Configure Layer 3 TLOC Extension

Contents

Introduction

This document describes how to configure TLOC-Extension Layer 3(L3) on a Software-Defined Wide Area Network (SD-WAN).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

•   SD-WAN general overview
•   Templates
•   TLOC-extension
•   Routing Protocols

Components Used

The information in this document is based on these software and hardware versions:

•   Cisco vManage Release 20.7.x or later
•   vManage Version 20.7.2
•   vBond Version 20.7.2
•   vSmart Version 20.7.2
•   Integrated Service Routers (ISR)4451/K9 Version 17.7.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background

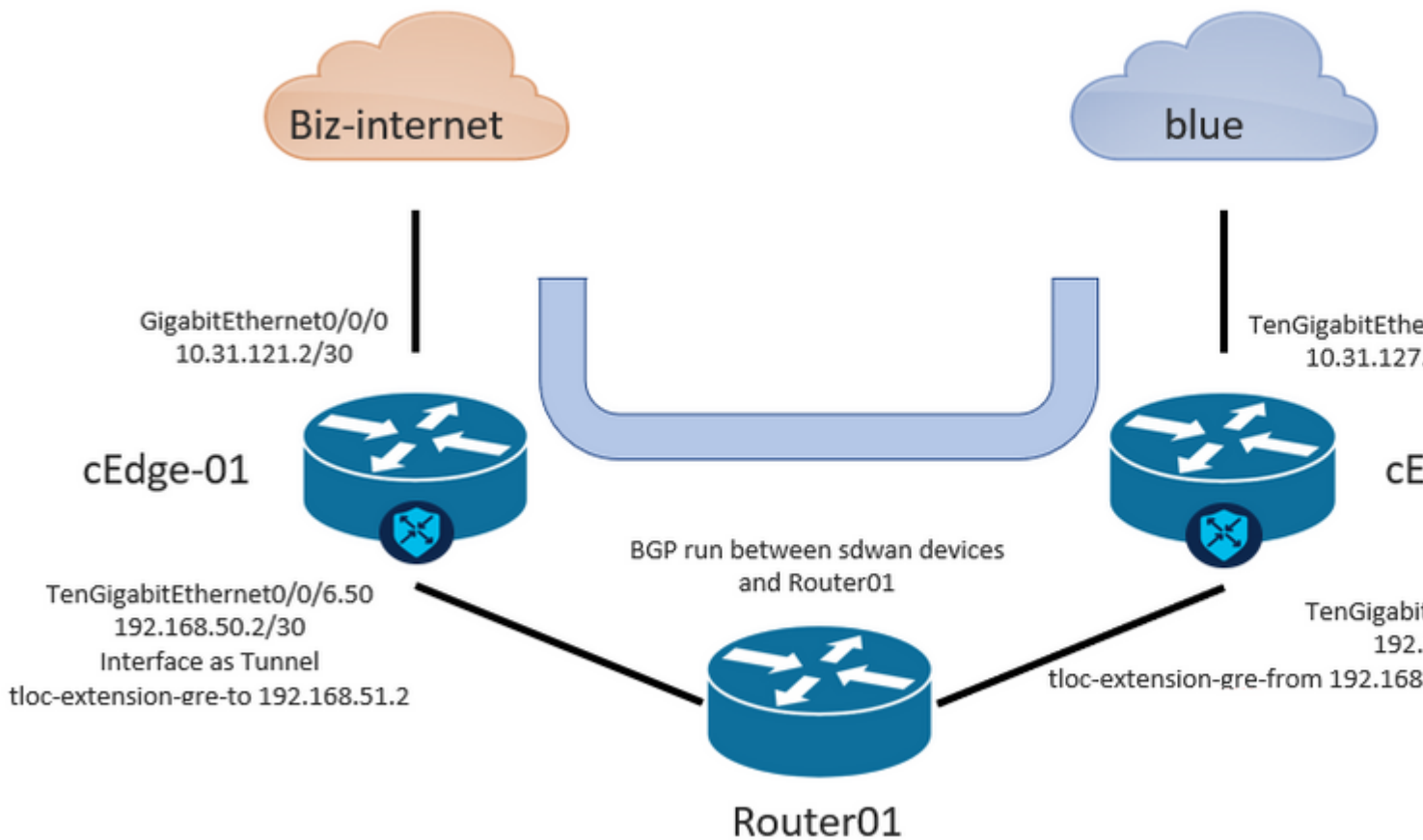The TLOC extension allows a WAN Edge router to:

•   Communicate over the WAN transport (connected to the adjacent WAN Edge router) through a TLOC-extension interface
•   Extend the TLOC to have redundancy on transport side.

There are two ways to configure TLOC Extension:

- Via L2
  - Connect another SD-WAN router at the same physical site
- Via L3
  - Needs a router with L3 capabilities used to configure any routing protocol
  - Connects between SD-WAN devices and non-SD-WAN device
  - Must be via GRE tunnel to extend the TLOC

Configure

Network Diagram

Configure TLOC Extension L3 from vManage GUI

Note: Must configure a routing protocol to communicate SD-WAN devices with a non-SW-WAN device, in this example BGP is configured.

