Mapping of Address and Port Using Translation

The Mapping of Address and Port Using Translation feature provides connectivity to IPv4 hosts across IPv6 domains. Mapping of address and port using translation (MAP-T) is a mechanism that performs double translation (IPv4 to IPv6 and vice versa) on customer edge (CE) devices and border routers.

This module provides an overview of MAP-T and explains how to configure this feature.

Table 1: Feature Information

Feature Name	Releases	Feature Information
MAP-T BR enhancements	Cisco IOS XE 17.18.1a release	Improves the MAP-T Border Router functionality by supporting IPv4 packet transmission over IPv6 networks. Key improvements include enhanced support for fragmented ICMP packets and support for fragmented UDP packets with a checksum of 0, preventing their drop. This provides a more resilient solution for maintaining IPv4 connectivity during the transition to an all-IPv6 environment.

Restrictions for Mapping of Address and Port Using Translation

- In Cisco IOS XE Denali 16.2 release, the support for MAP-T domains were extended to 10000 domains. For releases prior to Cisco IOS XE Denali 16.2, a maximum of 128 MAP-T domains are supported.
- Forwarding mapping rule (FMR) is not supported.

Information About Mapping of Address and Port Using Translation

Mapping of Address and Port Using Translation Overview

The Mapping of Address and Port Using Translation feature provides connectivity to IPv4 hosts across IPv6 domains. Mapping of address and port using translation (MAP-T) builds on the existing stateless IPv4 and IPv6 address translation techniques that are specified in RFCs 6052, 6144, and 6145.

MAP-T is a mechanism that performs double translation (IPv4 to IPv6 and vice versa) on customer edge (CE) devices and border routers.

The Mapping of Address and Port Using Translation feature leverages the Network Address Translation 64 (NAT64) translation engine and adds the MAP-T border router function to the NAT64 stateless function. MAP-T is enabled on IPv4 and IPv6 interfaces. MAP-T uses IPv4 and IPv6 forwarding, IPv4 and IPv6 fragmentation functions, and NAT64 translation functions. A MAP-T domain is one or more MAP CE devices and a border router, all connected to the same IPv6 network.

A MAP-T CE device connects a user's private IPv4 address and the native IPv6 network to the IPv6-only MAP-T domain. The MAP-T border router uses the stateless IPv4/IPv6 translation to connect external IPv4 networks to all devices available in the one or more MAP-T domains. MAP-T requires only one IPv6 prefix per network and supports the regular IPv6 prefix/address assignment mechanisms. The MAP-T domain contains regular IPv6-only hosts or servers that have an IPv4-translatable IPv6 address. MAP-T does not require the operation of an IPv4 overlay network or the introduction of a non-native-IPv6 network device or server functionality.

A MAP-T configuration provides the following features:

- Retains the ability for IPv4 end hosts to communicate across the IPv6 domain with other IPv4 hosts.
- Permits both individual IPv4 address assignment and IPv4 address sharing with a predefined port range.
- Allows communication between IPv4-only and IPv6-enabled end hosts and native IPv6-only servers in domains that use IPv4-translatable IPv6 addresses.
- Allows the use of IPv6 native network operations, including the ability to classify IP traffic and perform IP traffic routing optimization policies such as routing optimization based on peering policies for IPv4 destinations outside the domain.

MAP-T Mapping Rules

Mapping rules define the mapping between an IPv4 prefix and an IPv4 address or between a shared IPv4 address and an IPv6 prefix/address. Each mapping of address and port using translation (MAP-T) domain uses a different mapping rule.

A MAP-T configuration has one basic mapping rule (BMR), one default mapping rule (DMR), and one or more forwarding mapping rules (FMRs) for each MAP-T domain. You must configure the DMR before configuring the BMR for a MAP-T domain.

