

Policy Commands

- access-list, on page 2
- action (centralized policy), on page 4
- action (localized policy), on page 6
- app-agg-node, on page 8
- apply-policy, on page 9
- app-probe-class, on page 10
- app-route-policy, on page 11
- app-visibility, on page 12
- app-visibility-ipv6, on page 13
- burst, on page 13
- class (class-map), on page 15
- cos, on page 15
- count, on page 16
- data-policy, on page 17
- default-action, on page 17
- destination-ip, on page 18
- exceed, on page 19
- flow-visibility, on page 20
- flow-visibility-ipv6, on page 20
- icmp-echo, on page 21
- implicit-acl-on-bind-intf , on page 22
- inspect, on page 22
- ip-prefix, on page 23
- ip sla, on page 24
- ip sla reaction-configuration, on page 24
- ip sla responder, on page 26
- ip sla schedule, on page 27
- ip visibility cache entries, on page 28
- ipv6 access-list, on page 29
- ipv6 visibility cache entries, on page 29
- jitter, on page 30
- lists, on page 30
- lists data-prefix-list, on page 32

- lists (tag instance), on page 33
- loss, on page 34
- match (access-control-list), on page 35
- match as-path, on page 37
- match (data policy), on page 38
- match ip address, on page 40
- match protocol attribute application-group, on page 41
- parameter-map type inspect, on page 42
- policer, on page 42
- policy, on page 44
- policy ip visibility, on page 45
- policy log-rate-limit, on page 46
- queue-limit, on page 47
- rate, on page 49
- request-data-size, on page 50
- rewrite-rule, on page 50
- service-area, on page 52
- service-policy, on page 53
- set ip vrf, on page 54
- set ip next-hop verify-availability, on page 55
- sequence, on page 56
- sequence (access-control-list), on page 57
- sla-class, on page 58
- sig, on page 59
- site-list, on page 60
- tag (IP SLA), on page 61
- tag-instances, on page 62
- track ip sla, on page 63
- udp-jitter, on page 64
- utd-policy, on page 65
- vpn-list, on page 65
- vrf (IP SLA), on page 66

access-list

To define the access list, use the **access-list** command in policy configuration mode. To remove the access list, use the **no** form of this command.

access-list *access-list-name* [**sequence** *sequence-value* [**match** [**destination-ip** *dest-ip/length* | **source-ip** *src-ip/length* | **destination-port** *dest-port-range* | **source-port** *src-port-range* | **destination-data-prefix-list** *prefix* | **source-data-prefix-list** *prefix* | **destination-tag-instance** *dest-tag-name* | **source-tag-instance** *src-tag-name*] **action** { **accept** | [**class** | **count**] | **drop** | **count** } | **action**] | **default-access** | **drop accept**]
no access-list

Syntax Description

destination-data-prefix-list	(Optional) Specifies the destination prefix list.

destination-ip	(Optional) Specifies the list of destination addresses.
destination-port	(Optional) Specifies the list of destination ports.
count	(Optional) Specifies the number of packets/bytes matching this rule drop.
destination-tag-instance	(Optional) Specifies the name of the destination tag instance. Valid range is from 1 to 127 characters.
source-data-prefix-list	(Optional) Specifies the source data prefix list.
source-ip	(Optional) Specifies the list of source IP addresses.
source-port	(Optional) Specifies the list of source ports.
source-tag-instance	(Optional) Specifies the name of the source tag instance. Valid range is from 1 to 127 characters.

Command Default

The access list defaults to an implicit deny statement for everything. An implicit deny statement terminates an access list.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was modified. Policy match configuration is enhanced to include **source-tag-instance** and **destination-tag-instance** keyword parameters in ACL-matching attributes.

Usage Guidelines

After ACL is defined, it can be applied to an interface.

Examples

The following is a sample output of this command:

```
access-list acl1
   sequence 10
    match
     destination-ip 172.16.5.10
    !
    action drop
   default-action accept
    action drop
     count 192-167-199-DROP-CNT
  access-list 4451-Marking-Spoke
   sequence 1
    match
     destination-ip 172.16.10.5
    !
    action accept
     count SSL
     class LLQ
```

```
     count EXCHANGE
     class CONTROL-SIGNALING
```

The following example shows how to configure **source-tag-instance** in a localized policy:

```
policy
 lists
  data-prefix-list pfx1
   ip-prefix 10.20.24.0/24
  !
 !
 access-list acl
  sequence 10
   match
    source-tag-instance red
   !
   action accept
    count acl_input_wc
   !
  !
  default-action drop
 !
!
```

action (centralized policy)

To define the action to take when the match portion in a match–action pair is met, use the **action** command in sequence configuration mode. To remove configured sub-actions or reset the action to the default of drop, use the **no** form of this command.

action { **drop** { **count** *counter-name* | **log** } | **accept** { **count** *counter-name* | **nat use-vpn** *0* { } | **log** | **local-tloc** | **policer** *policer-name* | **next-hop** *ipv4-address* **next-hop-loose** | **set** { **vpn** *vpn-number* } | { **set tloc** *ip-address* **color** *color* } } }

no action { **drop** { **count** *counter-name* | **log** } | **accept** { **count** *counter-name* | **nat use-vpn** *0* { } | **log** | **local-tloc** | **policer** *policer-name* | **next-hop** *ipv4-address* **next-hop-loose** | **set** { **vpn** *vpn-number* } | { **set tloc** *ip-address* **color** *color* } } }

Syntax Description

drop	Defines the action to drop matching packets.
accept	Defines the action to accept matching packets and to perform any specified actions.
nat use-vpn *0*	Ensures that matching traffic is sent to VPN 0 after the source IP is translated, based on the policy match criteria.
count *counter-name*	Counts the packets that match the match criteria, saving the information to the specified filename.
log	Logs the packet headers into system logging (syslog) files.

set tloc *ip-address* **color** *color* [**encap** *ecapsulation*]	Sets the TLOC identified IP sddress and color Directs matching packets to a TLOC identified by its IP address and color, and optionally, by its encapsulation.*color* can be **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, and **silver**. By default, *encapsulation* is **ipsec**. It can also be **gre**.
policer *policer-name*	Police the packets using the specified policer.
set dscp *dscp-value*	For QoS, set or overwrite the DSCP value in the packet. Range: 0 through 63.
set local-vpn *local-vpn-number*	Sets the local VPN number. Range: 0 through 65530.
set next-hop *ipv4-address*	Sets the next-hop address. The address must be an IPv4 address.
set next-hop-loose	Routes the traffiic using an available route if the next-hop address is not available. This parameter is supported only for centralized data policies.