STEP 1. Configuration on cEdge-01.

1.1 Configure the Interface for TLOC-L3 connection and assign it to tunnel interface.

- In vManage GUI, Navigate **Configuration** > **Templates** > **Feature Template** > **Select Device** > **VPN Interface Ethernet** .
- Configure basic configuration of the Interface, assign an IP address, in this case, interface GigabitEthernet0/0/6.50.

- Navigate to **Tunnel** section and turn it on. Use the same color that the other SD-WAN device is used as local color, in this scenario, blue.

1.2 Enable TLOC extension statement from the device which gets the TLOC.

- Navigate to **Tunnel** > **Advance Option** > **GRE Tunnel destination IP.**

Note: The IP address must be the interface address assigned to the other SD-WAN device used for L3 connection.

Example: the IP address on cEdge-02 of interface TengigabitEthernet0/0/6.51.

BASIC CONFIGURATION

Shutdown	⊕ ▾	○ Yes	● No
Interface Name	⊕ ▾	GigabitEthernet0/0/6.50	
Description	⊘ ▾		

○ Dynamic   ● Static

IPv4 Address/ prefix-length	⊕ ▾	192.168.50.2/30	
Secondary IP Address (Maximum: 4)	⊕ Add		
DHCP Helper	⊘ ▾		
Block Non Source IP	⊘ ▾	○ Yes	● No
Bandwidth Upstream	⊘ ▾		
Bandwidth Downstream	⊘ ▾		
Auto Detect Bandwidth	⊘ ▾	○ On	● Off

TUNNEL

Tunnel Interface	⊕ ▾	● On	○ Off
Per-tunnel Qos	⊘ ▾	○ On	● Off
Color	⊕ ▾	blue ▾	

2. Enable TLOC extension statement from where the device gets the TLOC.

    Navigate to **Tunnel** > **Advance Option** > **GRE Tunnel destination IP.**

    The IP must be the IP address of interface assigned to the other SD-WAN device, which is used for L3 connection, in this case the IP address on cEdge-02 of interface TenGigabitEthernet0/0/6.51.

Advanced Options ⌄

Encapsulation		
GRE	⊘ ▾	○ On ⦿ Off
IPsec	⊘ ▾	⦿ On ○ Off
IPsec Preference	⊘ ▾	
IPsec Weight	⊘ ▾	1
Carrier	⊘ ▾	default
Bind Loopback Tunnel	⊘ ▾	
Last-Resort Circuit	⊘ ▾	○ On ⦿ Off
NAT Refresh Interval	⊘ ▾	5
Hello Interval	⊘ ▾	1000
Hello Tolerance	⊘ ▾	12
GRE tunnel destination IP	⊕ ▾	192.168.51.2

STEP 2. Configuration on cEdge-02.

2.1 In vManage GUI, Navigate to **Configuration** > **Templates** > **Feature Template** > **Select Device** > **VPN Interface Ethernet**.

> **Note**: In this interface, Tunnel must be OFF.

- Configure basic configuration of the Interface.
- Assign an IP address (TenGigabitEthernet0/0/6.51 in this case).

BASIC CONFIGURATION

Shutdown	⊕ ▾	○ Yes	● No
Interface Name	⊕ ▾	TenGigabitEthernet0/0/6.51	
Description	⊘ ▾		

○ Dynamic   ● Static

IPv4 Address/ prefix-length	⊕ ▾	192.168.51.2/30	
Secondary IP Address (Maximum: 4)	⊕ Add		
DHCP Helper	⊘ ▾		
Block Non Source IP	⊘ ▾	○ Yes	● No
Bandwidth Upstream	⊘ ▾		
Bandwidth Downstream	⊘ ▾		
Auto Detect Bandwidth	⊘ ▾	○ On	● Off

TUNNEL

Tunnel Interface	⊘ ▾	○ On	● Off

2.2 Navigate to **Advance** section and complete the information for **GRE tunnel source IP.**

> **Note**:
> - The IP address must be the interface address assigned to the other SD-WAN device used for L3 connection.
> - **xconnect** must be the WAN interface used to send traffic over the extended TLOC.

> **Example**: The IP address on cEdge-01 of interface GigabitEthernet0/0/6.50.

ADVANCED

Duplex	⊘ ▾
MAC Address	⊘ ▾
IP MTU	⊘ ▾ 1500
TCP MSS	⊘ ▾
Speed	⊘ ▾
ARP Timeout	⊘ ▾ 1200
Autonegotiation	⊘ ▾ ○ On ○ Off
Media type	⊘ ▾
TLOC Extension	⊘ ▾
Load Interval	⊘ ▾ 30 ⓘ
Tracker	⊘ ▾
ICMP/ICMPv6 Redirect Disable	⊘ ▾ ● On ○ Off
GRE tunnel source IP	⊕ ▾ 192.168.50.2
Xconnect	⊕ ▾ TenGigabitEthernet0/0/0
IP Directed-Broadcast	⊘ ▾ ○ On ● Off

Configure TlOC Extension L3 from CLI

In this section you can check how the configuration looks on CLI after template push.