The three types of mapping rules are described below:

- A BMR configures the MAP IPv6 address or prefix. The basic mapping rule is configured for the source address prefix. You can configure only one basic mapping rule per IPv6 prefix. The basic mapping rule is used by the MAP-T CE to configure itself with an IPv4 address, an IPv4 prefix, or a shared IPv4 address from an IPv6 prefix. The basic mapping rule can also be used for forwarding packets, where an IPv4 destination address and a destination port are mapped into an IPv6 address/prefix. Every MAP-T node (a CE device is a MAP-T node) must be provisioned with a basic mapping rule. You can use the **port-parameters** command to configure port parameters for the MAP-T BMR.
- A DMR is a mandatory rule that is used for mapping IPv4 information to IPv6 addresses for destinations outside a MAP-T domain. A 0.0.0.0/0 entry is automatically configured in the MAP rule table (MRT) for this rule.
- An FMR is used for forwarding packets. Each FMR results in an entry in the MRT for the rule IPv4 prefix. FMR is an optional rule for mapping IPv4 and IPv6 destinations within a MAP-T domain.

Note FMR is not supported by the Mapping of Address and Port Using Translation feature.

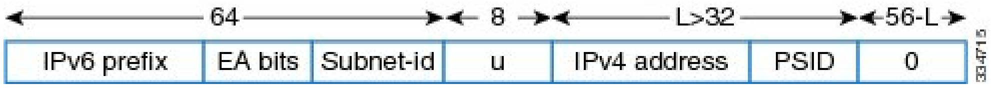
MAP-T Address Formats

The mapping of address and port using translation (MAP-T) customer edge (CE) device address format is defined by the IETF draft Mapping of Address and Port (MAP) . Address formats are used during mapping rule operations to construct the source and destination IPv6 addresses.

Note Forwarding mapping rule (FMR) is not supported by the Mapping of Address and Port Using Translation feature.

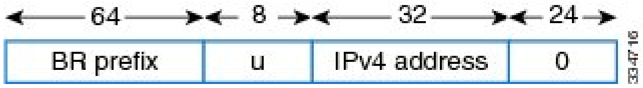
The figure below shows the mapped CE address format as defined in MAP-T configuration. This address format is used in basic mapping rule (BMR) and FMR operations.

Figure 1: IPv4-Translatable Address for BMR and FMR



The figure below shows the address format used by the MAP-T default mapping rule (DMR), an IPv4-translated address that specific to MAP-T configuration.

Figure 2: IPv4-Translated Address for DMR



Packet Forwarding in MAP-T Customer Edge Devices

Note The Mapping of Address and Port Using Translation feature does not support the MAP-T customer edge (CE) functionality. The CE functionality is provided by third-party devices.

IPv4-to-IPv6 Packet Forwarding

A mapping of address and port using translation (MAP-T) CE device that receives IPv4 packets performs Network Address Translation (NAT) and creates appropriate NAT stateful bindings. The resulting IPv4 packets contain the source IPv4 address and the source transport number defined by MAP-T. This IPv4 packet is forwarded to the CE's MAP-T, which performs IPv4-to-IPv6 stateless translation. IPv6 source and destination addresses are then derived by the MAP-T translation, and IPv4 headers are replaced with IPv6 headers.

IPv6-to-IPv4 Packet Forwarding

A MAP-T CE device that receives an IPv6 packet performs its regular IPv6 operations. Only the packets that are addressed to the basic mapping rule (BMR) address are sent to the CE's MAP-T. All other IPv6 traffic is forwarded based on the IPv6 routing rules on the CE device. The CE device checks if the transport-layer destination port number of the packets received from MAP-T is in the range that was configured and forwards packets that confirm to the port number. The CE device drops all nonconforming packets and responds with an Internet Control Message Protocol Version 6 (ICMPv6) "Address Unreachable" message.

Packet Forwarding in Border Routers

IPv4-to-IPv6 Packet Forwarding

An incoming IPv4 packet is processed by the IPv4 input interface, and the destination route lookup routes the IPv4 packet to the mapping of address and port using translation (MAP-T) virtual interface. The border router compares the packet against the IPv4 prefix lookup unit (PLU) tree to obtain the corresponding basic mapping rule (BMR), the default mapping rule (DMR), and the forwarding mapping rule (FMR). Based on the BMR or FMR rules, the border router constructs the IPv6 destination address by encoding the embedded address (EA) bits and adding a suffix. The IPv6 source address is constructed from the DMR rule.

