OMP Prefixes for IP-SGT Binding

Table 1: Feature History

Feature Name	Release Information	Description
OMP Prefixes for IP-SGT Binding	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	The OMP routes are typically present in the IOS RIB. The OMP routes aren't present in the IOS FIB containing entries that map destination IP addresses to next-hop IP addresses. The IOS FIB operates independently of the control plane, receiving the forwarding instructions from a centralized Cisco SD-WAN Controller instead of consuming the OMP routes from the IOS RIB. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the OMP prefixes get added to the IOS FIB which improves IP-SGT binding.

Information About OMP Prefixes for IP-SGT Binding

The Overlay Management Protocol (OMP) routes refer to the routes learned and exchanged by OMP in a network overlay architecture. OMP is a routing protocol used in Cisco Catalyst SD-WAN environments that dynamically establishes and manages overlay networks. The Overlay networks are virtual networks created on top of an existing physical network infrastructure.

OMP is a proprietary protocol running on Cisco IOS XE Catalyst SD-WAN device and Cisco SD-WAN Controllers and shares routing information such as the virtual network addresses, next-hop information, and

any policy or quality-of-service requirements to Cisco IOS XE Catalyst SD-WAN devices from Cisco SD-WAN Controllers.

IOS Forwarding Information Base (FIB) is a data structure used by Cisco IOS to store information about how to forward packets in a network. The FIB contains entries that map destination IP addresses to next-hop IP addresses, allowing routers to efficiently determine where to send packets based on their destination. The FIB is used in the forwarding process to make forwarding decisions and gets updated dynamically as the network topology changes. While the IOS FIB handles the forwarding decisions for IP packets in the physical network, the OMP routes establishe and maintains connectivity within the virtual overlay network. Therefore, the IOS FIB entries don't contain OMP routes, or the need for OMP route information didn't arise until the introduction of Security Group Tag (SGT) propagation with Cisco TrustSec Integration in Cisco IOS XE Catalyst SD-WAN Release 17.3.1a. For more information, see SGT propagation with Cisco TrustSec Integration.

Note Adding the OMP routes in IOS FIB is mandatory for SGT binding because it allows for the enforcement of security policies based on SGTs in a network.

In the SD-WAN mode, the OMP routes are present in the Routing Information Base (IOS RIB). In Cisco IOS, IOS RIB stands for a database residing in the memory of a Cisco router or switch. The IOS RIB contains information about routes learned from different routing protocols, static routes, and directly connected networks. In the SD-WAN mode, the control plane handles the packet forwarding. The IOS RIB stores all the routes learned during packet transfer, while the control plane stores the packet forwarding information.

The OMP routes aren't downloaded directly into the IOS FIB from the IOS RIB because of the way Cisco Catalyst SD-WAN architecture handles routing and forwarding. The IOS FIB is designed to work independently of the control plane. It doesn't directly consume the routes from the IOS RIB. Instead, it receives forwarding instructions from a centralized Cisco SD-WAN Controller. The Cisco IOS XE Catalyst SD-WAN devices receive these forwarding instructions from the Cisco SD-WAN Controller and program their local forwarding tables, which could include the IOS FIB. Therefore, while the OMP routes exist in the IOS RIB, they aren't directly downloaded into the IOS FIB. Instead, the Cisco SD-WAN Controller determines the appropriate forwarding paths and instructs the devices accordingly. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, OMP prefixes get added to the IOS FIB. Cisco Catalyst SD-WAN considers the route with OMP prefixes as a **CTS route**. The CTS route contains the OMP prefix, the length, and the associated SGT value. When the OMP prefixes get added to the OMP routes, it means that the OMP routes are now associated with specific IP address prefixes, further strengthening the IP-SGT binding.

Restrictions of OMP Prefixes for IP-SGT Binding

- In the autonomous mode, the IP-SGT binding allows for the enforcement of multicast route policies using the Security Group Access Control List (SGACL). However, starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the ability to add OMP prefixes to IP-SGT binding for multicast routes is no longer supported.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the support for adding OMP prefixes to IP-SGT binding is not available on SD-WAN OMP routes and SD-WAN NAT routes, which are the two types of SD-WAN routes for Direct Internet Access (DIA).
- Adding OMP prefixes to IP-SGT binding is not supported on multitenant Cisco IOS XE Catalyst SD-WAN devices.

