

Configuring the SDM Template

This section details the approximate number of resources supported in each templates for a router running the license.

- Prerequisites for the SDM Template, on page 1
- Restrictions for the SDM Template, on page 1
- Information About the SDM Template, on page 3
- Selecting the SDM Template, on page 14
- Verifying the SDM Template, on page 18
- SDM Template Supported Features on RSP3 Module, on page 18
- DHCP Snooping, on page 40

Prerequisites for the SDM Template

Before using an SDM template, you must set the license boot level.

For IPv6 QoS template, the license to use should be *metroipaccess*. You can view the license level using the **show version | in License Level** command

Note If you use *advancedmetroipaccess*, then your options may vary.

Restrictions for the SDM Template

- When using the templates SR 5 label push and SR PFP together, do not use the BDI_MTU template. If the BDI_MTU template is used, then the router may crash continuously, this is applicable from release Cisco IOS XE Amsterdam 17.1.1 to Cisco IOS XE Cupertino 17.9.1. From release Cisco IOS XE Dublin 17.10.1 onwards, during such situation, the router automatically reverts the BDI_MTU template change and performs an additional reboot.
- If you do not enable the EFP feature template, then there is no traffic flow between EFP and VFI (when EFP is with Split Horizon group and VFI is default). But when you enable the EFP feature template, then there is traffic flow between EFP and VFI because of design limitations.
- You cannot edit individual values in a template category as all templates are predefined.

- You cannot use a new SDM template without reloading the router.
- SDM templates are supported only by the Metro Aggregation Services license. Use the help option of the **sdm prefer** command to display the supported SDM templates.
- A mismatch in an SDM template between an active RSP and standby RSP results in a reload of the standby RSP. During reload, SDM template of the standby RSP synchronizes with the SDM template of the active RSP.
- To revert to the current SDM template after using the **sdm prefer** command (which initiates reload of a new SDM template), you must wait for the reload to complete.
- Using the **configure replace** command which results in changes in the current SDM template is not supported.
- The supported group numbers are for scaling in uni-dimension. When scaling in multidimension, the numbers can vary as certain features may share resources.
- When scaling, features using Multiprotocol Label Switching (MPLS) are limited by the number of MPLS labels.
- Internal TCAM usage that is reserved for IPv6 is 133-135 entries. TCAM space that is allotted for SDM template is 135 entries on the router.
- EAID Exhaust occurs when two paths are MPLS and two are IP. It does not occur if all the four paths are IP.
- The following restrictions apply to the maximum IPv6 QoS ACL SDM template:
  - The number of QoS ACL class maps and policy maps that are supported depends on the maximum TCAM entries available.
  - The software solution with expansion is applicable only for maximum QoS SDM template and more than eight Layer 4-port matches are supported for the maximum QoS SDM template. For other templates, due to hardware restriction, a maximum of eight Layer 4-port operators is supported per interface.
  - Ethernet CFM, Ethernet OAM, and Y.1731 protocols are not supported. Features dependent on these protocols are impacted.
  - Layer 2 monitoring features are not supported.
  - The S-TAG based fields are not supported for classification, if IPv6 address match exists in the policy-map.
  - Only eight Layer 4 operations are supported in templates other than maximum IPv6 QoS ACL template.

Note

Release	Time	Activity
16.6.1	49-50 mins	Reload to SSO bulk Sync state
16.7.1	50 mins	Reload to SSO bulk Sync state
16.8.1	-	-
16.9.1	75 mins	Reload to SSO bulk Sync state

Information About the SDM Template

The SDM templates are used to optimize system resources in the router to support specific features, depending on how the router is used in the network. The SDM templates allocate Ternary Content Addressable Memory (TCAM) resources to support different features. You can select the default template to balance system resources or select specific templates to support the required features.

The following table shows the approximate number of each resource supported in each of the templates for a router running the Metro Aggregation Services license on RSP3.

Table 1: Approximate Number of Feature Resources Allowed by Each SDM Template (RSP3)

Functionality	Default Template (RPF)	IPv4 Template (No RPF)	IPv6 Template
MAC table	200K	200K	200K
IPv4/VPNv4 Routes	Without MPLS 32k urpf ipv4 routes + 160k ipv4 routes With MPLS 32k urpf ipv4 routes + 160k (ipv4 routes + mpls labels) MPLS Labels = 32000	Without MPLS 192k ipv4 routes With MPLS 192k (ipv4 routes + mpls labels) MPLS Labels = 32000	Without MPLS 76k ipv4 routes With MPLS 76k (ipv4 routes + mpls labels) MPLS Labels = 32000
IPv6/VPNv6 Routes	8192	8192	36864
uRPF IPv4 routes	32768	32768	32768
IPv4 mcast routes (mroutes)	4000	4000	4000
IPv6 mcast routes (mroutes)	1000	1000	1000

Functionality	Default Template (RPF)	IPv4 Template (No RPF)	IPv6 Template
Bridge Domains	4094	4094	4094
EoMPLS Tunnels	4000	4000	4000
MPLS VPN	1000	1000	1000
VRF Lite	1000	1000	1000
VPLS Instances[1]	3500	3500	3500
IPv4 ACL entries	1000 (984 user configurable)	1000 (984 user configurable)	1000 (984 user configurable)
IPv6 ACL entries	128 (124 user configurable)	128 (124 user configurable)	128 (124 user configurable)
v4 QOS Classifications	16000	16000	16000
v6 QoS Classifications	NS	NS	NS
Egress policers per ASIC	NS	NS	NS
OAM sessions	1000	1000	1000
IPSLA sessions	1000	1000	1000
EFP	16000	16000	16000
Maximum VLANs per port	4,000 per ASIC	4,000 per ASIC	4,000 per ASIC
Maximum VPLS neighbors	64	64	64
Maximum attachment circuit per BD	64	64	64
STP Instances	16	16	16
Maximum Etherchannel groups	48	48	48
Maximum Interfaces per Etherchannel groups	8	8	8
Maximum VRRP per system	255	255	255
Maximum HSRP per system	255	255	255
Maximum Ingress MPLS labels	32000	32000	32000

Functionality	Default Template (RPF)	IPv4 Template (No RPF)	IPv6 Template
Maximum FRR/TE Headend	500	500	500
Maximum FRR/TE Midpoints	5000	5000	5000
Maximum E-LMI sessions	128	128	128
Maximum BFD sessions	1023	1023	1023
Maximum SPAN/RSPAN sessions	10	10	10
Maximum Queue counters per ASIC/system	40000/48000	40000/48000	40000/48000
Maximum Policer counters per ASIC/system	12000/24000	12000/24000	12000/24000
Max BDI for L3	1000	1000	1000
Multicast OIF per group for VF Lite or mVPN	255	255	255
Multicast OIF per group for native multicast	255	255	255
Queues per ASIC/system	40000/48000	40000/48000	40000/48000
Max Queues per EFP	8	8	8
Ingress Classifications	16000	16000	16000
Egress Classifications	48000	48000	48000
Max Ingress Policers per ASIC/system	12000/24000	12000/24000	12000/24000
Max Egress Policers per ASIC/system	NS	NS	NS
Maximum EFPs per BD	256	256	256
Maximum number of BDI for PW	128	128	128
Maximum Layer 3 interfaces	1000	1000	1000
Max REP segments	NS	NS	NS
Maximum class-maps	1000	1000	1000

Functionality	Default Template (RPF)	IPv4 Template (No RPF)	IPv6 Template
Maximum policy maps	1000	1000	1000
Max number of OSPF Neighbors	400	400	400
Max number of ISIS neighbors	400	400	400
Max number of ISIS instances	30	30	30
Max number of BGP neighbors	250	250	250
Max number IEEE 802.1ag/Y.1731(CFM) instances at 1sec for xconnect	1000	1000	1000
Max number IEEE 802.1ag/Y.1731(CFM) instances at 3.3 ms for BD & xconenct	1000	1000	1000
Max number IEEE 802.1ag/Y.1731(CFM) instances at 100 ms for BD & xconnect	1000	1000	1000
Max number IEEE 802.1ag/Y.1731(CFM) instances at 1Sec for BD	1000	1000	1000
Max number of Y.1731 instances	1000	1000	1000
Maximum Class-maps in policy-map	512	512	512
Max number of match statements per class-map	16	16	16
Max number of BFD sessions at 3.3ms	1023	1023	1023
Max number of BFD sessions at 100ms	1023	1023	1023
Max number of BFD sessions at 1S	1023	1023	1023

Functionality	Default Template (RPF)	IPv4 Template (No RPF)	IPv6 Template
Max number of IGP Prefixes protected via LFA-FRR	1500	1500	1500
Max number of L3VPN Prefixes protected via LFA-FRR	4000	4000	4000
Max number of L2VPN sessions protected via LFA-FRR	2000	2000	2000

[1] From release 16.7.x the VPLS backup PW feature is supported, so if VPLS instance is configured then the maximum VPLS session is limited to 1000 instead of 3500.