Command Default

The default behavior is dropped.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was modified. Added next-hop-loose keyword to redirect application traffic to an available route when next-hop address is not available.
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command was modified. Added the **nat use vpn***0* keyword for NAT66 to configure the centralized data policy.

Usage Guidelines

The sequence numbering feature applies sequence numbers to match-action pairs. The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when it matches the conditions in one of the pairs.

When a packet matches one of the match conditions, the defined action is taken. Or if no match occurs, the default action is taken.

This command can be used to define the action to take when the match portion in a match–action pair is met.

Note The **set next-hop-loose** option can be applied only if **set next-hop** action is defined.

Example

The following example shows how to create a centralized control policy that changes the TLOC for accepted packets:

```
Device(config)# policy
  control-policy change-tloc
    sequence 10
      action accept
        set tloc 10.1.1.2
```

The following example shows how to create a data policy using next-hop-loose command inorder to route the packet using routing entry from routing table if next-hop is not reachable.

```
show policy from-vsmart
from-vsmart data-policy data_pol_nh1
 direction all
 vpn-list vpn1
  sequence 12
   match
    source-ip 10.20.24.150/32
   action accept
    count data_pol_nh1_ctr
    set
     next-hop 96.0.1.100
     next-hop-loose
  sequence 122
   match
    source-ip 10.20.25.150/32
   action accept
  default-action drop
```

The following example shows how to configure a NAT66 DIA route using a centralized data policy so that data traffic is NATed before entering the overlay tunnel that is located in the transport VPN:

```
Device(config)# policy
 data-policy policy-name
  vpn-list vpn_list
  sequence number
  match
   source-ipv6 ipv6-address
  !
  action accept
   nat use-vpn 0
   nat fallback
   set
    local-tloc-color lte
```

For more information about, see the section *NAT66 DIA With Centralized Data Policy* in *Information About NAT DIA*

action (localized policy)

To define the action to take when the match portion in a match–action pair is met, use the **action** command in access control list sequence configuration mode. To remove configured sub-actions or reset the action to the default of drop, use the **no** form of this command.

action { **drop** { **count** *counter-name* | **log** } | **accept** { **class** *class-name* | **count** *counter-name* | **log** | **mirror** *mirror-name* | **policer** *policer-name* } | **set** { **dscp** *dscp-value* | **local-vpn** *local-vpn-number* | **next-hop** *ipv4-address* **next-hop-loose** } }
no action { **drop** { **count** *counter-name* | **log** } | **accept** { **class** *class-name* | **count** *counter-name* | **log** | **mirror** *mirror-name* | **policer** *policer-name* } | **set** { **dscp** *dscp-value* | **local-vpn** *local-vpn-number* | **next-hop** *ipv4-address* } }

Syntax Description

drop	Defines the action to drop matching packets.
accept	Defines the action to accept matching packets and to perform any specified actions.
count *counter-name*	Counts the packets that match the match criteria, saving the information to the specified filename.
log	Logs the packet headers into system logging (syslog) files.
class *class-name*	Assigns the packets to the specified QoS class name.
mirror *mirror-name*	Mirrors the packets to the specified mirror.
policer *policer-name*	Police the packets using the specified policer.
set dscp *dscp-value*	For QoS, set or overwrite the DSCP value in the packet. Range: 0 through 63.
set local-vpn *local-vpn-number*	Sets the local VPN number. Range: 0 through 65530.

Command Default

The default behavior is dropped.

Command Modes

Access control list sequence configuration (config-sequence-{sequence-number})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Access control lists (ACLs) perform packet filtering to control which packets move through an interface of a router. The packet filtering provides security by helping to limit the network traffic, restrict the access of users and devices to a network, and prevent the traffic from leaving a network interface. An access control list is a sequential list consisting of match-action pairs.

The sequence numbering feature applies sequence numbers to match-action pairs. The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when it matches the conditions in one of the pairs.

When a packet matches one of the match conditions, the defined action is taken. Or if no match occurs, the default action is taken.

This command can be used to define the action to take when the match portion in a match–action pair is met.

Example

The following example creates an access control list named ACL-TEST-1, defines sequence #10, enters the match configuration mode, specifies destination IP 10.10.10.10/32 as a match parameter, and defines the action to drop and logs the packet when matched.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# match
Device(config-match)# destination-ip 10.10.10.10/32
Device(config-match)# exit
Device(config-sequence-10)# action drop
Device(config-action)# log
```

The following example creates an access control list named ACL-TEST-1, defines sequence #20, enters the match configuration mode, specifies packet length of 10 as a match parameter and defines the action to accept and applies the policer policy POL1 when matched.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 20
Device(config-sequence-20)# match
Device(config-match)# packet-length 10
Device(config-match)# exit
Device(config-sequence-20)# action accept
Device(config-action)# policer POL1
```

Table 1: Related Commands

Commands	Description
match	Enters the match configuration mode or to define match parameters.

app-agg-node

To set the maximum rate of Flexible NetFlow (FNF) records of aggregated traffic data that a device sends to Cisco SD-WAN Manager, use the **app-agg-node** command in policy configuration mode on a device. To restore the default limit, use the **no** form of the command.

app-agg-node *max-records-per-minute*

no app-agg-node

Syntax Description

max-records-per-minute	Maximum number of FNF records per minute of aggregated traffic data for a device to send to Cisco SD-WAN Manager. Range: 16 to 10000 FNF records per minute Default: 10000 FNF records per minute

Command Modes

Policy configuration (config-policy)

Command Default

10000 FNF records per minute

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

When traffic flow visibility is enabled (see Configure Global Flow Visibility), devices in the network send raw and aggregated traffic flow data to Cisco SD-WAN Manager.

To aggregate flow data, routers use 4-tuples of flow data (containing VPN ID, application name, ingress interface of the flow, and egress interface of the flow) as a key for consolidating the raw data of multiple flows. The router consolidates each flow for which the 4-tuple is identical into a single aggregated FNF record.

