TLOC

TLOC

A TLOC (Transport Locator) is a unique identifier in Cisco Catalyst SD-WAN that

- represents a WAN Edge device's connection to a WAN transport, and
- is defined by the combination of its system IP address, a color indicating the type of transport, and an encapsulation type.

Components of TLOC

A TLOC is made up of three components:

- System IP address: The unique IP address of the SD-WAN device.
- Color: A Cisco Catalyst SD-WAN software construct that identifies the transport tunnel.
- Encapsulation: The method used to encapsulate the overlay tunnel data.

Tunnel interface

A tunnel interface in Cisco Catalyst SD-WAN is a network connection that you configure for secure data transport. On a Cisco SD-WAN Controller or Cisco SD-WAN Manager, you can configure one tunnel interface. On a Cisco IOS XE Catalyst SD-WAN device, you can configure up to eight tunnel interfaces.

To limit the remote TLOCs that the local TLOC can establish BFD sessions with, mark the TLOC with the **restrict** option. When a TLOC is marked as restricted, a TLOC on the local router establishes tunnel connections with a remote TLOC only if the remote TLOC has the same color.

When a WAN edge device is configured with two IPv6 TLOCs, one with static default route and the other one with IPv6 address autoconfig default which is the IPv6 neighbor discovery default route, the IPv6 neighbor discovery default route is not installed in the routing table. In this case, the IPv6 TLOC with IPv6 neighbor discovery default route does not work.

For IPv6 TLOC with IPv6 neighbor discovery default route to work, you can configure the static route for TLOC with IPv6 neighbor discovery to overwrite the IPv6 neighbor discovery default route and ensure that both the static routes are installed into the routing table. You can also use the IPv6 neighbor discovery default route on all interfaces.

A tunnel interface allows only DTLS, TLS, and, for Cisco IOS XE Catalyst SD-WAN devices, IPsec traffic to pass through the tunnel. To allow additional traffic to pass without having to create explicit policies or access lists, enable them by including one **allow-service** command for each service. You can also explicitly disallow services by including the **no allow-service** command. Note that services affect only physical interfaces.

STUN server

In Cisco Catalyst SD-WAN, Session Traversal Utilities for NAT (STUN) is a protocol used by Cisco IOS XE Catalyst SD-WAN devices to discover their public IP address and port assigned by a Network Address Translator (NAT).

Use the **allow-service stun** command to enable or disable a Cisco IOS XE Catalyst SD-WAN device from sending requests to a generic STUN server. This allows the device to determine if it is behind a NAT, identify the NAT type, and discover its public IP address and port number. On a Cisco IOS XE Catalyst SD-WAN device that is behind a NAT, you can also configure a tunnel interface to obtain its public IP address and port number from the Cisco SD-WAN Validator.

When you configure the Cisco IOS XE Catalyst SD-WAN device to use the Cisco SD-WAN Validator as a STUN server, the device determines its public IP address and public port number, which enables it to establish TLOC connections and form the overlay fabric over various public transports like broadband or cellular networks. However, the device cannot identify the type of NAT it is behind in this setup. The tunnel interface configured for the Cisco SD-WAN Validator does not carry overlay network control traffic or exchange encryption keys, but BFD establishes connectivity and allows data traffic. Because this tunnel does not support control traffic, you must configure at least one additional tunnel interface to ensure the device can exchange control traffic with the Cisco SD-WAN Controller and Cisco SD-WAN Manager.

You can log the headers of all packets that the system drops because they do not match a service configured with an **allow-service** command. You can use these logs for security purposes, for example, to monitor the flows that are being directed to a WAN interface and to determine, in the case of a DDoS attack, which IP addresses to block.

System IP address

A system interface IP address is a persistent address that

- identifies the Cisco IOS XE Catalyst SD-WAN device,
- is similar to a router ID on a regular router, and
- is used to identify the router from which packets originated.

System IP address configuration

You configure a system interface for each Cisco IOS XE Catalyst SD-WAN device using the **system system-ip** command. Specify the system IP address as an IPv4 address in decimal four-part dotted notation, without including the prefix length; the /32 prefix is implicit. The system IP address must not be within the following ranges: 0.0.0.0/8, 127.0.0.0/8, 224.0.0.0/4, or 240.0.0.0/4 and later. Assign a unique system IP address to each device in the overlay network. You cannot assign this address to another interface in VPN 0.

The system interface is placed in VPN 0 as a loopback interface named **system**. This loopback is not the same as a loopback address that you configure for a specific interface. To display information about the system interface, use the **show interface** command.

Role in OMP TLOC identification

The system IP address is used as one of the attributes of the OMP TLOC (Overlay Management Protocol Transport Locator). Each TLOC is uniquely identified by a 3-tuple: the system IP address, a color, and an encapsulation. Use the **show omp tlocs** command to display TLOC information.

Device management

For device management, configure the same system IP address on a loopback interface located in a service-side VPN appropriate for management purposes. Use a loopback interface because it remains reachable whenever the router is operational and the overlay network is up. Avoid configuring the system IP address on a physical interface, since both the router and the interface must be up for reachability in that case.

Assign the loopback interface to a service-side VPN, which is any VPN other than VPN 0 (the WAN transport VPN) or VPN 512 (the management VPN). Service-side VPNs are used to route data traffic and remain reachable from the data center.

Color

A color is a Cisco Catalyst SD-WAN software construct that

- identifies the transport tunnel,
- includes options such as **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**, and
- designates **metro-ethernet**, **mpls**, and **private1** through **private6** as private colors that use private addresses for private networks, which can be used on public networks only if there is no NAT device between the local and remote Cisco IOS XE Catalyst SD-WAN devices.

Encapsulation

An encapsulation is a required configuration on Cisco IOS XE Catalyst SD-WAN devices that

- specifies the tunnel encapsulation type as either IPsec or GRE, and
- sets the default MTU to 1442 bytes for IPsec and 1468 bytes for GRE, which is enabled by default on all TLOCs, based on BFD path MTU discovery.

You can configure both IPsec and GRE encapsulation by including two **encapsulation** commands under the same **tunnel-interface** command. On the remote Cisco IOS XE Catalyst SD-WAN device, you must configure the same tunnel encapsulation type or types so that the two routers can exchange data traffic. Data transmitted out of an IPsec tunnel can be received only by an IPsec tunnel, and data sent on a GRE tunnel can be received only by a GRE tunnel. The Cisco Catalyst SD-WAN software automatically selects the correct tunnel on the destination Cisco IOS XE Catalyst SD-WAN device.