The following table shows the approximate number of each resource supported in each of the templates for a router running the Metro Aggregation Services license on RSP2.

Table 2: Approximate Number of Feature Resources Allowed by Each SDM Template (RSP2)

Resource	Default Template	Video Template	IP Template	Maximum IPv6 QoS Template
MAC table	16000	16000	16000	16000
Virtual local area network (VLAN) mapping	4000	4000	65536	4000
IPv4 routes[2]	20000	12000	24000	20000
IPv6 routes	3962	3962	1914	3962
VPNv4 routes[3]	20000	12000	24000	20000
VPNv6 routes	3962	3962	1914	3962
IPv4 multicast routes (mroutes)	1000	2000	1000	1000
Layer 2 multicast groups[4]	NA	NA	NA	NA
Bridge Domains (BD)	4000	4000	4000	4000
MAC-in-MAC	0	0	0	0
Ethernet over MPLS (EoMPLS) tunnels	2000	2000	2000	2000

Resource	Default Template	Video Template	IP Template	Maximum IPv6 QoS Template
MPLS Virtual Private Network (VPN)	128	128	128	128
Virtual Routing and Forwarding (VRF) lite	128	128	128	128
Virtual Private LAN Services (VPLS) instances	2000	2000	2000	2000
Access Control List (ACL) entries[5]	2000	4000	2000	2000
Queues per Application-Specific Integrated Circuit (ASIC) [6]	4095	4095	4095	4095
IPv4 Quality of Service (QoS) classifications	4096	2048	4096	4096
Policers	4096	4096	4096	4096
Ethernet Operations, Administration, and Maintenance (OAM) sessions	1000	1000	1000	0
IP Service Level Agreements (IPSLA) sessions	1000	1000	1000	1000
Ethernet Flow Point (EFP)	8000	8000	8000	8000
Maximum VLANs per port	4094	4094	4094	4094
Maximum I-TAG per system	500	500	500	500
Maximum VPLS neighbors	64	64	64	64
Maximum attachment circuit per BD	128	128	128	128
STP Instances	16	16	16	16

Resource	Default Template	Video Template	IP Template	Maximum IPv6 QoS Template
Maximum Etherchannel groups	64	64	64	64
Maximum Interfaces per Etherchannel groups	8	8	8	8
Maximum Hot Standby Router Protocol (HSRP)	128 (For Cisco IOS-XE Release 3.14 and earlier) 256 (For Cisco IOS-XE Release 3.15 and later)	128 (For Cisco IOS-XE Release 3.14 and earlier) 256 (For Cisco IOS-XE Release 3.15 and later)	128 (For Cisco IOS-XE Release 3.14 and earlier) 256 (For Cisco IOS-XE Release 3.15 and later)	128 (For Cisco IOS-XE Release 3.14 and earlier) 256 (For Cisco IOS-XE Release 3.15 and later)
Maximum Virtual Router Redundancy Protocol (VRRP)	128 (For Cisco IOS-XE Release 3.14 and earlier) 255 (For Cisco IOS-XE Release 3.15 and later)	128 (For Cisco IOS-XE Release 3.14 and earlier) 255 (For Cisco IOS-XE Release 3.15 and later)	128 (For Cisco IOS-XE Release 3.14 and earlier) 255 (For Cisco IOS-XE Release 3.15 and later)	128 (For Cisco IOS-XE Release 3.14 and earlier) 255 (For Cisco IOS-XE Release 3.15 and later)
Maximum Ingress MPLS labels	32000	32000	32000	32000
Maximum Egress MPLS labels	28500	28500	28500	28500
Maximum Fast Reroute (FRR)/Traffic Engineering (TE) headend	500	500	500	500
Maximum FRR/TE midpoints	5000	5000	5000	5000
Maximum Enhanced Local Management Interface (E-LMI) sessions	1000	1000	1000	1000
Maximum Bidirectional Forwarding Detection (BFD) sessions	1023	1023	1023	1023

Resource	Default Template	Video Template	IP Template	Maximum IPv6 QoS Template
Maximum Switched Port Analyzer (SPAN)/Remote SPAN (RSPAN) sessions	32	32	32	32
Maximum Queue counters (packet & byte)	65536	65536	65536	65536
Maximum Policer counters (packet & byte)	49152	49152	49152	49152
Maximum number of BDI for Layer 3	1000	1000	1000	1000
IPv6 ACL	1000	1000	1000	2000
IPv6 QoS classification	4096	4096	4096	4096
Maximum Number of Layer 4 Source/Destination matches per interface [7]	8	8	8	NA

[2] Using IPv4 and VPNv4 routes concurrently reduces the maximum scaled value as both the routes use the same TCAM space.
[3] Due to label space limitation of 16000 VPNv4 routes, to achieve 24000 VPNv4 routes in IP template use per VRF mode.
[4] Using Layer 2 and Layer 3 multicast groups concurrently reduces the scale number to 1947.
[5] ACLs contend for TCAM resources with Multicast Virtual Private Network (MVPN).
[6] User available queues are 1920.
[7] TCAM consumption for IPv6 Qos ACL Layer 4 port match operations increase with Maximum IPv6 Qos SDM template.

The following table shows the approximate number of each resource supported in each of the templates for a router running the Metro Aggregation Services license on RSP1A.

Table 3: Approximate Number of Feature Resources Allowed by Each SDM Template (RSP1A)

Resource	IP template	Video template
MAC table	16000	16000
Virtual local area network (VLAN) mapping	4000	4000
IPv4 routes[8]	24000	12000

Resource	IP template	Video template
IPv6 routes[9]	4000	4000
VPNv4 routes[10]	24000	12000
VPNv6 routes	4000	4000
IPv4 multicast routes (mroutes)	1000	2000
Layer 2 multicast groups[11]	1000	2000
Bridge Domains (BD)	4094	4094
MAC-in-MAC	0	0
Ethernet over MPLS (EoMPLS) tunnels	512	512
MPLS Virtual Private Network (VPN)	128	128
Virtual Routing and Forwarding (VRF) lite	128	128
Virtual Private LAN Services (VPLS) instances	26	26
Access Control List (ACL) entries[12]	2000	4000
Queues per Application-Specific Integrated Circuit (ASIC) [13]	2048	2048
IPv4 Quality of Service (QoS) classifications	4096	2048
Policers	1024	1024
Ethernet Operations, Administration, and Maintenance (OAM) sessions	1000	1000
IP Service Level Agreements (IPSLA) sessions	1000	1000
Ethernet Flow Point (EFP)	4000	4000
Maximum VLANs per port	4094	4094
Maximum I-TAG per system	500	500
Maximum VPLS neighbors	62	62
Maximum attachment circuit per BD	62	62
STP Instances	16	16
Maximum Etherchannel groups	26	26

Resource	IP template	Video template
Maximum Interfaces per Etherchannel groups	8	8
Maximum Hot Standby Router Protocol (HSRP)/Virtual Router Redundancy Protocol (VRRP)	128	128
Maximum Ingress MPLS labels	16000	16000
Maximum Egress MPLS labels	28500	28500
Maximum Fast Reroute (FRR)/Traffic Engineering (TE) headend	512	512
Maximum FRR/TE midpoints	5000	5000
Maximum Enhanced Local Management Interface (E-LMI) sessions	1000	1000
Maximum Bidirectional Forwarding Detection (BFD) sessions	511	511
Maximum Switched Port Analyzer (SPAN)/Remote SPAN (RSPAN) sessions	32	32
Maximum Queue counters (packet & byte)	65536	65536
Maximum Policer counters (packet & byte)	49152	49152
Maximum number of BDI for Layer 3	256	256
IPv6 ACL	1000	1000
IPv6 QoS classification	4096	2048

[8] Using IPv4 and VPNv4 routes concurrently reduces the maximum scaled value as both the routes use the same TCAM space.
[9] User available routes are 3967.
[10] Due to label space limitation of 16000 VPNv4 routes, to achieve 24000 VPNv4 routes in IP template use per VRF mode.
[11] Using Layer 2 and Layer 3 multicast groups concurrently reduces the scale number to 1947.
[12] ACLs contend for TCAM resources with Multicast Virtual Private Network (MVPN).
[13] User available queues are 1920.