Benefits of OMP Prefixes for IP-SGT Binding

- In Cisco TrustSec, switches, routers, and firewalls examine Security Group Tags (SGTs) to classify user/device groups and enforce traffic policies. When it comes to Cisco IOS XE Catalyst SD-WAN egress, the Cisco IOS XE Catalyst SD-WAN device maps the destination IP address to a SGT mapping and performs a lookup for the destination SGT. These mappings can be received through Security Group Exchange Protocol (SXPs), OMP, or static configuration. Once the SGT is identified, the Cisco IOS XE Catalyst SD-WAN device enforces Security Group Access Control Lists (SGACLs) using downloaded or static SGACLs. The enforcement can occur at the branch site or the data center (DC) headend, depending on the deployment configuration. The SGACL ensures that traffic complies with the designated policies associated with the corresponding SGT, enhancing network security and control.

  Adding OMP prefixes to the SGTs enforces SGT based security policies to the overlay traffic.This can be enforced at a branch or at the headend. The SGT based security policy can be enforced on the DIA traffic. Adding OMP prefixes to the SGTs enables binding to the overlay prefixes as well.

- With OMP prefixes in the IOS FIB, the forwarding instructions received from the centralized Cisco SD-WAN Controller can be more accurate and specific, resulting in optimized routing and improved network performance.

- Adding the OMP prefixes provides greater flexibility in managing and controlling traffic within the Cisco Catalyst SD-WAN environment, enabling efficient utilization of network resources.

- The current FIB infrastructure allows OMP and CTS route information to exist together in routing entries. This information is accessible to the shim layer through the HW-API interface.

Configure OMP Prefixes for IP-SGT Binding Using Cisco SD-WAN Manager

The following are the three ways to configure OMP prefixes for IP-SGT Binding using Cisco SD-WAN Manager.

- Use SXP to propagate SGTs across network devices if your hardware does not support inline tagging. Using Cisco Identity Services Engine (ISE), create an IP-to-SGT binding (Dynamic IP-SGT) and download IP-SGT binding using SXP to a Cisco IOS XE Catalyst SD-WAN device for propagation of SGT over the Cisco Catalyst SD-WAN network. See Configure SXP for Dynamic IP-SGT Binding Using Cisco SD-WAN Manager.

- Alternatively, there's an option to manually configure IP-SGT binding (Static IP-SGT) and then push the configuration to a Cisco IOS XE Catalyst SD-WAN device using a CLI Add-On template to propagate SGT over the Cisco Catalyst SD-WAN network. See Configure Static IP-SGT Binding Using Cisco SD-WAN Manager.

Note Ensure that you enter the right **Peer IP** address and **Source IP** while creating a new SXP connection.

Note For more information on the SGT propagation options using Cisco SD-WAN Manager , and the LAN to WAN and WAN to LAN behavior see, SGT Propagation options.

- When the Cisco SD-WAN Controller establishes a connection to Cisco ISE, it obtains the IP-to-username and user-to-user-group mappings from Cisco ISE and Cisco pxGrid. The Cisco SD-WAN Controller subsequently pushes the identity mapping information containing IP-to-username to user-group mapping to the Cisco IOS XE Catalyst SD-WAN devices. The identity mapping information is used when creating firewall policies in Cisco SD-WAN Manager. For information on creating identity-based firewall policies, see Configure Cisco SD-WAN Identity-Based Firewall Policy.

Monitor OMP Prefixes for IP-SGT Binding Using the CLI

Monitor the Next-hop info

The command **show ip cef vrf detail** displays detailed information about the Cisco Express Forwarding (CEF) table for a specific Virtual Routing and Forwarding (VRF) instance. When OMP routes are advertised, they include next-hop information that indicates the IP address of the remote system from which the OMP route was learned. This next-hop information helps in determining the path to reach the destination network.

The following is a sample output from the **show ip cef vrf detail** command:

```
Device# show ip cef vrf 1 172.16.255.112/32 detail
172.16.255.112/32, epoch 0, flags [SDWAN], per-destination sharing
  Covered dependent prefixes: 1
    notify cover updated: 1
  nexthop 172.16.255.11 Sdwan-system-intf
  nexthop 172.16.255.21 Sdwan-system-intf
```

The example displays the OMP route containing the next-hop information attached with a remote system IP along with a SD-WAN flag set. By flagging routes as SD-WAN routes, the network infrastructure can distinguish them from other types of routes and treat them differently based on the requirements and policies of the Cisco Catalyst SD-WAN deployment.