After the IPv6 source and destination addresses are constructed, the packet uses the Network Address Translation 64 (NAT64) IPv4-to-IPv6 translation to construct the IPv6 packet. A routing lookup is done on the IPv6 packet, and the packet is forwarded to the IPv6 egress interface for processing and transmission.

IPv6-to-IPv4 Packet Forwarding

An incoming IPv6 packet is processed by the IPv6 input interface, and the destination route lookup routes the IPv6 packet to the MAP-T virtual interface. The software compares the packet against the IPv6 PLU tree to obtain the corresponding BMR, DMR, and FMR rules. The border router checks whether the port-set ID (PSID) and the port set match. If the port-set ID and port set match, the DMR rule matches the packet destination of the IPv6 packet. Based on the BMR and FMR, the border router constructs the IPv4 source address and extracts the IPv4 destination address from the IPv6 destination address. The IPv6 packet uses the NAT64 IPv6-to-IPv4 translation engine to construct the IPv4 packet from the IPv6 packet. A routing lookup is done on the IPv4 packet, and the IPv4 packet is forwarded to the IPv4 egress interface for processing and transmission.

ICMP/ICMPv6 Header Translation for MAP-T

Mapping of address and port using translation (MAP-T) customer edge (CE) devices and border routers use the ICMP/ICMPv6 translation for address sharing of port ranges.

Unlike TCP and UDP, which provide two port fields to represent source and destination addresses, the Internet Control Message Protocol (ICMP) and ICMP Version 6 (ICMPv6) query message headers have only one ID field.

When an ICMP query message originates from an IPv4 host that exists beyond a MAP-T CE device, the ICMP ID field is exclusively used to identify the IPv4 host. The MAP-T CE device rewrites the ID field to a port-set value that is obtained through the basic mapping rule (BMR) during the IPv4-to-IPv6 translation, and the border router translates ICMPv6 packets to ICMP.

When a MAP-T border router receives an ICMP packet that contains an ID field that is bound for a shared address in the MAP-T domain, the MAP-T border router uses the ID field as a substitute for the destination port to determine the IPv6 destination address. The border router derives the destination IPv6 address by mapping the destination IPv4 address without the port information for packets that do not contain the ID field, and the corresponding CE device translates the ICMPv6 packets to ICMP.

Path MTU Discovery and Fragmentation in MAP-T

Mapping of address and port using translation (MAP-T) uses path maximum transmission unit (MTU) discovery and fragmentation for IPv4-to-IPv6 translation because the size of IPv4 (more than 20 octets) and IPv6 (40 octets) headers is different. The MTU defines the largest size of a packet that an interface can transmit without the need to fragment the packet. IP packets larger than the MTU must go through IP fragmentation procedures.

When an IPv4 node performs path MTU discovery by setting the Don't Fragment (DF) bit in the packet header, path MTU discovery operates end-to-end across the MAP-T border router and customer edge (CE) translators. During IPv4 path MTU discovery, either the IPv4 device or the IPv6 device can send ICMP “Packet Too Big” messages to the sender. When IPv6 devices send these messages as Internet Control Message Protocol Version 6 (ICMPv6) errors, the packets that follow the message pass through the translator and result in an appropriate ICMP error message sent to the IPv4 sender.

When the IPv4 sender does not set the DF bit, the translator fragments the IPv4 packet and includes the packet with fragment headers to fit the packet in the minimum MTU 1280-byte IPv6 packets. When packets are fragmented, either by the sender or by IPv4 devices, the low-order 16 bits of the fragment identification are carried end-to-end across the MAP-T domain to ensure that packets are reassembled correctly.

How to Configure Mapping of Address and Port Using Translation

Prerequisites for Configuring MAP-T

There are no prerequisites to configure MAP-T.

Restrictions for Configuring MAP-T

- Application-level Gateway (ALG) is not supported with this feature.

- The maximum number of MAP-T domains supported is 10000.
- Forwarding Mapping Rule (FMR) is not supported.