The following table shows the approximate number of each resource supported in each of the templates for a router running the Metro Aggregation Services license on RSP1B.

Table 4: Approximate Number of Feature Resources Allowed by Each SDM Template (RSP1B)

Resource	VPNv4/v6 template	Video template
MAC table	256000	256000
IVLAN mapping	4000	4000
EVLAN mapping	4000	4000
Maximum VLANS per port	4094	4094
Maximum security addresses per EFP	1000	1000
Maximum security addresses per BD	10000	10000
Maximum security addresses	256000	256000
Maximum security configuration addresses	256000	256000
EFPs per BD	62	62
IPv4 routes	80000	80000
IPv6 routes	40000	8000
Maximum BD interfaces	1000	1000
Maximum ITAG per system	500	500
IPv4 routing groups[14]	2000	8000
IPv6 routing groups[15]	2000	8000
IPv4 multicast groups[16]	2000	10000
IPv6 multicast groups[17]	2000	10000
BDs	4000	4000
MAC-in-MAC	0	0
EoMPLS tunnels	8000	8000
MPLS VPN	1000	1000
Virtual Routing and Forwarding Scale (VRFS)	1000	1000
VPLS instances	2000	2000
Maximum VPLS neighbors	62	62
ACL entries	4000	4000
IPv6 ACL entries	1000	1000
Queues per ASIC	16384	16384
Classifications	12288	12288
Ingress policers per ASIC	8192	8192

Resource	VPNv4/v6 template	Video template
Egress policers per ASIC	4096	4096
Maximum class maps	4096	4096
Maximum policy maps	1024	1024
Maximum queue counters	65536	65536
Maximum policer counters	48152	48152
OAM sessions	4000	4000
ELMI sessions	1000	1000
SLA sessions	1000	1000
EFPs	8000	8000
MPLS ingress labels	64000	64000
MPLS egress labels	80000	80000
FRR TE headend	1000	1000
FRR TE midpoints	7000	7000
STP instances	128	128
BFD sessions	511	511
HSRP VRRP sessions	256	256
Maximum EC groups	16	16
Maximum interfaces per EC groups	8	8
Maximum SPAN RSPAN sessions	32	32
IPv4 tunnel entries	1000	1000
Maximum VPNv4 and VPNv6 pre-fixes[18]	64000	64000

[14] Overall multicast groups in video template can be scaled to 8000 individually or in combination with other multicast features. For example: IPv4 routing groups can be scaled to 8000 or IPv4 routing groups and IPv6 routing groups together can be scaled to 8000.
[15] See footnote 7.
[16] See footnote 7.
[17] See footnote 7.
[18] VPNv4 and VPNv6 together can be scaled up to 64000 in per-prefix mode.

Selecting the SDM Template

To select an SDM template, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**sdm prefer** {**default** | **video** | **ip** | **mvpn_rsp1a** | **VPNv4/v6** | **max-ipv6-acl** | **enable_4x_priority** | **enable_copp** | **enable_acl_copp** | **ipv4** | **ipv6** | **efp_feat_ext** | **enable_8k_efp** | | **enable_bdi_mtu** | **enable_copp** | **enable_l3vpn_cm** | **enable_color_blind_policer** | **enable_l3vpn_cm** | **enable_match_inner_dscp** | **enable_portchannel_qos_multiple_active** | **vpls_stats_enable** | **enable_dhcp_snoop** | **enable_hitless_switching** | **enable_l2pt_fwd_all** | **enable_l3vpn_cm** | **enable_latching_loopback** | **enable_multicast_stats** | **enable_qos_scale** | **enable_tdm_to_ip_iw** | **enable_vlan_translation** | **ipv4ipv4_ipv6** | **ipv6** | **no_efp_feat_ext** | **sr_5_label_push_enable** | **sr_pfp_enable**} **Example:** `Router(config)# sdm prefer default`	Specifies the SDM template to be used on the router. • default—Balances all functions. • video—Increases multicast routes and ACLs. • mvpn_rsp1a—Supports MVPN. This option is available only on RSP1A. • VPNv4/v6—Increases IPv4/VPNv4 routes. This option is available only on RSP1B. • max-ipv6-acl—Supports IPv6 QoS ACL routes. The NEQ Layer 4 operation is supported in maximum IPv6 QoS ACL template. • ipv4—Enables the IPv4 template. This is supported on the RSP3 module. • ipv6—Enables the IPv6 feature template. This is supported on the RSP3 module. • efp_feat_ext—Enables the EFP feature template. This is supported on the RSP3 module. • enable_8k_efp—Enables the 8K EFP feature template. This is supported on the RSP3 module. • enable_bdi_mtu—Enables the BDI MTU feature template. This is supported on the RSP3 module. • enable_4x_priority—Enables the 4x Priority feature template. This is supported on the RSP3 module.

	Command or Action	Purpose
		• enable_copp—Enables the COPP feature template. This is supported on the RSP3 module. • enable_acl_copp—Enables the COPP ACL feature template. This is supported on the RSP3 module. • enable_l3vpn_cm—Enables the L3VPN conditional marking feature template. This is supported on the RSP3 module. • enable_color_blind_policer—Enables the Color Blind Policer feature template. This is supported on the RSP3 module. • enable_match_inner_dscp—Enables the match inner dscp feature template. This is supported on the RSP3 module. • enable_portchannel_qos_multiple_active—Enables the port channel QoS multiple active feature template. This is supported on the RSP3 module. • vpls_stats_enable—Enables the VPLS statistics feature template. This is supported on the RSP3 module. • enable_dhcp_snoop—Allows the DHCP traffic which ingress on the cross-connect service instance to be forwarded in the data plane, whereas the Bridge Domain (BD) service instance frames should be trapped to CPU to support the DHCP Option 82. • enable_hitless_switching—Enables the Hitless Switching feature template. This is supported on the RSP3 module. • enable_l2pt_fwd_all—Enables the L2PT forward All feature template. This is supported on the RSP3 module. • enable_l3vpn_cm—Enables the L3VPN CM feature template. This is supported on the RSP3 module. • enable_latching_loopback—Enables the Latching Loopback feature template. This is supported on the RSP3 module.

	Command or Action	Purpose
		• enable_multicast_stats —Enables the Multicast Stats feature template. This is supported on the RSP3 module. • enable_qps_scale—Enables the Qos Scale feature template. This is supported on the RSP3 module. • enable_tdm_to_ip_iw—Enables the TDM to IP IW feature template. This is supported on the RSP3 module. • enable_vlan_translation—Enables the VLAN Translation feature template. This is supported on the RSP3 module. • ipv4—Enables the IPv4 feature template. This is supported on the RSP3 module. • ipv4_ipv6—Enables the IPv4_IPv6 feature template. This is supported on the RSP3 module • ipv6—Enables the IPv6 feature template. This is supported on the RSP3 module. • no_efp_feat_ext—Enables the No EFP FEAT EXT feature template. This is supported on the RSP3 module. • sr_5_label_push_enable —Enables the SR 5 labels Push feature template. This is supported on the RSP3 module. • sr_pfp_enable—Enables the SR PFP feature template. This is supported on the RSP3 module. **Note** When changing the SDM template, the router waits for two minutes before reloading. Do not perform any operation till the router reloads. **Note** For the new SDM template to take effect, you must save and reload the new configuration, otherwise the current SDM template is retained. **Note** For more information, see Supported SDM Template.