Cisco SD-WAN Manager uses the aggregated data to provide a high-level view of network traffic flow information. The aggregated data shows the network applications that are producing traffic, but is less granular than the full traffic flow data. It does not provide source and destination addresses, or source and destination ports for traffic flows.

You can configure a maximum rate of aggregated traffic data FNF records that a device can send to reduce the performance demands (CPU and memory) on the device. This may be helpful when there is a large number of applications producing network traffic.

Example 1

The following configures a device to send a maximum of 1000 FNF records per minute.

```
Device(config)# policy
Device(config-policy)# app-agg-node 1000
```

Example 2

The following restores a device to the default value of sending a maximum of 10000 FNF records per minute.

```
Device(config)# policy
Device(config-policy)# no app-agg-node
```

apply-policy

To have a policy take effect by applying it to sites within the overlay network (on Cisco vSmart Controllers only), use the **apply-policy** command in the policy lists configuration mode. To remove the listing of sites, use the **no apply-policy** form of this command.

apply-policy

no apply-policy

Syntax Description

This command has no arguments or keywords.

Command Default None

Command Modes policy lists configuration (config-lists)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

```
vSmart(config)# apply-policy
vSmart(config-apply-policy)# site-list cedge_1
vSmart(config-site-list-cedge_1)# data-policy sig_ha_zscaler_data_policy_cedge from-service
```

```
vSmart(config)# apply-policy
vSmart(config-apply-policy)# site-list cedge_1
vSmart(config-site-list-cedge_1)# data-policy sig_ha_zscaler_data_policy_cedge from-tunnel
```

```
vSmart(config)# apply-policy
vSmart(config-apply-policy)# site-list cedge_1
vSmart(config-site-list-cedge_1)# data-policy sig_ha_zscaler_data_policy_cedge all
```

app-probe-class

To define a forwarding class and DSCP marking per color that a particular class of applications is forwarded to, use the **app-probe-class** command in global configuration mode.

app-probe-class *app-probe-class-name*

no app-probe-class *app-probe-class-name*

Syntax Description

app-probe-class	Specifies the app-probe-class of SLA class applications that is forwarded to devices.
app-probe-class-name	Specifies the app-probe-class name.

Command Default There are no default values.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

In the following example, you can create real-time-video app-probe-class with DSCP measurements:

```
vSmart(config)# app-probe-class real-time-video
vSmart(config)# forwarding-class videofc
vSmart(config)# color mpls dscp 34
vSmart(config)# color biz-internet dscp 40
```

```
vSmart(config)# color lte dscp 0
```

app-route-policy

To configure application route policy for the Cisco IOS XE Catalyst SD-WAN devices, use the **app-route-policy** command in the policy configuration mode.

app-route-policy *policy-name*

Syntax Description

app-route-policy *policy-name*	Name of the application-aware routing policy to configure or to apply to a list of sites in the overlay network. *policy-name* can be up to 32 characters long.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in CLI templates.

Usage Guidelines

For more information about this command, see Policies Configuration guide.

The following example shows how to configure and apply a data policy for application-aware routing:

```
vSmart# show running-config policy
policy
 sla-class test_sla_class
  latency 50
 !
 app-route-policy test_app_route_policy
  vpn-list vpn_1_list
   sequence 1
    match
     protocol 6
    !
    action sla-class test_sla_class strict
   !
   sequence 2
    match
     protocol 17
    !
    action sla-class test_sla_class
   !
   sequence 3
    match
     protocol 1
    !
    action sla-class test_sla_class strict
   !
  !
 !
 lists
  vpn-list vpn_1_list
   vpn 1
  !
```

```
  site-list site_500
   site-id 500
  !
  site-list site_600
   site-id 600
  !
 !
!
apply-policy
 site-list site_500
  app-route-policy test_app_route_policy
 !
!
```

The following example shows how to configure a policy for application-aware routing:

```
policy
  app-route-policy policy-name
    vpn-list list-name
      default-action sla-class sla-class-name
      sequence number
        match
          app-list list-name
          destination-data-prefix-list list-name
          destination-ip prefix/length
          destination-port number
          dns (request | response)
          dns-app-list list-name
          dscp number
          plp (high | low)
          protocol number
          source-data-prefix-list list-name
          source-ip prefix/length
          source-port address
        action
          backup-sla-preferred-color colors
          count counter-name
          log
          sla-class sla-class-name [strict] [preferred-color colors]
```

app-visibility

To enable application visibility so that a router can monitor and track the applications running on the LAN use the **app-visibility** command. Use the **no** form of this command to disable application visibility.

app-visibility

Command Default

Disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines To enable NBAR feature to recognize applications. Use the **show sdwan app-fwd dpi** command to see DPI flows.

Examples Enable application-visibility on a router:

```
Router(config)# policy
Router(config-policy)# app-visibility
```

app-visibility-ipv6

To enable application visibility IPv6, so that a router can monitor and track the applications running on the LAN use the **app-visibility-ipv6** command. Use the **no** form of this command to disable application visibility IPv6.

app-visibility-ipv6

Command Default Disabled.

Command Modes Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines To enable NBAR feature to recognize applications. Use the **show sdwan app-fwd dpi** command to see DPI flows.

Examples Enable application-visibility on a router:

```
Router(config)# policy
Router(config-policy)# app-visibility-ipv6
```

burst

To define the burst size for a policer profile, use the **burst** command in policer configuration mode.

burst *burst-size*

Note Burst is a required parameter in a policer profile. Entering **no burst** *burst-size* is valid, but causes **commit** to fail.

Syntax Description

burst-size	Maximum traffic burst size, in bytes. The range is from 15000 to 10000000.

Command Default

None

Command Modes

Policer configuration (config-policer-{profile-name})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

This command can be used to define the burst size for a policer profile.