Information for Configuring MAP-T

To support the MAP-T Customer Edge (CE) functionality, the current IOS-XE NAT64 architecture is used. It performs the translation of IPv4 packets to IPv6 packets, and vice versa. As MAP-T CE needs to perform the NAT44 to translate the private IPv4 address, it also utilizes the existing IOS-XE NAT44 pool-based translation to perform the NAT44 translation before going through the NAT64 translation.

The difference between MAP-E and MAP-T is mainly the packet encapsulation format. While MAP-T translates the IPv4 header to the IPv6 header (and vice versa), MAP-E encapsulates the entire IPv4 packet into the IPv6 packet. When handling the Basic Mapping Rule (BMR) and Default Mapping Rule (DMR) parameters, MAP-E and MAP-T have similar behaviour.

Description of the Algorithms

When a MAP-T domain is defined via CLI, an IPv6 and IPv4 routing entry would also be installed on the router to point to the NVI (Nat Virtual Interface). The NVI interface is a virtual interface which is used by IOS-XE NAT64 to perform the translation between IPv4 and IPv6 packets. Depending on the mode of the router (whether it is a CE or Border Router (BR)), the routes installed are different. If the router is a BR, an IPv6 routing entry is created based on the DMR IPv6 prefix, and an IPv4 routing entry is created based on the BMR IPv4 prefix. Whereas, if the router is a CE, an IPv6 routing entry is created based on the BMR IPv6 prefix. The IPv4 routing entry on the CE would need to be defined via the “nat64 route” CLI. It is a default route which points to the NVI.

When the CE receives an IPv4 packet in the LAN, it would need to determine the MAP-T domain which contains all the mapping parameters required to translate the IPv4 packet to an IPv6 packet. This is done by a longest IPv4 prefix search on the source address against the local IPv4 prefix defined in the BMR of the MAP-T domain. If a match is found, it would use the BMR and DMR parameters defined in the domain to process the packet further. In addition, it would create a NAT44 session to translate the private IPv4 source address to a public IPv4 address.

The handling of the IPv6 packet on the CE is the opposite of the IPv4 packet handling. It would first perform a longest IPv6 prefix search on the destination address against the BMR IPv6 prefix defined in the domain. If a match is found, it would translate the IPv6 header to an IPv4 header, based on the BMR and DMR parameters defined in the domain. After that, the IPv4 packet would be handled by the NAT44 component to translate the public IPv4 address to a private IPv4 address.

Configuring MAP-T for CE

SUMMARY STEPS

1. **nat64 settingsmap-tce**
2. **nat64 map-t domain** *number***vrf***vrf-name*
3. **nat64 routevrf** *vrf-nameipv4-prefixinterface-name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**nat64 settingsmap-tce**	Sets the router to be in the CE mode, instead of BR (which is the default). It must be configured before any map-t domain is defined.
Step 2	**nat64 map-t domain** *number***vrf***vrf-name*	Defines a map-t domain by optionally specifying the vrf. • The port-set-id defines the port-set id used by the CE. This is a mandatory config on the CE. • The local-ipv4-prefix is used as the selector to identify the correct domain for the local traffic. Defines a map-t domain by optionally specifying the vrf. • The port-set-id defines the port-set id used by the CE. This is a mandatory config on the CE. • The local-ipv4-prefix is used as the selector to identify the correct domain for the local traffic.
Step 3	**nat64 routevrf** *vrf-nameipv4-prefixinterface-name*	This CLI defines the routing to route the local traffic in a vrf to the NVI (Nat Virtual Interface), for nat64 handling.

Configuring MAP-T for BR

SUMMARY STEPS

1. **nat64 settingsmap-tbr**
2. **nat64 map-t domain** *number*
3. **nat64 settingsv4 udp-0-checksum**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**nat64 settingsmap-tbr**	Sets the router to be in the BR (Border Relay) mode, which is the default. This must be configured before any map-t domain is defined.
Step 2	**nat64 map-t domain** *number*	Defines a map-t domain for BR mode.
Step 3	**nat64 settingsv4 udp-0-checksum**	Enables support for fragmented IPv4 packets with a UDP checksum value of 0. This must be enabled on the device

	Command or Action	Purpose
		to prevent such packets from being dropped during translation.