	Command or Action	Purpose

Step 4	**sdm prefer enable_vlan_translation**
	Example:
	`sdm prefer enable_vlan_translation`
	
	`Router(config)#sdm prefer enable_vlan_translation`
	`Standby is reloaded, it will come up with init required for new template`
	`once standby comes up`
	`Please trigger SSO`
	`Changes to VLAN Translation template stored`
		Enables VLAN Translation on the Cisco RSP3 module.

Step 5	**sdm prefer disable_vlan_translation**
	Example:
	`sdm prefer disable_vlan_translation`
	
	`Router(config)#sdm prefer disable_vlan_translation`
	`Standby is reloaded, it will come up with init required for new template`
	`once standby comes up`
	`Please trigger SSO`
	`Changes to VLAN Translation template stored`
		Disables VLAN Translation on the Cisco RSP3 module.

Verifying the SDM Template

You can use the following **show** commands to verify configuration of your SDM template:

- **show sdm prefer**—Displays the resource numbers supported by the specified SDM template.

SDM Template Supported Features on RSP3 Module

This section details the supported SDM template features on the RSP3 module. The sdm prefer command provides the follwing templates:

Table 5: SDM Templates and Supported Features

SDM Template	Supported Feature
sdm prefer vpls_stats_enable	VPLS Statistics
sdm prefer efp_feat_ext	Split-Horizon Groups
sdm prefer enable_8k_efp	8K EFP (4 Queue Model)
sdm prefer enable_match_inner_dscp	Match Inner DSCP

SDM Template	Supported Feature
sdm prefer enable_copp	Control Plane Policing
sdm prefer enable_portchannel_qos_multiple_active	QoS Support on Port Channel LACP Active Active 16K EFP Support on Port Channel
sdm prefer ipv4_ipv6	Enhance uRPF scale to 32K
sdm prefer enable_vlan_translation	VLAN Translation for RSP3
sdm prefer enable_hitless_switching	Hitless Switching on C37.94 Interface Module

VPLS Statistics

VPLS statistic feature supports packet and byte count in ingress and egress directions. The following are the required criteria to enable this feature:

- Metro Aggregation services license
- Special SDM template

  Use the following commands to enable or disable VPLS statistics feature:

```
sdm prefer vpls_stats_enable
sdm prefer vpls_stats_disable
```

After template configuration, the node is auto reloaded.

Restrictions

- EFP statistics is not supported when VPLS statistics is enabled.
- Transit packet drops data is not supported.
- There is a sync time of 10 seconds between the software and the hardware for fetching the statistics.
- If access rewrite is configured (pop 1), VC statistics show 4 bytes less than the actual size (in both imposition and disposition node) because pop 1 removes the VLAN header.
- VC statistics do not account LDP and VC label. It displays what is received from access in both imposition and disposition node.

Example

The following example shows a sample VPLS Statics counter output:

```
router#show mpls l2transport vc 2200 detail

Local interface: Gi0/14/2 up, line protocol up, Ethernet:100 up
  Destination address: 10.163.123.218, VC ID: 2200, VC status: up
    Output interface: Te0/7/2, imposed label stack {24022 24025}
    Preferred path: not configured
    Default path: active
    Next hop: 10.163.122.74
  Create time: 20:31:49, last status change time: 16:27:32
    Last label FSM state change time: 16:27:44
  Signaling protocol: LDP, peer 10.163.123.218:0 up
    Targeted Hello: 10.163.123.215(LDP Id) -> 10.163.123.218, LDP is UP
```

```
  Graceful restart: configured and enabled
  Non stop routing: configured and enabled
  Status TLV support (local/remote)   : enabled/supported
    LDP route watch                   : enabled
    Label/status state machine        : established, LruRru
    Last local dataplane   status rcvd: No fault
    Last BFD dataplane     status rcvd: Not sent
    Last BFD peer monitor  status rcvd: No fault
    Last local AC  circuit status rcvd: No fault
    Last local AC  circuit status sent: No fault
    Last local PW i/f circ status rcvd: No fault
    Last local LDP TLV     status sent: No fault
   Last remote LDP TLV    status rcvd: No fault
    Last remote LDP ADJ    status rcvd: No fault
  MPLS VC labels: local 110, remote 24025
  Group ID: local 40, remote 67109248
  MTU: local 9000, remote 9000
  Remote interface description: TenGigE0_0_2_3.2200
Sequencing: receive disabled, send disabled
Control Word: Off (configured: autosense)
SSO Descriptor: 10.163.123.218/2200, local label: 110
Dataplane:
  SSM segment/switch IDs: 16911/90633 (used), PWID: 71
VC statistics:
  transit packet totals: receive 100, send 200
  transit byte totals:   receive 12800, send 25600
  transit packet drops:  receive 0, seq error 0, send 0
```

Split Horizon Enhancements on the RSP3 Module

Starting with Cisco IOS XE Release 16.6.1, the **efp_feat_ext** template is introduced. This template when enabled allows configuration of two split-horizon groups on the EVC bridge-domain.

- Two Split-horizon groups—Group 0 and Group 1 are configured through using the **bridge-domain** *bd number* **split-horizon group** *0-1* command.

Prerequisites for Split-Horizon Groups on the RSP3 Module

- The efp_feat_ext template must be configured to enable the feature.
- Metro services license must be enabled; LICENSE_ACTIVE_LEVEL=metroaggrservices,all:ASR-903;

Restrictions for Split-Horizon Groups on the RSP3 Module

- If a VPLS VFI is part of the bridge-domain configuration, the VPLS is by default part of Split-horizon group 0 and the scale for Split-horizon group 1-2 and No group is applicable as in the Table 2.
- The overall scale of EFPs is 8K, only if the split-horizon groups are configured. For information, see supported scale.



Note If split-horizon based-EFPs aren't configured, the total EFPs supported are 4K.

- EFPs configured on the same bridge domain and same split-horizon group, can't forward to or receive traffic from each other.

- We don’t recommended configuration of Y.1564 and split-horizon group on the same EFP.
- We don’t recommend configuring MAC security with split-horizon group.
- Split-horizon group isn’t supported for CFM on this template. Configuring split-horizon groups on CFM-based MEPs may result in MEPs being unlearned, and unexpected behavior may be observed.
- If ethernet loopback is configured, and if a dynamic change in split-horizon group occurs on the EFP-BD, the ELB session must be restarted.
- A change in the split-horizon group configuration on a regular EFP results in hardware programming update and may impact L2 traffic. This results in a MAC-flush and relearn of traffic with new MAC address.

Following are known behavior of split-horizon groups:

- Changing the split-horizon group on any EFP, results in traffic flooding back to same EFP for few milliseconds.
- A small traffic leak may be observed on defaulting an interface with higher number of EFP with split-horizon configured.
- BFD flaps and underlying IGP flaps may be observed upon changing split-horizon groups, if BFD is hardware-based.

Split-Horizon Supported Scale

8K EFPs are supported across RSP3-400 and 4K EFPs on RSP3-200.



Note If the split-horizon configuration does not exist, then the number of EFPs supported are reduced to 4K EFPs prior to Cisco IOS XE 16.7 release. Starting with Cisco IOS XE 16.7, when the **efp_feat_ext** SDM template is enabled, then the maximum supported EFP scale limit is 3K per ASIC. This 3K EFP scale includes 2K EFPs without SH group and 1K EFPs (500 + 500) split between 2 SH group.

Table 6: Split-Horizon Supported Template - Cisco IOS XE 16.7 release

Split-Horizon Group	RSP3-400	RSP3-200
Default (No config)	2K EFP	2K EFP
Group 0	500 EFP	500 EFP
Group 1	500 EFP	500 EFP

Table 7: Split-Horizon Supported Template prior to Cisco IOS XE 16.7 release

Split-Horizon Group	RSP3-400	RSP3-200
Default (No config)	4K EFP	2K EFP
Group 0	2K EFP	1K EFP
Group 1	2K EFP	1K EFP

Note Port-channel scale is half the regular scale of the EFP.