Example

The following example defines a policer profile named pol1. It sets the rate to 500,000,000 bps, and burst size to 15,000 bytes, and configures to drop the traffic if the burst size or traffic rate is exceeded.

```
Device(config)# policy
Device(config-policy)# policer pol1
Device(config-policy-pol1)# rate 500000000
Device(config-policy-pol1)# burst 15000
Device(config-policy-pol1)# exceed drop
```

The following example applies a policer using an Access List named ACL-TEST-1.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 1
Device(config-sequence-1)# action drop
Device(config-action)# policer pol1
```

Note Rate, burst, and exceed must be defined before committing, otherwise the commit is aborted.

Table 2: Related Commands

Commands	Description
exceed	Action to take when the burst size or traffic rate is exceeded.
rate	Bandwidth for 1G interfaces, the range is from 8 to 1000000000 bps; for 10G interfaces, the range is from 8 to 10000000000 bps.

class (class-map)

To specify the name of the class whose policy you want to create or change before you configure its policy, use the **class**command in class-map configuration mode. To remove a class from the class map, use the **no** form of this command.

class *class-name*
no class { *class-name* }

Syntax Description

class-name	Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map.

Command Default

No class is specified.

Command Modes

Class-map configuration (config-class-map)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE, class command.

Examples

The following is an example of this command:

```
Device(config)# policy
Device(config-policy)# class-map
Device(config-class-map)# class VOICE queue 0
```

cos

To set the class of service (CoS) for a Cisco IOS IP Service Level Agreements (SLAs) Ethernet operation, use the **cos** command in the appropriate submode of IP SLA configuration or IP SLA Ethernet monitor configuration mode. To return to the default value, use the **no** form of this command.

cos-value	Class of service (CoS) value. The range is from 0 to 7. The default is 0.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE cos command.

Examples

The following example shows how to configure this command:

```
Interface interface-name
 cfm mep domain domain-name mpid id service service-name
  alarm notification all*
  cos 0-7
```

count

To specify the number of packets that matches the match criteria, use the **count** command in the action configuration mode. To remove the count that matches the match criteria, use the **no** form of this command.

count { *counter-name* }

no count { *counter-name* }

Syntax Description

counter-name	Specifies the count of the packets that match the match criteria, and saving the information to a specified filename.

Command Default

None

Command Modes

action configuration (config-action)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see Centralized Policy.

The following example creates an access control list named ACL-TEST-1, defines sequence #10, enters the match configuration mode, specifies destination IP 10.10.10.10/32 as a match parameter, defines the action to accept, and specifies the packets that match the match criteria in the seqcnt_100 file.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# match
Device(config-match)# destination-ip 10.0.0.0/8
Device(config-match)# exit
Device(config-sequence-10)# action accept
Device(config-action)# count seqcnt_100
```

data-policy

To configure or apply a centralized data policy based on data packet header fields (on Cisco vSmart controllers only), use the **data-policy** command in policy configuration mode. To remove the configured centralized data policy for deep packet inspection, use the **no** form of this command.

data-policy { *policy-name* }

no data-policy { *policy-name* }

Syntax Description

policy-name	Specifies the name of the centralized data policy to configure or to apply to a list of sites in the overlay network. The maximum characters allowed are 32.

Command Default

None

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see configuring the deep packet inspection in the Policies Configuration Guide.

```
vSmart(config)# policy
vSmart(config-policy)# data-policy sig_ha_zscaler_data_policy_cedge
```

default-action

To configure the default action to be taken when the match condition in an access list isn't met for the Cisco IOS XE Catalyst SD-WAN devices, use the **default-action** command in the policy access list configuration mode. To remove the default configuration, use the **no default-action** form of this command.

default-action [**drop**] { **accept** | **drop** }

no default-action

Syntax Description

accept|**drop**	Specifies the default action to take if a route being evaluated by a policy matches none of the match conditions. If you configure a policy and define an access list with one or more match–action sequences, the default action, is to either accept or drop the item, depending on the policy type.

Command Default

None

Command Modes policy access list configuration (config-access-list)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For more information about this command, see Localized Policy.

The following example shows that if a packet being evaluated doesn't match any of the match conditions in an access list, a default action is applied to this packet. By default, the packet is dropped.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# match
Device(config-match)# destination-ip 10.10.10.10/32
Device(config-match)# exit
Device(config-match)# exit
Device(config-access-list-ACL-TEST-1)# default-action accept
```

destination-ip

To list the destination addresses for an access control list, use the **destination-ip** command in the match configuration mode. To remove the list of destination addresses, use the **no** form of this command.

destination-ip { *ipv4-prefix/prefix-length* }

no destination-ip { *ipv4-prefix/prefix-length* }

Syntax Description

ipv4-prefix/prefix-length	Specifies IPv4 prefix in dotted decimal and the length of the IPv4 prefix. Specifies the prefix-length, which is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Default None

Command Modes match configuration (config-match)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines For more information about this command, see Centralized Policy.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# match
```

```
Device(config-match)# destination-ip 10.10.10.10/32
Device(config-match)# exit
```

exceed

To define the exceed action for a policer profile, use the **exceed** command in policer configuration mode.

exceed { *drop* | *remark* }

Syntax Description

drop	Drops excess traffic when the burst size or traffic rate is exceeded. The drop action is equivalent to setting the packet loss priority (PLP) to low.
remark	Remarks the traffic. The remark action sets the PLP to high.

Command Default

None

Command Modes

Policer configuration (config-policer-{profile-name})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

This command can be used to define the action to take if the burst size or traffic rate is exceeded.

Example

The following example defines a policer profile named pol1. It sets the rate to 500,000,000 bps, and burst size to 15,000 bytes, and configures to drop the traffic if the burst size or traffic rate is exceeded.

```
Device(config)# policy
Device(config-policy)# policer pol1
Device(config-policy-pol1)# rate 500000000
Device(config-policy-pol1)# burst 15000
Device(config-policy-pol1)# exceed drop
```

The following example applies a policer using an Access List named ACL-TEST-1.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 1
Device(config-sequence-1)# action drop
Device(config-action)# policer pol1
```

Note Rate, burst, and exceed must be defined before committing, otherwise the commit is aborted.

Table 3: Related Commands

Commands	Description
burst	Maximum traffic burst size, in bytes.The range is from 15000 to 10000000.
rate	Bandwidth for 1G interfaces, the range is from 8 to 1000000000 bps; for 10G interfaces, the range is from 8 to 10000000000 bps.

flow-visibility

To enable flow visibility so that a router can perform traffic flow monitoring on traffic coming to the router from the LAN use the **flow-visibility** command. To disable the flow visibility use the **no** form of this command.

flow-visibility

no flow-visibility

Command Default

Disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **show sdwan app-fwd cflowd** command to enable cflowd flow monitoring.

Examples

The following is an example of this command