Monitor the CTS Route Inheriting the OMP Route

The CTS routes that inherit OMP routes will include next-hop information indicating the IP address of the remote system from which the OMP route information was learned. This next-hop information helps routers determine the path to reach the destination network associated with the CTS route. The CTS routes that inherit the OMP routes will also have the SD-WAN flag set. The SD-WAN flag indicates that these routes are part of the SD-WAN infrastructure and are specifically designated for use within the Cisco Catalyst SD-WAN framework. The inherited flag is set to true for the CTS routes. The inherited flag signifies that the CTS route inherits the route information from the OMP route. It indicates that the CTS route is derived from the OMP route and carries forward the properties of the original OMP route.

The following is a sample output from the **show ip cef vrf detail**

```
Device# show ip cef vrf 1 10.2.2.0/24 detail
10.2.2.0/24, epoch 0, flags [cover dependents, SDWAN]
  Covered dependent prefixes: 1
```

```
    notify cover updated: 1
  nexthop 172.16.255.11 Sdwan-system-intf

vm5#show run | i cts
cts role-based sgt-map vrf 1 10.2.2.1 sgt 10

vm5#show ip cef vrf 1 10.2.2.1/32 detail
10.2.2.1/32, epoch 0, flags [subtree context, SDWAN]
  SC owned,sourced: FIB_SC: RBAC - [SGT 10 S D]
  1 IPL source [active source]
    Dependent covered prefix type inherit, cover 10.2.2.0/8
  recursive via 10.2.2.0/24
    nexthop 172.16.0.0 Sdwan-system-intf
```

Note The CTS routes that inherit OMP routes will have Internet Protocol Layer (IPL) as the source. This indicates that the route information originates from the IP layer of the network protocol stack.

Monitor the OMP Route Inheriting the CTS Route

Monitor the OMP route inheriting the CTS route using **show ip route vrf**.

The following is a sample output from the **show ip route vrf** command:

```
Device#  show ip route vrf 1 10.2.2.0
Routing Table: 1
Routing entry for 10.2.2.0/24
  Known via "omp", distance 251, metric 0, type omp
  Redistributing via ospf 1
  Advertised by ospf 1 subnets
  Last update from 172.16.0.0 on Sdwan-system-intf, 00:33:31 ago
  Routing Descriptor Blocks:
  * 172.16.255.11 (default), from 172.16.255.11, 00:33:31 ago, via Sdwan-system-intf
      Route metric is 0, traffic share count is 1
Device#  show run | i cts
cts role-based sgt-map vrf 1 10.2.0.0/16 sgt 16

Device#  sho ip cef vrf 1 10.2.2.0/24 detail
10.2.2.0/24, epoch 0, flags [cover dependents, subtree context, SDWAN]
  Covered dependent prefixes: 1
    notify cover updated: 1
  SC inherited: FIB_SC: RBAC - [SGT 16 S D]
  nexthop 172.16.0.0 Sdwan-system-intf
```

Monitor the Prefix Sourced Both from OMP and CTS Routes

When an exact prefix is sourced from both the OMP and CTS routes, the resulting route will have the next-hop information from OMP and SGT tag info from the CTS route.

The following is a sample output from the **show ip route vrf**

```
Device# show ip route vrf 1 10.2.2.0
Routing Table: 1
Routing entry for 10.2.2.0/24
  Known via "omp", distance 251, metric 0, type omp
  Redistributing via ospf 1
  Advertised by ospf 1 subnets
  Last update from 172.16.255.11 on Sdwan-system-intf, 00:39:49 ago
  Routing Descriptor Blocks:
  * 172.16.00 (default), from 172.16.255.11, 00:39:49 ago, via Sdwan-system-intf
      Route metric is 0, traffic share count is 1
```

```
Device# show run | i cts
cts role-based sgt-map vrf 1 10.2.2.0/24 sgt 24
Device# sho ip cef vrf 1 10.2.2.0/24 detail
10.2.2.0/24, epoch 0, flags [cover dependents, subtree context, SDWAN]
  Covered dependent prefixes: 1
    notify cover updated: 1
  SC owned,sourced: FIB_SC: RBAC - [SGT 24 S D]
  1 IPL source [no flags]
  nexthop 172.16.255.11 Sdwan-system-intf
```