Configuring Split-Horizon Group on the RSP3 Module

```
interface GigabitEthernet0/2/2
service instance 1 ethernet
  encapsulation dot1q 100
  bridge-domain 100 split-horizon group 0  □ When you configure split-horizon group 0,(0
is optional)

 interface GigabitEthernet0/2/2
service instance 2 ethernet
  encapsulation dot1q 102
  bridge-domain 102 split-horizon group 1 □ When you configure split-horizon group 1
```

8K EFP (4 Queue Model)

In Cisco IOS XE Release 3.18SP, the 8K EFP (4 Queue Model) support allows up to 8000 EFPs at the system level. EFP scale implementation follows the static model, that is, eight queues are created per EFP by default.

Information About 8000 (8K) EFP

- In default model, 5000 EFPs can be configured on Cisco NCS 4200 RSP3 module.
- The Switch Database Management (SDM) template feature can be used to configure 8000 EFPs across ASIC(4000 EFPs per ASIC interfaces).
- In 8K EFP model, each EFP consumes four Egress queues. If 8K EFP SDM template is not enabled, each EFP consumes eight Egress queues.
- Ingress policy map can specify more than eight traffic classes based on PHB matches, which remains the same. However, Egress policy map can have three user defined class and class-default class.
- Each Egress class-maps can be mapped to a single or multiple traffic classes and each class-map mapped to a single queue.
- Maximum of two queues are set to Priority according to policy configuration.
- All the existing QOS restrictions that apply in default model are also applicable to 8K EFP model.

Prerequisites for 8000 (8K) EFP

- Activate the Metro Aggregation Services license on the device.
- To configure 8000 EFPs, enable the SDM template using CLI **sdm prefer enable_8k_efp**.
- Reset the SDM template using the CLI **sdm prefer disable_8k_efp** .

Restrictions for 8000 (8K) EFP

- With the **enable_8k_efp** SDM template, shut or noshut on Port-channel (PoCH) is blocked. To make the PoCH as UP or DOWN, all the port channel member links must be either shut or noshut.

- Traffic class to Queue mapping is done per interface and not per EVC.
- Four traffic classes including class-default can be supported in Egress policy.
- Same three traffic classes or subset of three traffic classes match is supported on EVCs of an interface.
- Traffic classes to queue mapping profiles are limited to four in global, hence excluding class-default, only three mode unique combinations can be supported across interfaces.
- TRTCM always operates with conform-action transmit, exceed-action transmit and violate-action drop.
- By default, 1R2C Policer will behave as 1R3C Policer in 4 Queue model.
- All the QOS restrictions that is applicable in default mode is also applicable in 8k EFP mode

Configuring 8K Model

Configuring 8K EFP Template

Below is the sample configuration to enable 8K EFP or 4 Queue mode template. On enabling **sdm prefer enable_8k_efp**, the router reloads and boots up with 8K EFP template.

```
RSP3-903(config)#sdm prefer enable_8k_efp

Template configuration has been modified. Save config and Reload? [yes/no]: yes
Building configuration...

Jul 22 05:58:30.774 IST: Changes to the EFP template preferences have been stored[OK]
Proceeding with system reload...
Reload scheduled for 06:00:38 IST Fri Jul 22 2016 (in 2 minutes) by console
Reload reason: EFP template change
```

Verifying 8K EFP Template

You can verify the current template as below.

```
Device#sh sdm prefer current

The current sdm template is "default" template and efp template is "enable_8k_efp" template
```

Configuring QOS in 8K EFP Model

Below is sample configuration to configure egress policy map when 4Q mode is enabled.

```
Device#enable
Device#configure terminal
Device(config)#interface GigabitEthernet0/3/0
Device(config-if)#service instance 10 e
Device(config-if-srv)#service-policy output egress



Current configuration : 193 bytes
!
policy-map egress
class qos2
  shape average 2000000
 class qos3
  shape average 3000000
 class qos4
  shape average 4000000
```

```
 class class-default
  shape average 5000000
!
end
```

```
Device#sh run class-map qos2
Building configuration...

Current configuration : 54 bytes
!
class-map match-all qos2
match qos-group 2
!
end
```

```
Device#sh run class-map qos3
Building configuration...

Current configuration : 54 bytes
!
class-map match-all qos3
match qos-group 3
!
end
```

```
Device#sh run class-map qos4
Building configuration...

Current configuration : 54 bytes
!
class-map match-all qos4
match qos-group 4
!
end
```

Verifying QOS in 8K EFP Model

You need to verify the interface and policy-map details to check 8K model queue is working.

```
Device# show run interface g0/3/0
Building configuration...

Current configuration : 217 bytes
!
interface GigabitEthernet0/3/0
no ip address
negotiation auto
service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  service-policy output egress
  bridge-domain 10
!
end
```

```
Router#show running-config policy-map egress
Building configuration...

Current configuration : 193 bytes
!
policy-map egress
class qos2
shape average 2000000
```

```
class qos3
shape average 3000000
class qos4
shape average 4000000
class class-default
shape average 5000000
!
end
```

```
Device#sh policy-map int g0/3/0 serv inst 10
Port-channel10: EFP 10

Service-policy output: egress

Class-map: qos2 (match-all)
122566 packets, 125262452 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 2
Queueing
queue limit 4096000 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/119746/0
(pkts output/bytes output) 2820/2882040
shape (average) cir 2000000, bc 8000, be 8000
target shape rate 2000000

Class-map: qos3 (match-all)
122566 packets, 125262452 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 3
Queueing
queue limit 2730666 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/118806/0
(pkts output/bytes output) 3760/3842720
shape (average) cir 3000000, bc 12000, be 12000
target shape rate 3000000

Class-map: qos4 (match-all)
245131 packets, 250523882 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: qos-group 4
Queueing
queue limit 2048000 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/239961/0
(pkts output/bytes output) 5170/5283740
shape (average) cir 4000000, bc 16000, be 16000
target shape rate 4000000

Class-map: class-default (match-any)
245131 packets, 250523882 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: any
Queueing
queue limit 1638400 us/ 1024000 bytes
(queue depth/total drops/no-buffer drops) 1032720/239961/0
(pkts output/bytes output) 5170/5283740
shape (average) cir 5000000, bc 20000, be 20000
target shape rate 5000000
Device#
```

16K EFP Support on Port Channel

Starting with Cisco IOS XE 16.8.1 release, 16K EFPs on port channel are supported on the RSP3 module.

The following are the key features supported:

- In order to enable 16K EFP over a port channel, you need to enable the following template:

  enable_portchannel_qos_multiple_active

- 16000 EFPs are supported on the RSP3 module (8K EFPs are supported per ASIC). Each port can have a maximum of 8K EFPs configured.
- 8K bridge domains are supported.
- On the RSP3 module, 1024 BDI interfaces that include physical interface, port channel interface, and BDI are available, and these interfaces can be configured upto 4096 BDI interfaces.

Note

- If a port channel is configured on an application-specific integrated circuit (ASIC), for example ASIC 0 , then ensure that physical members to be added to port channel also should be in the same ASIC.
- While adding member links to port channels with 3K to 8K EFPs, the router sends CPUHOG messages to the console output to inform that this process has consumed CPU memory. The number of messages increases with the increase in the scale of the EFPs. Such messages do not impact any functionality. They ensure that the system does not become unresponsive or locked up due to the total consumption of the CPU.

Restrictions for 16K EFP on Port Channel

- G.8032, SADT, CFM, and TEFP are not supported on the port channel.
- 16k EFP scale is not supported if SDM template is enabled for split horizon scale.
- Minimal traffic outage (for example, in milliseconds) is observed, when a policy map is applied or removed.
- In a complete scale environment, the EFP statistics update requires more than 1 minute to complete.

Configuring 16K EFP on Port Channel

To configure 16K EFP on port channel, use the following commands:

```
router>enable
router#configure terminal
router(config)#sdm prefer enable_portchannel_qos_multiple_active
router(config)#platform port-channel 10 members-asic-id 1
router(config)#platform qos-port-channel_multiple_active port-channel 10
router(config)#interface port-channel 10
router(config-if)#end
```

After the SDM template update, the device reloads automatically and you need to enter *yes* to save the configuration.