```
Router(config)# policy
Router(config-policy)# flow-visibility
```

flow-visibility-ipv6

To enable flow visibility IPv6, so that a router can perform traffic flow monitoring on traffic coming to the router from the LAN use the **flow-visibility-ipv6** command. To disable the flow visibility use the **no** form of this command.

flow-visibility-ipv6

no flow-visibility-ipv6

Command Default

Disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use the **show sdwan app-fwd cflowd** command to enable cflowd flow monitoring.

Examples

The following is an example of this command

```
Router(config)# policy
Router(config-policy)# flow-visibility-ipv6
```

icmp-echo

To configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) echo operation, use the **icmp-echo**command in IP SLA configuration mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE icmp-echo command

Examples

In the following example, IP SLAs operation 10 is created and configured as an echo operation using the ICMP protocol and the destination IPv4 address 10.16.1.175:

```
Device# config-transaction
Device(config)# ip sla 10
Device(config-ip-sla)# icmp-echo 10.16.1.175
Device(config-ip-sla-echo)#
```

In the following example, IP SLAs operation 11 is created and configured as an echo operation using the ICMP protocol and the destination IPv6 address 2001:DB8:100::1:

```
Device# config-transaction
Device(config)# ip sla 11
Device(config-ip-sla)# icmp-echo 2001:DB8:100::1
Device(config-ip-sla-echo)#
```

implicit-acl-on-bind-intf

To enable implicit ACL protection on a physical interface (bound to a loopback interface), use the **implicit-acl-on-bind-intf**command in the global configuration mode. To remove this change, use the no form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

The following example shows how to enable a physical interface as a TLOC.

```
Device(config)# sdwan interface Loopback1
Device(config-interface-Loopback1)# tunnel-interface
Device(config-tunnel-interface)# encap ipsec
Device(config-tunnel-interface)# color 3g
Device(config-tunnel-interface)# bind GigabitEthernet1
Device(config-tunnel-interface)#implicit-acl-on-bind-intf
```

inspect

To enable Cisco IOS stateful packet inspection, use the **inspect** command in policy-map-class configuration mode. To disable stateful packet inspection, use the **no** form of this command.

inspect
no inspect

Command Default

Cisco IOS stateful packet inspection is disabled.

Command Modes

Policy-map-class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE inspect command.

Examples

The following example specifies inspection parameters and requests the **inspect** action with the specified inspect parameter:

```
policy-map type inspect mypolicy
 class type inspect inspect-traffic
  inspect
```

ip-prefix

To define an IP prefix for a data-prefix-list or prefix-list, use the **ip-prefix** command in data-prefix-list or prefix-list configuration mode. To remove an IP prefix for a data-prefix-list or prefix-list, use the **no** form of this command.

ip-prefix *IP/length* [**ge** *length*] [**le** *length*]
no ip-prefix *IP/length*

Syntax Description

IP/length	IP address and CIDR.
ge	(Optional) (Prefix-list only, not available for data-prefix-list) Specifies the minimum prefix length to be matched.
le	(Optional) (Prefix-list only, not available for data-prefix-list) Specifies the maximum prefix length to be matched.
length	Specifies the prefix length, ranges from 1 to 32.

Command Default

None

Command Modes

data-prefix-list configuration (config-data-prefix-list-{data-prefix-list list-name})

prefix-list configuration (config-prefix-list-{prefix-list list-name})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Lists are used to create groupings of similar objects, such as IP prefixes, sites, TLOC addresses, and AS paths, for use when configuring policy match conditions or action operations and for when applying a policy.

Data-prefix-list is a list of prefixes used in data-policy to define prefix and upper layer ports, either individually or jointly, for traffic matching.

Prefix-list is a list of prefixes used in route-maps. This command can be used to define the ip prefix for a data-prefix-list or prefix-list.

Example

The following example defines a data prefix list named Email-Server. The IP prefix of 10.10.10.10/32 is added to the data prefix list Email-Server.

```
Device(config)# policy
Device(config-policy)# lists
Device(config-lists)# data-prefix-list Email-Server
Device(config-data-prefix-list-Email-Server)# ip-prefix 10.10.10.10/32
```

The following example defines a prefix list named Web-Server. The IP prefix of 10.10.0.0/16 is added to the data prefix list Web-Server.

```
Device(config)# policy
Device(config-policy)# lists
Device(config-lists)# prefix-list Web-Server
Device(config-prefix-list-Web-Server))# ip-prefix 10.10.0.0/1
```

ip sla

To begin configuring a Cisco IOS IP Service Level Agreements (SLAs) operation and enter IP SLA configuration mode, use the **ip sla**command in global configuration mode. To remove all configuration information for an operation, including the schedule of the operation, reaction configuration, and reaction triggers, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip sla command.

Configure **static ip sla {value}** before configuring an endpoint-tracker. If you configure endpoint-tracker, which dynamically assigns IP SLA index. When you try to configure SLA through CLI template, if the index is same, then you might get an error stating SLA is already configured.

Examples

The following example shows how to configure a Cisco IOS IP SLA operation.

