Understanding MAP-T Exception Handling

The MAP-T Exception Handling with VSM feature handles fragmented packets, TCP MSS clamping, path MTU and ICMP packets. Depending on the header details of the fragmented packets, the CGN application directly interacts with the line cards to process or forward the packets to VSM.

Note When MAP-T is configured for exception handling with VSM, the static route details are automatically configured with Service App details for an IPV6 to IPv4 translated packet. No manual configuration is required to configure the static routes. But in the case of an IPv4 to IPv6 translated packet, static routes have to be manually configured.

Configuration and Scalability Limits

- Starting from Release 24.4.1, ICMP rate limiting is supported.
- Ensure that ServiceInfra is configured before other steps are executed to configure MAP-T for exception handling. The service infrastructure is used for the management plane.
- Configuring map-t-cisco instances :
  - Only a single external domain can be configured for each map-t-cisco instance.
  - The maximum number of CPE domains that can be configured for MAP-T exception handling is 1024.
  - The number of map-t-cisco instances supported for exception handling is 32 and the maximum number of CPE domain parameters that can be used in a single map-t-cisco instance is 256.
  - A map-t-cisco instance can be configured only with a default VRF.

- To ensure IPv4/IPv6 translation is successfully performed, set the path MTU of the tunnel for both IPv4 and IPv6 traffic to 1500 bytes.
- The IOS XR software does not support IPv6 fragmentation.
  - If an IPv4 packet that does not have a DF bit set is translated to an IPv6 packet that exceeds the configured MTU, the packet is translated by VSM and forwarded.

Note

- If the Path-MTU value is not configured, the default value is assumed to be 1280 bytes.
- Configure the MTU on physical VSM interfaces to 1518 bytes.

  - If an IPv6 packet that does not have a fragment header set is translated to an IPv4 packet that exceeds the minimum MTU, the packet is dropped and an ICMP error message is sent.

- Modification of path-mtu value is not recommended. If you modify the path-mtu setting, delete the service-inline interface and configure it again for the path-mtu changes to take effect.
- Deletion of ServiceApp configuration from a MAP-T domain is not permitted.

Supported IPv6 Extension Headers

This implementation of MAP-T exception handling supports the following IPV6 extension headers:

- Hop-by-Hop Options header (if this header exists, it must be the first one following the main/regular header)
- Destination Options header.
- Routing header.
- Fragment header.

Processing of Fragmented Packets

The following table shows how MAP-T handles a fragmented IPv6 packet that is translated to an IPv4 packet.

Fragment Header	More Fragment flag	Fragment off	Action taken
0	x	x	Lookup success. Processed by 8X100 GE line card
1	0	0	Lookup success based on protocol field. Forward packet to VSM

Fragment Header	More Fragment flag	Fragment off	Action taken
1	0	1	Last fragment. Forward packet to VSM.
1	1	0	First fragment. Forward packet to VSM
1	1	1	Middle fragment. Forward packet to VSM

The following table shows how MAP-T handles fragmentation for an IPv4 packet that is translated to an IPv6 packet.

Do Not Fragment bit	More Fragment bit	Fragment off	Action
0	0	0	Lookup success based on protocol value. The translated packet will contain a Fragment header
0	0	1	Lookup fail. Forward to VSM
0	1	0	Lookup fail. Forward to VSM
0	1	1	Lookup fail. Forward to VSM
1	0	0	Lookup success. Processed by 8X100 GE line card