Verifying 16k EFP on Port Channel

The following are examples to verify for 16K EFP configuration on port channel.

show etherchannel summary

```
Router# show etherchannel summary
Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
10      Po10(RU)                LACP     Te0/5/0(bndl) Te0/5/1(bndl)

RU - L3 port-channel UP State
SU - L2 port-channel UP state
P/bndl -  Bundled
S/susp  - Suspended
```

show ethernet service instance id interface stats

```
Router# show ethernet service instance id 12000 interface port-channel 10 stats
Port maximum number of service instances: 16000
Service Instance 12000, Interface port-channel 10
   Pkts In   Bytes In   Pkts Out  Bytes Out
       252     359352        252     359352
```

show ethernet service instance summary

```
Router# show ethernet service instance summary
System summary
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain     16000    16000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all         16000    16000        0        0        0        0        0        0
Associated interface: port-channel 10
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain      8000     8000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all          8000     8000        0        0        0        0        0        0
Associated interface: port-channel 11
            Total       Up  AdminDo     Down  ErrorDi  Unknown  Deleted  BdAdmDo
bdomain      8000     8000        0        0        0        0        0        0
xconnect        0        0        0        0        0        0        0        0
local sw        0        0        0        0        0        0        0        0
other           0        0        0        0        0        0        0        0
all          8000     8000        0        0        0        0        0        0
```

Control Plane Policing

The Control Plane Policing feature allows you to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOSCisco IOS XE routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can

help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

Restrictions for Control Plane Policing

Input Rate-Limiting Support

Input rate-limiting is performed in silent (packet discard) mode. Silent mode enables a router to silently discard packets using policy maps applied to input control plane traffic with the **service-policy input** command. For more information, see the “Input Rate-Limiting and Silent Mode Operation” section.

MQC Restrictions

The Control Plane Policing feature requires the Modular QoS CLI (MQC) to configure packet classification and traffic policing. All restrictions that apply when you use the MQC to configure traffic policing also apply when you configure control plane policing.

Match Criteria Support

Only the extended IP access control lists (ACLs) classification (match) criteria is supported.

Restrictions for CoPP

- IPv6 is not supported.
- Port range ACL is not supported.
- Due to hardware limitation, to match the control plane packets against CoPP, ACL rules that match with IP addresses should be added, since adding generic ACL rules with any any matches both the data plane and control plane traffic.
- On RSP2, when CoPP is configured with ACL rules, the decision to forward or punt packets is determined by the forwarding engine, rather than the ACL engine. This is due to a known hardware limitation, where packets processed by the ACL engine cannot differentiate between control packets and data packets.

Restrictions for CoPP on the RSP3

- CoPP does not support multi match. ACLs with DSCP and fragment option enabled does not filter or classify packets under CoPP.
- Effective Cisco IOS XE Bengaluru 17.5.1 **`enable_copp_copp`** and **`enable_acl`** template must be configured on the RSP3 module to activate CoPP.
- Ingress and Egress marking are not supported.
- Egress CoPP is not supported. CoPP with marking is not supported.
- CPU bound traffic (punted traffic) flows is supported via the same queue with or without CoPP.
- Only match on access group is supported on a CoPP policy.
- Hierarchical policy is not supported with CoPP.
- Class-default is not supported on CoPP policy.
- User-defined ACLs are not subjected to CoPP classified traffic.

- A CoPP policy map applied on a physical interface is functional.
- When CoPP template is enabled, classification on outer VLAN, inner VLAN, Inner VLAN Cos, destination MAC address, source IP address, and destination IP address are not supported.

  The template-based model is used to enable CoPP features and disable some of the above mentioned QoS classifications.
- When **enable_acl_copp** template is enabled, **sdm prefer enable_match_inner_dscp** template is not supported.
- Only IP ACLs based class-maps are supported. MAC ACLs are not supported.
- Multicast protocols like PIM and IGMP are not supported.
- Only CPU destined Unicast Layer3 protocols packets are matched as part of CoPP classification.
- Do not configure CoPP and BDI-MTU SDM templates together, as it is not supported.
- Management packets cannot be filtered based on source TCP/UDP Ports and destination IP address.
- Ensure to enable the CoPP Version 2 template to enable the CoPP feature.
- Two ACL entries will be added for IPV4 and L3VPN cases for each ACL entry in the configuration.

Restrictions on Firmware

- Port ranges are not supported.
- Only exact matches are supported, greater than, less than and not equal are not supported.
- Internet Control Message Protocol (ICMP) inner type's classification not supported.
- Match any is only supported at a class-map level.
- Policing action is supported on a CoPP policy map.

Supported Protocols

The following table lists the protocols supported on Control Plane Policing feature. It is mandatory that the IP address should match the source or destination IP address.

Table 8: Supported Protocols

Supported Protocols	Criteria	Match	Queue#
TFTP - Trivial FTP	Port Match	IP access list ext copp-system-acl-tftp permit udp any any eq 69	NQ_CPU_HOST_Q
TELNET	Port Match	IP access list ext copp-system-acl-telnet permit tcp any any eq telnet	NQ_CPU_CONTROL_Q

Supported Protocols	Criteria	Match	Queue#
NTP - Network Time Protocol	Port Match	IP access list ext copp-system-acl-ntp permit udp any any eq ntp	NQ_CPU_HOST_Q
FTP - File Transfer Protocol	Port Match	IP access list ext copp-system-acl-ftp permit tcp host any any eq ftp	NQ_CPU_HOST_Q
SNMP - Simple Network Management Protocol	Port Match	IP access list ext copp-system-acl-snmp permit udp any any eq snmp	NQ_CPU_HOST_Q
TACACS - Terminal Access Controller Access-Control System	Port Match	IP access list ext copp-system-acl-tacacs permit tcp any any tacacs	NQ_CPU_HOST_Q
FTP-DATA	Port Match	IP access list ext copp-system-acl-ftpdata permit tcp any any eq 20	NQ_CPU_HOST_Q
HTTP - Hypertext Transfer Protocol	Port Match	IP access list ext copp-system-acl-http permit tcp any any eq www	NQ_CPU_HOST_Q
WCCP - Web Cache Communication Protocol	Port Match	IP access list ext copp-system-acl-wccp permit udp any eq 2048 any eq 2048	NQ_CPU_HOST_Q
SSH - Secure Shell	Port Match	IP access list ext copp-system-acl-ssh permit tcp any any eq 22	NQ_CPU_HOST_Q
ICMP - Internet Control Message Protocol	Protocol Match	IP access list copp-system-acl-icmp permit icmp any any	NQ_CPU_HOST_Q
DHCP - Dynamic Host Configuration Protocol	Port Match	IP access list copp-system-acl-dhcp permit udp any any eq bootps	NQ_CPU_HOST_Q

Supported Protocols	Criteria	Match	Queue#
MPLS- OAM	Port Match	IP access list copp-system-acl-mplsoam permit udp any eq 3503 any	NQ_CPU_HOST_Q
LDP - Label Distribution Protocol	Port Match	IP access list copp-system-acl-ldp permit udp any eq 646 any eq 646 permit tcp any any eq 646	NQ_CPU_CFM_Q
RADIUS - Remote Authentication Dial In User Service	Port Match	IP access list copp-system-radius permit udp any any eq 1812 permit udp any any eq 1813 permit udp any any eq 1645 permit udp any any eq 1646 permit udp any eq 1812 any permit udp any eq 1813 any permit udp any eq 1645 any	NQ_CPU_HOST_Q
Network Configuration Protocol (NETCONF)	IP/Port Match	IP access list ext copp-system-acl-telnet permit tcp any any eq 830 - NETCONF	NQ_CPU_HOST_Q
PostgreSQL Support	IP/Port Match	IP access list ext copp-system-acl-telnet PostgreSQL IP/Port Match permit tcp 169.223.252.0.0 0.0.3.255 host 169.223.253.1 eq 5432	NQ_CPU_HOST_Q

Supported Protocols	Criteria	Match	Queue#
Source IP or Destination IP	IP/Port Match	Permit IP host 10.1.1.1 or 10.1.1.2 **Note** The **permit ip any any** command is not supported.	NQ_CPU_HOST_Q

Input Rate-Limiting and Silent Mode Operation

A router is automatically enabled to silently discard packets when you configure input policing on control plane traffic using the **service-policy input** *policy-map-name* command.

Rate-limiting (policing) of input traffic from the control plane is performed in silent mode. In silent mode, a router that is running Cisco IOS XE software operates without receiving any system messages. If a packet that is entering the control plane is discarded for input policing, you do not receive an error message.