```
Device# config-transaction
Device(config)# ip sla 1
Device(config-ip-sla)#
```

ip sla reaction-configuration

To configure proactive threshold monitoring parameters for an IP Service Level Agreements (SLAs) operation, use the **ip sla reaction-configuration** command in global configuration mode. To disable all the threshold monitoring configuration for a specified IP SLAs operation, use the **no** form of this command.

Syntax Description

operation-number	Number of the IP SLAs operation for which reactions are to be configured.

react *monitored-element* (continued)	• **packetLoss** —Specifies that a reaction should occur if the packet loss value violates the upper threshold or lower threshold. The path of the packets is unknown. • **packetLossDS** —Specifies that a reaction should occur if the one-way destination-to-source packet loss value violates the upper threshold or lower threshold. • **packetLossSD** —Specifies that a reaction should occur if the one-way source-to-destination packet loss value violates the upper threshold or lower threshold. • **rtt** —Specifies that a reaction should occur if the round-trip time violates the upper threshold or lower threshold. • **timeout** —Specifies that a reaction should occur if there is a one-way timeout for the monitored operation. The **threshold-value** keyword does not apply to this monitored element.
action-type *option*	(Optional) Specifies what action or combination of actions the operation performs when threshold events occur. If the **threshold-typenever**keywords are defined, the **action-type** keyword is disabled. The *option* argument can be one of the following keywords: • **none** —No action is taken. This option is the default value. • **trapAndTrigger** —Trigger a Simple Network Management Protocol (SNMP) trap and start another IP SLAs operation when the violation conditions are met, as defined in the **trapOnly** and **triggerOnly** options. • **trapOnly** —Send an SNMP logging trap when the specified violation type occurs for the monitored element. • **triggerOnly** —Transition one or more target operation's operational state from pending to active when the violation conditions are met. The target operations to be triggered are specified using the **ipslareaction-trigger** command.
threshold-type average [*number-of-measurements*]	(Optional) When the average of a specified number of measurements for the monitored element exceeds the upper threshold or when the average of a specified number of measurements for the monitored element drops below the lower threshold, perform the action defined by the **action-type** keyword. For example, if the upper threshold for **reactrttthreshold-typeaverage3** is configured as 5000 ms and the last three results of the operation are 6000, 6000, and 5000 ms, the average would be 6000 + 6000 + 5000 = 17000/3 = 5667, thus violating the 5000 ms upper threshold. The default number of 5 averaged measurements can be changed using the *number-of-measurements* argument. The valid range is from 1 to 16. This syntax is not available if the **connectionLoss**, **timeout**, or **verifyError** keyword is specified as the monitored element, because upper and lower thresholds do not apply to these options.

threshold-type immediate	(Optional) When a threshold violation for the monitored element is met, immediately perform the action defined by the **action-type** keyword.
threshold-value *upper-threshold lower-threshold*	(Optional) Specifies the upper-threshold and lower-threshold values of the applicable monitored elements. See the Default Threshold Values for Monitored Elements table in the "Usage Guidelines" section for a list of the default values. **Note** For MOS threshold values (**reactmos**), the number is expressed in three digits representing ones, tenths, and hundredths. For example, to express a MOS threshold of 3.20, enter **320**. The valid range is from 100 (1.00) to 500 (5.00).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE `ip sla reaction-configuration` command.

Examples

```
ip sla 7001
 icmp-echo 172.31.17.222 source-ip 172.31.17.216
  request-data-size 64
  tag 7001:AVAILABILITY DSO-D7S
  frequency 30
ip sla schedule 7001 life forever start-time now
ip sla reaction-configuration 6001 react rtt threshold-value 40 40 threshold-type immediate
 action-type trapAndTrigger
ip sla reaction-configuration 6001 react timeout threshold-type immediate action-type
trapAndTrigger
ip sla reaction-configuration 6001 react packetLossDS threshold-value 1 1 threshold-type
immediate action-type trapAndTrigger
ip sla reaction-configuration 6001 react packetLossSD threshold-value 1 1 threshold-type
immediate action-type trapAndTrigger
ip sla reaction-configuration 7001 react timeout threshold-type immediate action-type
trapAndTrigger
```

ip sla responder

To enable the Cisco IOS IP Service Level Agreements (SLAs) Responder for general IP SLAs operations, use the **ip sla responder** command in global configuration mode. To disable the IP SLAs Responder, use the **no** form of this command.

Syntax Description

This command has no arguments or keywords.

Command Default

The IP SLAs Responder is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

This command is used on the destination device for IP SLAs operations to enable the sending and receiving of IP SLAs control packets. Enabling the IP SLAs Responder allows the generation of packet loss statistics on the device sending IP SLAs operations.

Prior to sending an operation packet to the IP SLAs Responder, the IP SLAs operation sends a control message to the IP SLAs Responder to enable the destination port.

For more information about this command, see the Cisco IOS XE `ip sla responder` command.

Examples

The following example shows how to enable the IP SLAs Responder:

```
ip sla responder
```

ip sla schedule

To configure the scheduling parameters for a single Cisco IOS IP Service Level Agreements (SLAs) operation, use the **ip sla schedule**command in global configuration mode. To stop the operation and place it in the default state (pending), use the **no** form of this command.

Syntax Description

operation-number	Number of the IP SLAs operation to schedule.
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
start-time	(Optional) Time when the operation starts.
hh **:** *mm* [**:** *ss*]	Specifies an absolute start time using hour, minute, and (optionally) second. Use the 24-hour clock notation. For example, **start-time 01:02** means “start at 1:02 a.m.,” and **start-time 13:01:30** means “start at 1:01 p.m. and 30 seconds.” The current day is implied unless you specify a *month* and *day*.
month	(Optional) Name of the month to start the operation in. If month is not specified, the current month is used. Use of this argument requires that a day be specified. You can specify the month by using either the full English name or the first three letters of the month.
day	(Optional) Number of the day (in the range 1 to 31) to start the operation on. If a day is not specified, the current day is used. Use of this argument requires that a month be specified.
pending	(Optional) No information is collected. This is the default value.
now	(Optional) Indicates that the operation should start immediately.

after *hh* **:** *mm* **:** *ss*	(Optional) Indicates that the operation should start *hh* hours, *mm* minutes, and *ss* seconds after this command was entered.
random *milliseconds*	(Optional) Adds a random number of milliseconds (between 0 and the specified value) to the current time, after which the operation will start. The range is from 0 to 10000.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ip sla schedule command.

Examples

```
Device(config)#
```

In the following example, operation 1 begins collecting data after a 5-minute delay:

```
Device(config)# ip sla schedule 1 start-time after 00:05:00
```

In the following example, operation 3 begins collecting data immediately and is scheduled to run indefinitely:

```
Device(config)# ip sla schedule 3 start-time now life forever
```

ip visibility cache entries

To configure the number of entries in IP visibility cache use the **ip visibility cache entries** command. To remove a configured number of entries, use the **no** form of this command.

ip visibility cache entries

Command Default

Disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Examples

Enable application-visibility on a router:

```
Router(config)# policy
Router(config-policy)# ip visibility cache entries 20
```

ipv6 access-list

To define an IPv6 access list and to place the device in IPv6 access list configuration mode, use the **ipv6 access-list**command in global configuration mode. To remove the access list, use the **no** form of this command.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE ipv6 access-list command.

Examples