Configuration on cEdge-01.

```
cEdge-01#show sdwan running-config
system
 system-ip             <system_ip>
 site-id               <site_id>
 organization-name     <organization_name>
 vbond <vbond>
!
hostname cEdge-01
!
ip route 0.0.0.0 0.0.0.0 10.31.121.1
```

```
interface GigabitEthernet0/0/0
 no shutdown
 ip address 10.31.121.2 255.255.255.252
exit
interface GigabitEthernet0/0/6
 no shutdown
 ip mtu 1504
 mtu 1504
 negotiation auto
exit
interface GigabitEthernet0/0/6.50
 no shutdown
 encapsulation dot1Q 50
 ip address 192.168.50.2 255.255.255.252
exit
interface Loopback100
 no shutdown
 ip address 10.10.10.10 255.255.255.255
exit
interface Tunnel0
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 tunnel source GigabitEthernet0/0/0
 tunnel mode sdwan
exit
interface Tunnel10101012
 no shutdown
 ip unnumbered GigabitEthernet0/0/6.50
 no ip redirects
 ipv6 unnumbered GigabitEthernet0/0/6.50
 no ipv6 redirects
 tunnel source GigabitEthernet0/0/6.50
 tunnel mode sdwan
exit
router bgp 65001
 bgp log-neighbor-changes
 bgp router-id 10.10.10.10
 neighbor 192.168.50.1 remote-as 65003
 address-family ipv4 unicast
  neighbor 192.168.50.1 activate
  network 192.168.50.0 mask 255.255.255.252
  exit-address-family
 !
sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation ipsec
   color biz-internet
   allow-service all
  exit
 exit
 interface GigabitEthernet0/0/6.50
  tunnel-interface
   encapsulation ipsec
   color blue
   tloc-extension-gre-to 192.168.51.2
  exit
exit
cEdge-01#
```

Configuration on cEdge-02.

```
cEdge-02#show sdwan running-config
system
 system-ip              <system_ip>
 site-id                <site_id>
 organization-name      <organization_name>
 vbond <vbond>
!
hostname cEdge-02
!
ip route 0.0.0.0 0.0.0.0 10.31.127.1
ip nat inside source list nat-dia-vpn-hop-access-list interface TenGigabitEthernet0/0/0 overload
interface TenGigabitEthernet0/0/0
 no shutdown
 ip address 10.31.127.2 255.255.255.252
 ip nat outside
exit
interface TenGigabitEthernet0/0/6
 no shutdown
 mtu 1504
exit
interface TenGigabitEthernet0/0/6.51
 no shutdown
 encapsulation dot1Q 51
 ip address 192.168.51.2 255.255.255.252
exit
interface Loopback200
 no shutdown
 ip address 10.200.200.200 255.255.255.255
exit
interface Tunnel0
 no shutdown
 ip unnumbered TenGigabitEthernet0/0/0
 ipv6 unnumbered TenGigabitEthernet0/0/0
 tunnel source TenGigabitEthernet0/0/0
 tunnel mode sdwan
exit
router bgp 65002
 bgp log-neighbor-changes
 bgp router-id 10.200.200.200
 neighbor 192.168.51.1 remote-as 65003
 address-family ipv4 unicast
  neighbor 192.168.51.1 activate
  network 192.168.51.0 mask 255.255.255.252
  exit-address-family
 !
sdwan
 interface TenGigabitEthernet0/0/0
  tunnel-interface
   encapsulation ipsec
   color blue
   allow-service all
   allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
```

```
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
 exit
 interface TenGigabitEthernet0/0/6.51
  tloc-extension-gre-from 192.168.50.2 xconnect TenGigabitEthernet0/0/0
 exit
cEdge-02#
```

Verify

Validation on cEdge-01.

cEdge-01 must create control connections with local TLOC (biz-internet) and TLOC Extension (blue).

```
cEdge-01L#show sdwan control connections
                                                                PEER
PEER     PEER PEER         SITE     DOMAIN PEER                 PRIV PEER
TYPE     PROT SYSTEM IP    ID       ID     PRIVATE IP           PORT PUBLIC IP
-------------------------------------------------------------------------------------
vsmart   dtls              10       1      192.168.21.34        32953 172.18.121.
vsmart   dtls              10       1      192.168.21.34        32953 172.18.121.
vbond    dtls              0        0      172.18.121.105       32853 172.18.121.
vbond    dtls              0        0      172.18.121.105       32853 172.18.121.
vmanage  dtls              10       0      192.168.28.25        32953 172.18.121.

cEdge-01#show sdwan control local-properties

                        PUBLIC        PUBLIC PRIVATE        PRIVATE
INTERFACE               IPv4          PORT   IPv4           IPv6

-------------------------------------------------------------------------------------
GigabitEthernet0/0/0          10.31.121.87   32853  10.31.121.87    ::
GigabitEthernet0/0/6.50       10.31.127.62   5063   192.168.50.2    ::
```

Troubleshoot

In case you have an issue form control connections:

Troubleshoot SD-WAN Control Connections