How to Use Control Plane Policing

Defining Control Plane Services

Perform this task to define control plane services, such as packet rate control and silent packet discard for the RP.

Before you begin

Before you enter control-plane configuration mode to attach an existing QoS policy to the control plane, you must first create the policy using MQC to define a class map and policy map for control plane traffic.

- Platform-specific restrictions, if any, are checked when the service policy is applied to the control plane interface.
- Input policing does not provide any performance benefits. It simply controls the information that is entering the device.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **control-plane**

Example:

```
Device(config)# control-plane
```

Enters control-plane configuration mode (which is a prerequisite for defining control plane services).

Step 4 **service-policy** [**input** |**output**] *policy-map-name*

Example:

```
Device(config-cp)# service-policy input control-plane-policy
```

Attaches a QoS service policy to the control plane.

- **input**—Applies the specified service policy to packets received on the control plane.
- *policy-map-name*—Name of a service policy map (created using the **policy-map** command) to be attached.

Step 5 **end**

Example:

```
Device(config-cp)# end
```

(Optional) Returns to privileged EXEC mode.

Configuration Examples for Control Plane Policing

Example: Configuring Control Plane Policing on Input Telnet Traffic

The following example shows how to apply a QoS policy for aggregate control plane services to Telnet traffic that is received on the control plane. Trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 forward Telnet packets to the control plane but are still policed for a maximum rate.

All remaining Telnet packets are dropped by the control-plane.

```
! Define trusted host traffic.
DEVICE(config)#ip access-list extended telnet-trust
DEVICE(config-ext-nacl)#10 permit tcp host 10.1.1.1 any eq telnet
DEVICE(config-ext-nacl)#20 permit tcp host 10.1.1.2 any eq telnet
DEVICE(config-ext-nacl)#exit

! Define all other Telnet traffic.
DEVICE(config)#ip access-list extended telnet-drop
DEVICE(config-ext-nacl)#10 permit tcp any any eq telnet
DEVICE(config-ext-nacl)#exit

! Define class map for trusted hosts
DEVICE(config)#class-map match-all copp-trust
DEVICE(config-cmap)#match access-group name telnet-trust
DEVICE(config-cmap)#exit

! Define class map for un-trusted hosts
DEVICE(config)#class-map match-all copp-drop
DEVICE(config-cmap)#match access-group name telnet-drop
DEVICE(config-cmap)#exit
```

```
! Define the policy-map for both type of hosts
DEVICE(config)#policy-map control-plane-in
DEVICE(config-pmap)#class copp-trust
DEVICE(config-pmap-c)#police 1000000 conform-action transmit  exceed-action drop
DEVICE(config-pmap-c-police)#class copp-drop
DEVICE(config-pmap-c-police)#exit
DEVICE(config-pmap-c)#police 1000000 conform-action drop  exceed-action drop
DEVICE(config-pmap-c-police)#exit
DEVICE(config-pmap-c)#exit
DEVICE(config-pmap)#exit

! Define aggregate control plane service for the active route processor.
DEVICE((config)#control-plane
DEVICE(config-cp)#service-policy input control-plane-in
DEVICE(config-cp)#end


! Rate-limit all other Telnet traffic.
Device(config)# access-list 140 permit tcp any any eq telnet


! Define class-map "telnet-class."
Device(config)# class-map telnet-class
Device(config-cmap)# match access-group 140
Device(config-cmap)# exit
Device(config)# policy-map control-plane-in
Device(config-pmap)# class telnet-class
Device(config-pmap-c)# police 80000 conform transmit exceed drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit

! Define aggregate control plane service for the active route processor.
Device(config)# control-plane
Device(config-cp)# service-policy input control-plane-in
Device(config-cp)# end
```

Verification Examples for CoPP

The following example shows how to verify control plane policing on a policy map.

```
Router# show policy-map control-plane
           Control Plane
         Service-policy input: control-plane-in
         Class-map: telnet-class (match-all)
           10521 packets, 673344 bytes
           5 minute offered rate 18000 bps, drop rate 15000 bps
           Match: access-group 102
           police:  cir 64000 bps, bc 8000 bytes
           conformed 1430 packets, 91520 bytes; actions:
           transmit
           exceeded 9091 packets, 581824 bytes; actions:
           drop
          conformed 2000 bps, exceeded 15000 bps
     Class-map: class-default (match-any)
           0 packets, 0 bytes
           5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: any
```

The following command is used to verify the TCAM usage on the router.

```
Router# show platform hardware pp active feature qos resource-summary 0
RSP3 QoS Resource Summary
```

```
Type Total Used Free
------------------------------------------------------------------------------
QoS TCAM 2048 2 2046
VOQs 49152 808 48344
QoS Policers 32768 2 32766
QoS Policer Profiles 1023 1 1022
Ingress CoS Marking Profiles 16 1 15
Egress CoS Marking Profiles 16 1 15
Ingress Exp & QoS-Group Marking Profiles 64 3 61
Ingress QOS LPM Entries 32768 0 32768
```

QoS Support on Port Channel LACP Active Active

Link Aggregation Control Protocol (LACP) supports the automatic creation of ether channels by exchanging LACP packets between LAN ports. Cisco IOS XE Everest 16.6.1 release introduces the support of QoS on port channel LACP active active mode. A maximum of eight member links form a port channel and thus the traffic is transported through the port channel. This feature is supported on Cisco RSP3 Module.

Benefits of QoS Support on Port Channel LACP Active Active

- This feature facilitates increased bandwidth.
- The feature supports load balancing.
- This features allows support on QoS on Port Channel with one or more active member links.

Restrictions for QoS Support on Port Channel Active Active

- Policy-map on member links is not supported.
- 100G ports and 40G ports cannot be a part of the port channel.
- Total number of port channel bandwidth supported on a given ASIC should not exceed 80G.
- This feature is not supported on multicast traffic.
- Only 3k service instance (EFP) scale is supported on port channel active active.
- Ensure that 2-3 seconds of delay is maintained before and after unconfiguring and re-configuring the port channel with the **platform qos-port-channel_multiple_active** command.



Note This delay increases when you have scaled EVC configurations on the port channel.

Configuring QoS Support on Port Channel Active Active

Enabling Port Channel Active/Active

Use the following commands to enable port channel active active:

```
enable
configure terminal
sdm prefer enable_portchannel_qos_multiple_active
end
```



Note The device restarts after enabling the **sdm prefer enable_portchannel_qos_multiple_active** command. After a successful reboot, verify the configuration using the command **show sdm prefer current**

Disabling Port Channel Active/Active

Use the following commands to disable port channel active active:

```
enable
configure terminal
sdm prefer disable_portchannel_qos_multiple_active
end
```

Configuring Active Active Port Channel per bundle

Use the following commands to configure active active port channel per bundle:

```
enable
configure terminal
platform qos-port-channel_multiple_active 10
end
```

Creating Port Channel Interface

Use the following commands to configure the port channel interface:

```
enable
configure terminal
interface port-channel 10
no shutdown
end
```

Attaching member link to port channel

Use the following commands to attach a member link to the port channel:

```
enable
configure terminal
interface Te0/4/0
channel-group 10 mode active
end
```

Configuring QoS Class Map and Policy Map

Use the following commands to configure QoS class map and policy map:

```
enable
configure terminal
class-map match-any qos1
match qos-group 1
class-map match-any qos2
match qos-group 2
policy-map policymapqos
class qos1
shape average 10000 k
class qos2
shape average 20000 k
end
```

Attaching Configured Policy Map (policymapqos) on Port Channel Interface on Egress Direction

Use the following commands to attach the configured policy map (policymapqos) on the port channel interface on egress direction:

```
enable
configure terminal
interface port-channel 10
service-policy output policymapqos
end
```

Verification of QoS Support on Port Channel LACP Active Active

Use the commands below to verify the port channel summary details:

```
Device#show etherchannel summary
 Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


 Number of channel-groups in use: 1
 Number of aggregators:           1

 Group  Port-channel  Protocol    Ports
 ------+-------------+-----------+-----------------------------------------------
 10      Po10(RU)         LACP     Te0/4/0(bndl)
```