Configuring MAP-T for Exception Handling with VSM

Perform these tasks to configure MAP-T for exception handling with VSM

Running Configuration

```
interface ServiceInfra1
ipv4 address 1.1.1.1 255.255.255.252
service-location 0/4/CPU0
!
interface ServiceApp1
ipv4 address 40.40.40.1 255.255.255.0
service cgv6 cgn123 service-type map-t-cisco
!
```

```
service cgv6 cgn123
service-location preferred-active 0/4/CPU0
service-inline interface tenGigE 0/0/0/0/2
service-type map-t-cisco map1
address-family ipv4
interface ServiceApp1
tcp mss 335
path-mtu 1200
!
address-family ipv6
interface ServiceApp2
tcp mss 1254
path-mtu 1500
!
cpe-domain ipv4 prefix length 24
cpe-domain ipv6 vrf default
cpe-domain ipv6 prefix length 48
sharing-ratio 256
contiguous-ports 16
cpe-domain-name cpe0 ipv4-prefix 192.1.1.0 ipv6-prefix 2301:0:1122::
cpe-domain-name cpe1 ipv4-prefix 192.1.2.0 ipv6-prefix 2301:1:1122::
cpe-domain-name cpe2 ipv4-prefix 192.1.3.0 ipv6-prefix 2301:2:1122::
cpe-domain-name cpe3 ipv4-prefix 192.1.4.0 ipv6-prefix 2301:3:1122::
cpe-domain-name cpe4 ipv4-prefix 192.1.5.0 ipv6-prefix 2301:4:1122::
cpe-domain-name cpe5 ipv4-prefix 192.1.6.0 ipv6-prefix 2301:5:1122::
cpe-domain-name cpe6 ipv4-prefix 192.1.7.0 ipv6-prefix 2301:6:1122::
cpe-domain-name cpe7 ipv4-prefix 192.1.8.0 ipv6-prefix 2301:7:1122::
cpe-domain-name cpe8 ipv4-prefix 192.1.9.0 ipv6-prefix 2301:8:1122::
cpe-domain-name cpe9 ipv4-prefix 192.1.10.0 ipv6-prefix 2301:9:1122::
cpe-domain-name cpe10 ipv4-prefix 192.1.11.0 ipv6-prefix 2301:a:1122::
cpe-domain-name cpe11 ipv4-prefix 192.1.12.0 ipv6-prefix 2301:b:1122::
cpe-domain-name cpe12 ipv4-prefix 192.1.13.0 ipv6-prefix 2301:c:1122::
cpe-domain-name cpe13 ipv4-prefix 192.1.14.0 ipv6-prefix 2301:d:1122::
cpe-domain-name cpe14 ipv4-prefix 192.1.15.0 ipv6-prefix 2301:e:1122::
```

```
cpe-domain-name cpe15 ipv4-prefix 192.1.16.0 ipv6-prefix 2301:f:1122::
cpe-domain-name cpe16 ipv4-prefix 192.1.17.0 ipv6-prefix 2301:10:1122::
cpe-domain-name cpe17 ipv4-prefix 192.1.18.0 ipv6-prefix 2301:11:1122::
cpe-domain-name cpe18 ipv4-prefix 192.1.19.0 ipv6-prefix 2301:12:1122::
cpe-domain-name cpe19 ipv4-prefix 192.1.20.0 ipv6-prefix 2301:13:1122::
cpe-domain-name cpe20 ipv4-prefix 192.1.21.0 ipv6-prefix 2301:14:1122::
cpe-domain-name cpe21 ipv4-prefix 192.1.22.0 ipv6-prefix 2301:15:1122::
cpe-domain-name cpe22 ipv4-prefix 192.1.23.0 ipv6-prefix 2301:16:1122::
cpe-domain-name cpe23 ipv4-prefix 192.1.24.0 ipv6-prefix 2301:17:1122::
cpe-domain-name cpe24 ipv4-prefix 192.1.25.0 ipv6-prefix 2301:18:1122::
cpe-domain-name cpe25 ipv4-prefix 192.1.26.0 ipv6-prefix 2301:19:1122::
cpe-domain-name cpe26 ipv4-prefix 192.1.27.0 ipv6-prefix 2301:1a:1122::
cpe-domain-name cpe27 ipv4-prefix 192.1.28.0 ipv6-prefix 2301:1b:1122::
cpe-domain-name cpe28 ipv4-prefix 192.1.29.0 ipv6-prefix 2301:1c:1122::
cpe-domain-name cpe29 ipv4-prefix 192.1.30.0 ipv6-prefix 2301:1d:1122::
cpe-domain-name cpe30 ipv4-prefix 192.1.31.0 ipv6-prefix 2301:1e:1122::
cpe-domain-name cpe31 ipv4-prefix 192.1.32.0 ipv6-prefix 2301:1f:1122::
ext-domain-name ext1 ipv6-prefix 6301:d01:1122::/48 ipv4-vrf default
!
```

Troubleshooting ICMP Errors

This section covers details of errors encountered during translation of packets from IPv4 to IPv6 and vice versa.

Translating ICMP IPv4 Headers to ICMP IPv6 Headers

Translating ICMP IPv6 Headers to ICMP IPv4 Headers

Translating ICMP IPv4 Headers to ICMP IPv6 Headers

	IPv4 Header	IPv6 Header	Description of the error
Destination Unreachable (Type 3)	Network Unreachable (code 0)	Type 1 code 0	Communication with destination administratively prohibited
	Host Unreachable (code 1)	Type 1 code 0	No route to destination

	IPv4 Header	IPv6 Header	Description of the error
	Protocol Unreachable (code 2)	Type 4 code 1	Unrecognized Next Header type encountered
	Port Unreachable (code 3)	Type 1 code 4	Port unreachable
	Fragmentation Needed and DF was set (code 4)		No route to destination
	Source Route Failed(code 5)		No route to destination
	code 6	Type 1 code 0	No route to destination
	code 7	Type 1 code 0	No route to destination
	code 8	Type 1 code 0	No route to destination
	code 9	Type 1 code 1	
	code 10	Type 1 code 1	Communication with destination administratively prohibited
	code 11	Type 1 code 0	No route to destination
	code 12	Type 1 code 0	No route to destination
	code 13	Type 1 code 0	No route to destination
	code 14	Drop	
	code 15	Type 1 code 1	Communication with destination administratively prohibited
	Time Exceeded (type 11)	Type 3	Time Exceeded
Parameter Problem (Type 12)	Pointer indicates the error (code 0)	Type 4 code 0	Parameter Problem
	Missing a required option (code 1)	Drop	
	Bad Length (code 2)	Type 4 code 0	Erroneous header field encountered
	Echo request (Type 8)	Type 128	Echo Request
	Echo reply (Type 0)	Type 129	Echo Reply

Translating ICMP IPv6 Headers to ICMP IPv4 Headers

	IPv6 Header	IPv4 Header	Description of the error
Destination Unreachable (Type 1)	No route to destination (code 0)	code 1	No route to destination

	IPv6 Header	IPv4 Header	Description of the error
	Communication with destination prohibited (code 1)	code 10	Communication with destination prohibited
	Beyond scope 0f src address (code 2)	code 1	Beyond scope of src address
	Address unreachable (code 3)	code 1	Address unreachable
	Port unreachable (code 4)	code 3	Port unreachable
	Packet Too Big (Type 2)	Type 3 code 4	Fragmentation needed and Don't Fragment was Set
Time Exceeded (type 3)	Hop limit exceeded in transmit (code 0)	Type 11 code 0	Time to Live exceeded in Transit
	Fragment reassembly timeout (code 1)	Type 11 code 1	Fragment Reassembly Time Exceeded
Parameter Problem (Type 4)	Erroneous header field(code 0)	erroneous header field(code 0) Type 12 code 0	Pointer indicates the error
	Unrecognized nxt header field (code 1)	Type 3 code 2	Protocol Unreachable
	Unrecognized IPv6 option encountered (code 2)	drop	Communication with destination administratively prohibited