Sample Configurations

Sample configuration on CE (same vrf on IPv4 and IPv6):

```
vrf definition vrf2
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family
ipv6 unicast-routing
interface GigabitEthernet2
vrf forwarding vrf2
no ip address
nat64 enable
ipv6 address 2701:D01:4:1000:0:A601:1:1/64
ipv6 address autoconfig default
ipv6 enable
ipv6 virtual-reassembly in
interface GigabitEthernet4
vrf forwarding vrf2
ip address 100.100.0.93 255.255.255.0
nat64 enable
no ip nat service all-algs
ip nat pool pool-mapt 166.1.0.1 166.1.0.1 prefix-length 30
ip nat inside source route-map rm1 pool pool-mapt vrf vrf2 match-in-vrf overload
ip access-list extended inside-local
10 permit ip 100.100.0.0 0.0.255.255 any
route-map rm1 permit 10
match ip address inside-local
nat64 settings map-t ce
nat64 route vrf vrf2 0.0.0.0/0 GigabitEthernet2
nat64 map-t domain 1001 vrf vrf2
default-mapping-rule 3601:D01:3344:5566::/64
basic-mapping-rule
ipv6-prefix 2701:D01::/32
ipv4-prefix 166.1.0.0/18
port-parameters share-ratio 64 start-port 512
port-set-id 1
local-ipv4-prefix 100.100.0.0/16
```

Sample configuration on CE (IPv6 on global vrf):

```
vrf definition vrf2
address-family ipv4
exit-address-family
address-family ipv6
exit-address-family
ipv6 unicast-routing
interface GigabitEthernet2
no ip address
nat64 enable
ipv6 address 2701:D01:4:1000:0:A601:1:1/64
ipv6 address autoconfig default
ipv6 enable
ipv6 virtual-reassembly in
```

```
interface GigabitEthernet4
vrf forwarding vrf2
ip address 100.100.0.93 255.255.255.0
nat64 enable
no ip nat service all-algs
ip nat pool pool-mapt 166.1.0.1 166.1.0.1 prefix-length 30
ip nat inside source route-map rm1 pool pool-mapt overload
ip access-list extended inside-local
10 permit ip 100.100.0.0 0.0.255.255 any
route-map rm1 permit 10
match ip address inside-local
nat64 settings map-t ce
nat64 route vrf vrf2 0.0.0.0/0 GigabitEthernet2
nat64 map-t domain 1001
default-mapping-rule 3601:D01:3344:5566::/64
basic-mapping-rule
ipv6-prefix 2701:D01::/32
ipv4-prefix 166.1.0.0/18
port-parameters share-ratio 64 start-port 512
port-set-id 1
local-ipv4-prefix 100.100.0.0/16
```

Sample configuration on BR:

```
ipv6 unicast-routing
interface GigabitEthernet2
nat64 enable
ipv6 address 2701:D01:4:1000::9/64
ipv6 enable
ipv6 virtual-reassembly in
interface GigabitEthernet3
ip address 192.0.2.1 255.255.255.0
nat64 enable
nat64 map-t domain 1000
default-mapping-rule 3601:D01:3344:5566::/64
basic-mapping-rule
ipv6-prefix 2701:D01::/32
ipv4-prefix 166.1.0.0/18
port-parameters share-ratio 64 start-port 512
```

Sample configuration on BR

```
ipv6 unicast-routing
interface TenGigabitEthernet0/0/1
ip address 200.200.0.66 255.255.255.0
negotiation auto
nat64 enable
interface TenGigabitEthernet0/0/2
no ip address
negotiation auto
nat64 enable
ipv6 address 6600::1/64
ipv6 address 6601::1/64
ipv6 enable
ipv6 route 2A02:C7A:E43C::/46 6601::2
ipv6 route 2A02:C7A:E460::/43 6600::2
nat64 map-t domain 3002
default-mapping-rule 2A02:C79:FC03:43::/64
basic-mapping-rule
ipv6-prefix 2A02:C7A:E460::/43
ipv4-prefix 100.67.8.0/22
port-parameters share-ratio 8
nat64 map-t domain 3003
```

```
default-mapping-rule 2A02:C79:FC03:44::/64
basic-mapping-rule
ipv6-prefix 2A02:C7A:E43C::/46
ipv4-prefix 100.67.12.0/22
port-parameters share-ratio 1
```

Configure MAP-T CE to support DHCP

The MAP-T CE feature is enhanced to support the DHCP RFC 7598 (OPTION_S46_CONT_MAPT).