```
Device# config-transaction
Device(config)# ipv6 access-list test300_v6
Device(config-ip-acl)# sequence 100 permit ipv6 any 2001:DB8::/32
Device(config-ip-acl)#
```

ipv6 visibility cache entries

To configure the number of entries in IPv6 visibility cache use the **ipv6 visibility cache entries** command. To remove a configured number of entries, use the **no** form of this command.

ipv6 visibility cache entries

Command Default

The minimum cache size value is 16. The maximum of total cache size (IPv4 cache + IPv6 cache) should not exceed the limit for each platform. If cache size is not defined and the platform is not in the list, then default maximum cache entries is 200k.

The maximum cache entries is the maximum concurrent flows that Cflowd can monitor. The maximum cache entries vary on different platforms. For more information, contact Cisco Support.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Examples

Enable application-visibility on a router:

```
Router(config)# policy
Router(config-policy)# ipv6 visibility cache entries 100
```

jitter

To specify the threshold jitter value that Optimized Edge Routing (OER) will permit for an exit link, use the **jitter** command in OER master controller configuration mode. To reset the maximum jitter value to its default value, use the **no** form of this command.

jitter
no jitter

Command Default

No jitter values are specified.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates. A app-probe-class keyword is added.

Usage Guidelines

The **jitter** command is used to specify the maximum tolerable jitter value permitted on an exit link. Jitter is a measure of voice quality where the lower the jitter value, the better the voice quality. If the jitter value is greater than the user-defined or the default value, OER determines that the exit link is out-of-policy and searches for an alternate exit link.

Another measure of voice quality is the estimated Mean Opinion Score (MOS). Use the **mos** command and the **jitter** command in an OER policy to define voice quality.

Examples

The following example shows how to configure the master controller to search for a new exit link if the jitter threshold value exceeds 20 milliseconds:

```
Router(config)# oer policy
Router(config-policy-map)# jitter threshold 20
```

lists

To create groupings of similar objects, such as IP prefixes, data-prefixes, and AS paths for use when configuring policy match conditions or action operations, and when to apply a policy, use the **lists** command in the policy configuration mode. To remove the groupings, use the **no lists** form of this command.

lists { **app-list** *app-list-name* | **as-path-list** *path-list* | **community-list** *community-name* | **data-ipv6-prefix-list** *data-prefix-list-name* | **data-prefix-list** *prefix-list-name* | **ext-community-list** *ext-community-name* | **ipv6-prefix-list** *ipv6-prefix-list-name* | **prefix-list** *prefix-list-name* }

no lists { **app-list** *app-list-name* | **as-path-list** *path-list* | **community-list** *community-name* | **data-ipv6-prefix-list** *data-prefix-list-name* | **data-prefix-list** *prefix-list-name* | **ext-community-list** *ext-community-name* | **ipv6-prefix-list** *ipv6-list-name* | **prefix-list** *list-name* }

Syntax Description

app-list *app-list-name*	(Optional) Lists of one or more applications or application families running on the subnets connected to the Cisco IOS XE Catalyst SD-WAN devices. Each app-list can contain either applications or application families, but not both. To configure multiple applications or application families in a single list, include multiple app or app-family options, by specifying one application or application family in each app or app-family option. An application list can contain a mix of applications or application families, but not a mix of the two. We recommend not adding an application to more than one application list, to avoid excessive memory use on devices. Maximum number of application families in an application list: 10
as-path-list *path-list*	(Optional) Lists of one or more BGP AS paths. You can write each AS as a single number or as a regular expression. To specify more than one AS in a single path, include the list in quotation marks (" "). To configure multiple AS paths in a single list, include multiple as-path options, and specifying one AS path in each option.
community-list *community-name*	(Optional) BGP community or communities in the route. list-name is the name of a BGP community list defined with a policy lists community-list command.
data-ipv6-prefix-list *data-prefix-list-name*	(Optional) List of one or more IPv6 prefixes. You can specify both unicast and multicast prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option. Does not support: ::/0
data-prefix-list *prefix-list-name*	(Optional) List of one or more prefixes. You can specify both unicast and multicast prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option. Does not support: 0.0.0.0/0
ext-community-list *ext-community-name*	(Optional) BGP extended community or communities in the route. Specifies the name of a BGP extended community list defined with a policy lists **ext-community-list** command.
ipv6-prefix-list *ipv6-prefix-list-name*	(Optional) List of one or more IPv6 prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.
prefix-list *prefix-list-name*	(Optional) List of one or more IP prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.

Command Default

None

Command Modes

policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see Lists in Localized Policy.

This example defines a data prefix list named Email-Server. The IP prefix of 10.0.0.0/9 is added to the data prefix list Email-Server.

```
Device(config)# policy
Device(config-policy)# lists
Device(config-lists)# data-prefix-list Email-Server
Device(config-config-data-prefix-list-Email-Server)# ip-prefix 10.0.0.0/9
```

This example defines an application list called CollabList, with two applications.

```
Device(config)# policy
Device(config-policy)# lists
Device(config-lists)# app-list CollabList
Device(config-app-list-CollabList)# app ms-office-365
Device(config-app-list-CollabList)# app ms-office-web-apps
```

This example defines an application list called CollabList, with two application families.

```
Device(config)# policy
Device(config-policy)# lists
Device(config-lists)# app-list CollabList
Device(config-app-list-CollabList)# app-family microsoft-office
Device(config-app-list-CollabList)# app-family audio-video
```

This example defines an IPv6 prefix list called PrefixList1.

```
Device(config)# policy
Device(config-policy)# lists
Device(config-lists)# data-ipv6-prefix-list PrefixList1
Device(config-data-ipv6-prefix-list-PrefixList1)# ipv6-prefix 2001:DB8::/32
```

lists data-prefix-list

To configure a list of one or more IP prefixes, use **lists data-prefix-list** command in policy configuration mode. Use the **no** form of this command to remove the list.

lists data-prefix-list *list-name* { **ip-prefix** *prefix/length* }

no lists

data-prefix-list *list-name* **ip-prefix** *prefix/length*	IP Prefix: List of one or more IP prefixes. You can specify both unicast and multicast prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option. Does not support: 0.0.0.0/0

Command Default

None.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Configure a list of prefixes:

