer interface with NAT66 DIA:

```
interface Dialer100
 mtu 1492
 ipv6 address negotiated
 nat66 outside
 encapsulation ppp
 ipv6 tcp adjust-mss 1452
 dialer pool 100
 dialer down-with-vInterface
 endpoint-tracker tracker-google
 ppp authentication chap callin
 ppp chap hostname branch1.ppp1
 ppp chap password 7 01100F175804
 ppp ipcp route default
 service-policy output shape_GigabitEthernet0/0/1
!
interface GigabitEthernet0/0/1
 no ipv6 redirects
 pppoe enable group global
 pppoe-client dial-pool-number 100
!
sdwan
 interface Dialer100
  tunnel-interface
   encapsulation ipsec weight 1
   color mpls restrict
  exit
 exit
nat66 prefix inside 2001:A14:18::/80 outside interface Dialer100 vrf 100
nat66 route vrf 100 ::/0 global
```

Verify a Dialer Interface Configuration for NAT66 DIA

The following sections provide information on verifying a dialer interface configuration.

Verify NAT66 DIA Routes

```
Device# show nat66 route-dia
Total interface NAT66 DIA enabled count [1]
route add [1] addr [2001:A14:18::] vrfid [2] prefix len [64]
route add [1] addr [2001:A14:19::] vrfid [2] prefix len [64]
```

Display NAT66 Platform for Each Prefix Counter for Inside and Outside Translations

```
Device# show platform hardware qfp active feature nat66 datapath prefix
prefix hasht 0x89628400 max 2048 chunk 0x8c392bb0 hash_salt 719885386
NAT66 hash[1] id(1) len(64) vrf(0) in: 2001:0a14:0018:0000:0000:0000:0000:0000 out:
2001:db8:ab02:0000:0000:0000:0000:0000 in2out: 7 out2in: 7
```

Display Your PPPoE Sessions

In this sample output from the **show pppoe session** command, the PPPoE dialer interface displays as `UP`.

```
Device# show pppoe session
     1 client session

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st      Type
    N/A    391  84b2.61cc.9903  Gi0/0/1.100          Di100 Vi2        UP
                c884.a1f4.b981  VLAN: 100                  UP
```

The following is a sample output from the **show ppp all** command:

```
Device# show ppp all
Interface/ID OPEN+ Nego* Fail-     Stage    Peer Address    Peer Name
------------ -------------------- -------- --------------- --------------------
Vi2          LCP+ IPV6CP+ CDPCP-   LocalT   0.0.0.0         SDWAN-AGGREGE
```

Verify PPP Negotiation Information

In this sample output from the **show interfaces Dialer** command, `Dialer100` is up and the line protocol is up.

```
Device# show ipv6 interface Dialer100
Dialer100 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::72EA:1AFF:FE1E:C800
  No Virtual link-local address(es):
  Global unicast address(es):
2001:a0:14:0:8132:C37E:1172:A9C7, subnet is 2001:a0:14:0::/64
valid lifetime 2587577 preferred lifetime 600377
Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF78:5E00
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

Configuration Example for Using a Dialer Interface with NAT66 DIA

This example shows the configuration of a dialer interface.

Configure Static NAT Prefix Translation for NAT66 DIA

```
interface Dialer100
    nat66 outside
!
nat66 prefix inside 2001:DB8:380:1::/80 outside 2001:DB8:A1:F:0:1::/80 vrf 1
nat66 prefix inside 2001:DB8:A14:18::/80 outside 2001:DB8:A1:F::/80 vrf 1
nat66 route vrf 1 2001:DB8:A14:19::/64 global
nat66 route vrf 1 2001:DB8:3D0:1::/64 global
```

Configure DIA Using Stateless DHCP using CLI

```
interface Dialer100
     nat66 outside
!
nat66 prefix inside 2001:a14:18::/64 outside interface Dialer100 vrf 1
nat66 prefix inside 2001:a14:18::/64 outside interface Dialer100
```