Before you begin

If you have an existing MAP-T domain configured, you need to delete the domain using the **no nat64 map-t domain domain-number** command.

SUMMARY STEPS

1. Configure a WAN interface to use DHCP.
2. Configure NAT64 to route the traffic in a vrf to the interface.

DETAILED STEPS

Procedure

Step 1 Configure a WAN interface to use DHCP.

Example:

```
Router# configure terminal
Router(config)# interface interface-name
Router(config-if)# nat64 enable
Router(config-if)# ipv6 address dhcp
Router(config-if)# ipv6 address autoconfig default
Router(config-if)# ipv6 enable
Router(config-if)# end
```

Step 2 Configure NAT64 to route the traffic in a vrf to the interface.

Example:

```
Router# configure terminal
Router(config)# nat64 settings map-t ce
Router(config-nat64-mapt# nat64 route vrf vrf-name ipv4-prefix interface-name
Router(config-nat64-mapt# end
```

Example

Sample Configuration

```
vrf definition vrf2
 address-family ipv4
 exit-address-family
 address-family ipv6
 exit-address-family
```

```
ipv6 unicast-routing
interface GigabitEthernet2
 nat64 enable
 ipv6 address dhcp
 ipv6 address autoconfig default
 ipv6 enable
interface GigabitEthernet4
 vrf forwarding vrf2
 ip address 192.168.0.93 255.255.255.0
 nat64 enable
no ip nat service all-algs
nat64 settings map-t ce
nat64 route vrf vrf2 0.0.0.0/0 GigabitEthernet2
```

Configuring Mapping of Address and Port Using Translation

Before you begin

Prerequisites:

- Configure the **ipv6 enable** command on interfaces on which you configure the Mapping of Address and Port Using Translation feature.
- Configure the default mapping rule before you configure the basic mapping rule.
- While configuring mapping of address and port using translation (MAP-T), the default mapping rule (DMR) prefix, the IPv6 user prefix, and the IPv6 prefix plus the embedded address (EA) bits must be less than or equal to 64 bits, and the share ratio plus the contiguous ports plus the start port must be 16 bits.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **nat64 map-t domain** *number*
4. **default-mapping-rule** *ipv6-prefix/prefix-length*
5. **basic-mapping-rule**
6. **ipv6-prefix** *prefix/length*
7. **ipv4-prefix** *prefix/length*
8. **port-parameters share-ratio** *ratio* [**start-port** *port-number*]
9. **end**
10. **show nat64 map-t domain** *number*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter you password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**nat64 map-t domain** *number* **Example:** `Device(config)# nat64 map-t domain 1`	Configures the Network Address Translation 64 (NAT64) mapping of address and port using translation (MAP-T) domain and enters NAT64 MAP-T configuration mode.
Step 4	**default-mapping-rule** *ipv6-prefix/prefix-length* **Example:** `Device(config-nat64-mapt)# default-mapping-rule 2001:DA8:B001:FFFF::/64`	Configures the default domain mapping rule for the MAP-T domain.
Step 5	**basic-mapping-rule** **Example:** `Device(config-nat64-mapt)# basic-mapping-rule`	Configures the basic mapping rule (BMR) for the MAP-T domain and enters NAT64 MAP-T BMR configuration mode.
Step 6	**ipv6-prefix** *prefix/length* **Example:** `Device(config-nat64-mapt-bmr)# ipv6-prefix 2001:DA8:B001::/56`	Configures an IPv6 address and prefix for the MAP-T BMR.
Step 7	**ipv4-prefix** *prefix/length* **Example:** `Device(config-nat64-mapt-bmr)# ipv4-prefix 202.1.0.128/28`	Configures an IPv4 address and prefix for the MAP-T BMR.
Step 8	**port-parameters share-ratio** *ratio* [**start-port** *port-number*] **Example:** `Device(config-nat64-mapt-bmr)# port-parameters share-ratio 16 start-port 1024`	Configures port parameters for the MAP-T BMR.