Use the commands below to verify the attached policy map on the port channel interface:

```
Device#show policy-map interface brief
Service-policy input: ingress
TenGigabitEthernet0/4/0
Service-policy output: policymapqos
Port-channel10

      Device#show policy-map interface po10
  Port-channel10

    Service-policy output: policymapqos

    Class-map: qos1 (match-any)
      1027951 packets, 1564541422 bytes
      30 second offered rate 50063000 bps, drop rate 40020000 bps
      Match: qos-group 1
      Queueing
      queue limit 819200 us/ 1024000 bytes
      (queue depth/total drops/no-buffer drops) 0/821727/0
      (pkts output/bytes output) 206224/313872928
      shape (average) cir 10000000, bc 40000, be 40000
      target shape rate 10000000

    Class-map: qos2 (match-any)
      852818 packets, 1297988996 bytes
      30 second offered rate 41534000 bps, drop rate 21447000 bps
      Match: qos-group 2
      Queueing
      queue limit 409600 us/ 1024000 bytes
      (queue depth/total drops/no-buffer drops) 0/440370/0
      (pkts output/bytes output) 412448/627745856
      shape (average) cir 20000000, bc 80000, be 80000
      target shape rate 20000000
```

```
Class-map: class-default (match-any)
  1565 packets, 118342 bytes
  30 second offered rate 3000 bps, drop rate 0000 bps
  Match: any

  queue limit 102 us/ 1024000 bytes
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 1565/118342
```

Use the commands below to verify the configuration after enabling port channel active/active mode:

```
#show sdm prefer current
The current sdm template is "default"
The current portchannel template is "enable_portchannel_qos_multiple_active"
```

Match Inner DSCP on RSP3 Module

Starting with Cisco IOS XE Release 16.6.1, the match_inner_dscp template is introduced. This template allows DSCP policy map configuration on the RSP3 module for MPLS and tunnel terminated traffic.

Restrictions for Match Inner DSCP on RSP3 Module

- The IPv4 DSCP policy map configuration is not preserved in case of protection scenarios, where either primary or backup path is plane IP path and backup or primary is MPLS label path.
- Match on Inner DSCP for IPv6 is not supported.
- Only 1024 entries IPv4 TCAM entries are available. Hence, optimized usage of classes is recommended for configuration when policy map is applied on port channel or port or EFP.
- To support match on Inner DSCP for IPv4 when packets have MPLS forwarding type, three TCAM entries are added whenever there is a class map with match DSCP is configured.

  One match is for normal DSCP scenario, one entry for Inner DSCP when outer header is MPLS header and other entry is when there is tunnel termination.

  In Split Horizon template, each match DSCP class consumes 3 TCAM entries. For non-Split Horizon template, TCAM entries are one. For Class default, number of entries consumed is one. For TEFP, six entries are required for each match DSCP Class Map and two for class default.



Note Some of the IPv4 qualifiers are not supported when Split Horizon template is configured as there are limitation of Copy Engines in IPv4 Resource database. Whenever Split Horizon template is enabled, four new qualifiers are added in IPV4 QoS Field Group.

Configuring Match Inner DSCP on RSP3 Module

```
Class-map match-any dscp
Match dscp af13
exit
policy-map matchdscp
Class dscp
Police cir 1000000end
```

Verifying Match Inner DSCP on RSP3 Module

```
Router# show platform hardware pp active feature qos resource-summary 0
PE1#res
RSP3 QoS Resource Summary

Type                                        Total       Used        Free
------------------------------------------------------------------------------
QoS TCAM                                    1024         0          1024
VOQs                                        49152       408         48744
QoS Policers                                32768        0          32768
QoS Policer Profiles                        1023         0          1023
Ingress CoS Marking Profiles                16           1          15
Egress CoS Marking Profiles                 16           1          15
Ingress Exp & QoS-Group Marking Profiles    64           3          61
Ingress QOS LPM Entries                     32768        0          32768
```

Limitations for VLAN Translation with SDM Template for RSP3

Table 9: Feature History

Feature Name	Release Information	Feature Description
VLAN Translation for RSP3	Cisco IOS XE Bengaluru 17.4.1	VLAN translation provides flexibility in managing VLANs and Metro Ethernet-related services. You can configure 1:1 and 2:1 VLAN translations using the **sdm prefer enable_vlan_translation** command on the Cisco RSP3 module.

- On a dual RSP setup for the Cisco RSP3 module, enabling or disabling VLAN Translation template reloads the standby RP. Once standby RSP boots up, the system reaches SSO (Hot Standby State). A manual SSO (RP switchover) should to be performed before configuring any VLAN translation.

Note On a single RSP setup for the Cisco RSP3 module, enabling or disabling VLAN Translation template will save the configuration and reload the system.

Configuring VLAN Translation for RSP3

Below is sample configuration to VLAN Translation on Cisco RSP3 module.

Procedure

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal	Enters global configuration mode.

	Command or Action	Purpose

Step 3	sdm prefer enable_vlan_translation
	Example:
	`sdm prefer enable_vlan_translation`
	
	`Router(config)#sdm prefer enable_vlan_translation`
	`Standby is reloaded, it will come up with init required for new template`
	`once standby comes up`
	`Please trigger SSO`
	`Changes to VLAN Translation template stored`
		Enables VLAN Translation on the Cisco RSP3 module.

Step 4	sdm prefer disable_vlan_translation
	Example:
	`sdm prefer disable_vlan_translation`
	
	`Router(config)#sdm prefer disable_vlan_translation`
	`Standby is reloaded, it will come up with init required for new template`
	`once standby comes up`
	`Please trigger SSO`
	`Changes to VLAN Translation template stored`
		Disables VLAN Translation on the Cisco RSP3 module.

DHCP Snooping

Table 10: Feature History

Feature Name	Release Information	Feature Description
Enable DHCP Snooping Option 82 for RSP3	Cisco IOS XE Dublin 17.10.1	You can enable DHCP snooping option-82 on the Cisco RSP3 module using the **sdm prefer enable_dhcp_snoop** command. This feature provides additional security information to the relay agent that the information is from the trusted port.

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. It validates DHCP messages received from untrusted sources and filters out invalid messages. Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses. Utilizes the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

DHCP Option-82

Option-82 in DHCP is an additional security mechanism over DHCP snooping. The DHCP Relay Agent Information option (Option 82) allows the DHCP Relay Agent to insert additional information into a request

that is being forwarded to a DHCP server. The interface that receives “Option 82” must be a “trusted” port. If not, the packet is dropped.

The RSP3 platform supports DHCP or DHCP Snooping (option 82) feature currently using ASIC-supported system level DHCP-traps mechanism. The available DHCP-traps works at router level and traps the DHCP frames that ingress on any of the interfaces of router to CPU once enabled. Not all the DHCP frames on all types of service instances or interfaces need to be trapped to CPU. The DHCP frames that ingress on cross connect like service instances could be forwarded in data plane and does not need to be trapped to CPU always, which could avoid congestion of CPU queues further does not block the services.

Limitations for DHCP Snooping Option-82

- The Layer 2 ACL scale reduced from 512 to 256.
- The Layer 2 ACLs cannot use SRC MAC-based qualifiers.
- CFM over VPLS is not supported.
- The feature is supported only on the **enable_dhcp_snoop** template.
- The enable_dhcp_snoop and enable_l2pt_fwd_all templates are mutually exclusive.
- Maximum supported BD with DHCP snooping enabled is 10.
- A maximum of 20 EFPs can be associated to a BD which is configured with DHCP snooping. For example, single BD can be mapped to 20 EFPs or 2 to 3 BDs can also be mapped to 20 EFPs.
- This feature is supported only in normal EFP. TEFP and port-channel features are not supported for this template.
- The echo-BFD feature is not supported in the **enable_dhcp_snoop** template.
- DHCP snooping over VPLS is not supported in any of the templates.
- Layer 2 ACL is not supported on the DHCP-snooping enabled EFP.
- The scale of Layer 3 ACL is reduced from 512 to 256.

Enabling DHCP Snooping Template

To configure DHCP snooping on a service instance, use the following commands:

```
router>enable
router#configure terminal
router(config)#sdm prefer enable_dhcp_snoop
router(config-if)#end
```

After the SDM template update, the device reloads automatically and you need to enter *yes* to save the configuration.