Step 9	**end**
	Example:
	`Device(config-nat64-mapt-bmr)# end`
		Exits NAT64 MAP-T BMR configuration mode and returns to privileged EXEC mode.

Step 10	**show nat64 map-t domain** *number* **Example:** `Device# show nat64 map-t domain 1`	Displays MAP-T domain information.

Example:

The following is sample output from the **show nat64 map-t domain** command:

```
Device# show nat64 map-t domain 1

MAP-T Domain 1
Mode MAP-T
Default-mapping-rule
Ip-v6-prefix 2001:DA8:B001:FFFF::/64
Basic-mapping-rule
Ip-v6-prefix 2001:DA8:B001::/56
Ip-v4-prefix 202.1.0.128/28
Port-parameters
Share-ratio 16 Contiguous-ports 64 Start-port 1024
Share-ratio-bits 4 Contiguous-ports-bits 6 Port-offset-bits 6
```

Configuration Examples for Mapping of Address and Port Using Translation

Example: Configuring Mapping of Address and Port Using Translation

```
Device# configure terminal
Device(config)# nat64 map-t domain 1
Device(config-nat64-mapt)# $ping-rule 2001:DA8:B001:FFFF::/64
Device(config-nat64-mapt)# basic-mapping-rule
Device(config-nat64-mapt-bmr)# ipv6-prefix 2001:DA8:B001::/56
Device(config-nat64-mapt-bmr)# ipv4-prefix 202.1.0.128/28
Device(config-nat64-mapt-bmr)# $ters share-ratio 16 start-port 1024
Device(config-nat64-mapt-bmr)# end
```

Example: MAP-T Deployment Scenario

The following illustration shows a mapping of address and port using translation (MAP-T) deployment scenario.

The following is the configuration for the MAP-T deployment scenario:

```
Device(config)# nat64 map-t
Device(config)# nat64 map-t domain 1
Device(config-nat64-mapt)# $ping-rule 2001:DA8:B001:FFFF::/64
Device(config-nat64-mapt)# basic-mapping-rule
Device(config-nat64-mapt-bmr)# ipv6-prefix 2001:DA8:B001::/56
Device(config-nat64-mapt-bmr)# ipv4-prefix 202.1.0.128/28
Device(config-nat64-mapt-bmr)# $ters share-ratio 16 start-port 1024
Device(config-nat64-mapt-bmr)# end
```

At the PC:

An IPv4 packet goes from 202.1.0.130 to 11.1.1.1. At the customer edge (CE) device the Mapping of address and port mapping using translation (MAP-T) function translates the packet to Src: 2201:DA8:B001:2E:0:CA01:82:E00 Dest: 2001:DA8:B001:FFFF:B:0101:0100:0.

At the border router the MAP-T border router translates the packet to

Packet goes from 192.168.1.2 ---> 74.1.1.1, source 4000, destination port : 5000

At the CPE the MAP-T CE function translates the

packet to Src: 2201:DA8:B001:2E:0:CA01:82:E00 Dest: 2001:DA8:B001:FFFF:B:0101:0100:0.

At the BR the MAP-T BR function translates the packet to

Src:203.38.102.130 Dst:74.1.1.1 SrcPort:4000 DstPort:5000

From End device:

Src:74.1.1.1 Dst:203.38.102.130 SrcPort:4000 DstPort:5000

At the BR the MAP-T BR function translates the packet to

Src: 2201:DA8:B001:2E:0:CA01:82:E00 Dest: 2001:DA8:B001:FFFF:B:0101:0100:0.

At the CE the MAP-T CE function translates the packet from

Src: 2201:DA8:B001:2E:0:CA01:82:E00 Dest: 2001:DA8:B001:FFFF:B:0101:0100:0.

To

Src:74.1.1.1 Dst:203.38.102.130 SrcPort:4000 Dstport:5000

Additional References for Mapping of Address and Port Using Translation

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
NAT commands	Cisco IOS IP Addressing Services Command Reference

Standards and RFCs

Standard/RFC	Title
MAP	Mapping of Address and Port (MAP)
MAP Translation	MAP Translation (MAP-T) - specification
RFC 6052	IPv6 Addressing of IPv4/IPv6 Translators
RFC 6144	Framework for IPv4/IPv6 Translation
RFC 6145	IP/ICMP Translation Algorithm
RFC 7598	DHCPv6 Options for Configuration of Softwire Address and Port-Mapped Clients

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Mapping of Address and Port Using Translation

Glossary

EA bits—Embedded address bits. The IPv4 EA bits in the IPv6 address identify an IPv4 prefix/address (or part thereof) or a shared IPv4 address (or part thereof) and a port-set identifier.

IP fragmentation—The process of breaking a datagram into a number of pieces that can be reassembled later. The IP source, destination, identification, total length, and fragment offset fields, along with the More fragments and Don't Fragment (DF) flags in the IP header, are used for IP fragmentation and reassembly. A DF bit is a bit within the IP header that determines whether a device is allowed to fragment a packet.

IPv4-translatable address—IPv6 addresses that are used to represent IPv4 hosts. These addresses have an explicit mapping relationship to IPv6 addresses. This relationship is self-described by mapping the IPv4 address in the IPv6 address. Both stateless and stateful translators use IPv4-translatable (also called IPv4-converted) IPv6 addresses to represent IPv4 hosts.

IPv6-translatable address—IPv6 addresses that are assigned to IPv6 hosts for stateless translation. These IPv6-translatable addresses (also called IPv6-converted addresses) have an explicit mapping relationship to IPv4 addresses. This relationship is self-described by mapping the IPv4 address in the IPv6 address. The stateless translator uses corresponding IPv4 addresses to represent IPv6 hosts. The stateful translator does not use IPv6-translatable addresses because IPv6 hosts are represented by the IPv4 address pool in the translator via dynamic states.

MAP rule—A set of parameters that define the mapping between an IPv4 prefix, an IPv4 address or a shared IPv4 address, and an IPv6 prefix or address. Each MAP domain uses a different mapping rule set.

MAP-T border router—A mapping of address and port using translation (MAP-T)-enabled router or translator at the edge of a MAP domain that provides connectivity to the MAP-T domain. A border relay router has at least one IPv6-enabled interface and one IPv4 interface connected to the native IPv4 network, and this router can serve multiple MAP-T domains.

MAP-T CE—A device that functions as a customer edge (CE) router in a MAP-T deployment. A typical MAP-T CE device that adopts MAP rules serves a residential site with one WAN-side interface and one or more LAN-side interfaces. A MAP-T CE device can also be referred to as a “CE” within the context of a MAP-T domain.

MAP-T domain—Mapping of address and port using translation (MAP-T) domain. One or more customer edge (CE) devices and a border router, all connected to the same IPv6 network. A service provider may deploy a single MAP-T domain or use multiple MAP domains.

MRT—MAP rule table. Address and port-aware data structure that supports the longest match lookups. The MRT is used by the MAP-T forwarding function.

path MTU—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.

stateful translation—Creates a per-flow state when the first packet in a flow is received. A translation algorithm is said to be stateful if the transmission or reception of a packet creates or modifies a data structure in the relevant network element. Stateful translation allows the use of multiple translators interchangeably and also some level of scalability. Stateful translation enables IPv6 clients and peers without mapped IPv4 addresses to connect to IPv4-only servers and peers.

stateless translation—A translation algorithm that is not stateful. A stateless translation requires configuring a static translation table or may derive information algorithmically from the messages that it is translating. Stateless translation requires less computational overhead than stateful translation. It also requires less memory to maintain the state because the translation tables and the associated methods and processes exist in a stateful algorithm and do not exist in a stateless one. Stateless translation enables IPv4-only clients and peers to initiate connections to IPv6-only servers or peers that are equipped with IPv4-embedded IPv6 addresses. It also enables scalable coordination of IPv4-only stub networks or ISP IPv6-only networks. Because the source port in an IPv6-to-IPv4 translation may have to be changed to provide adequate flow identification, the source port in the IPv4-to-IPv6 direction need not be changed.