```
Device# policy
Device(config-policy)# lists
Device(config-policy)# data-prefix-list Email-Server
Device(config-policy)# ip-prefix 10.0.0.0/8
```

lists (tag instance)

To create groupings of similar objects within a tag-instance, such as IP prefixes, data-prefixes, and app-lists for use when configuring tag-instances, use the **lists** command in tag-instances configuration mode. To remove the groupings, use the **no** form of this command.

lists [**app-list** *app-list-name*] [**data-ipv6-prefix-list** *data-prefix-list-name*] [**data-prefix-list** *prefix-list-name*]
no lists [**app-list** *app-list-name*] [**data-ipv6-prefix-list** *data-prefix-list-name*] [**data-prefix-list** *prefix-list-name*]

Syntax Description

app-list-name	(Optional) Lists of one or more applications or application families running on the subnets connected to the . Each app-list can contain either applications or application families, but not both. To configure multiple applications or application families in a single list, include multiple app or app-family options, by specifying one application or application family in each app or app-family option.
data-prefix-list-name	(Optional) List of one or more IPv6 prefixes. You can specify both unicast and multicast prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.

prefix-list-name	(Optional) List of one or more prefixes. You can specify both unicast and multicast prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.

Command Default

None

Command Modes

tag-instances configuration (config-tag-instances)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

Lists configuration under tag-instances are not the same as the lists configured under policy. Tag-instances require their own lists to be configured.

Examples

The following example shows how to configure a data prefix list named pfx1. The IP prefix of 10.20.24.0/24 is added to the data prefix list pfx1:

```
vSmart(config)# tag-instances
vSmart(config-tag-instances)# lists
vSmart(config-lists)# data-prefix-list pfx1
vSmart(config-config-data-prefix-list-pfx1)# ip-prefix 10.20.24.0/24
```

loss

To set the relative or maximum packet loss limit that Optimized Edge Routing (OER) will permit for an exit link, use the **loss** command in OER master controller configuration mode. To return the packet loss limit to the default value, use the **no** form of this command.

loss
no loss

Command Default

OER uses the following default value if this command is not configured or if the no form of this command is entered:

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The **loss** command is used to specify the relative percentage or maximum number of packets that OER will permit to be lost during transmission on an exit link. If packet loss is greater than the user-defined or the default value, OER determines that the exit link is out-of-policy and searches for an alternate exit link.

The **relative** keyword is used to configure the relative packet loss percentage. The relative packet loss percentage is based on a comparison of short-term and long-term packet loss. The short-term measurement reflects the

percentage of packet loss within a 5-minute period. The long-term measurement reflects the percentage of packet loss within a 60-minute period. The following formula is used to calculate this value:

Relative packet loss = ((short-term loss - long-term loss) / long-term loss) * 100

The master controller measures the difference between these two values as a percentage. If the percentage exceeds the user-defined or default value, the exit link is determined to be out-of-policy. For example, if long-term packet loss is 200 PPM and short-term packet loss is 300 PPM, the relative loss percentage is 50 percent.

The **threshold** keyword is used to configure the absolute maximum packet loss. The maximum value is based on the actual number of PPM that have been lost.

Examples

The following example configures the master controller to search for a new exit link if the difference between long- and short-term measurements (relative packet loss) is greater than 20 percent:

```
Router(config)# oer master
Router(config-oer-mc)# loss relative 200
```

The following example configures OER to search for a new exit link when 20,000 packets have been lost:

```
Router(config)# oer master
Router(config-oer-mc)# loss threshold 20000
```

match (access-control-list)

To enter the match configuration in an access list, use the **match** command in access control list sequence configuration mode. To remove match parameters, use the **no** form of this command.

match [**destination-data-prefix-list** *list-name* | **destination-ip** *ip/length* | **destination-port** *number* | **destination-tag-instance** *dest-tag-name* | **dscp** *number* | **packet-length** *number* | **plp** { **high** | **low** } | **protocol** *number* | **source-data-prefix-list** *list-name* | **source-ip** *ip/length* | **source-port** *number* | **source-tag-instance** *src-tag-name* | **tag-instance** *tag-name* | **tcp syn**]
no match [**destination-data-prefix-list** *list-name* | **destination-ip** *ip/length* | **destination-port** *number* | **destination-tag-instance** *dest-tag-name* | **dscp** *number* | **packet-length** *number* | **plp** { **high** | **low** } | **protocol** *number* | **source-data-prefix-list** *list-name* | **source-ip** *ip/length* | **source-port** *number* | **source-tag-instance** *src-tag-name* | **tcp syn**]

Syntax Description

destination-data-prefix-list *list-name*	(Optional) Matches the specified destination prefix list name.
destination-ip *ip/length*	(Optional) Matches the specified destination IP.
destination-port *number*	(Optional) Matches the specified destination port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
dscp *number*	(Optional) Matches the specified DSCP. The range is from 0 to 63.

packet-length *number*	(Optional) Matches the specified packet length. The range is from 0 to 65535. You can enter a range of values.
plp {**high** | **low** }	(Optional) Matches the specified packet's loss priority (PLP).
protocol *number*	(Optional) Matches the TCP or IP protocol number. The range is from 0 to 255.
source-data-prefix-list *list-name*	(Optional) Matches the specified source prefix list name.
source-ip *IP/length*	(Optional) Matches the specified source IP.
source-port *number*	(Optional) Matches the specified source port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
tcp syn	(Optional) Matches the TCP SYN flag.
source-tag-instance *src-tag-name*	(Optional) Matches the specified source tag instance name. The character range is from 1 to 127.
destination-tag-instance *dest-tag-name*	(Optional) Matches the specified destination tag instance name. The character range is from 1 to 127.

Command Default

None

Command Modes

Access control list sequence configuration (config-sequence-{sequence-number})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was modified. Localized policy match configuration is enhanced to include **source-tag-instance**, and **destination-tag-instance** keyword parameters in matching attributes.

Usage Guidelines

Access control lists (ACLs) perform packet filtering to control which packets move through an interface of a router. Packet filtering provides security by helping to limit network traffic, restrict the access of users and devices to a network, and prevent the traffic from leaving a network interface. An access control list is a sequential list consisting of match-action pairs.

The Sequence Numbering feature applies sequence numbers to match-action pairs. The match–action pairs are evaluated in an order, by sequence number, starting with the lowest numbered pair and ending when it matches the conditions in one of the pairs.

When a packet matches one of the match conditions, the defined action is taken. Or, if no match occurs, the default action is taken.

The **match** command can be used to enter the match configuration mode or to define match parameters.

Examples

The following example shows how to create or enter an access control list named ACL-TEST-1, define sequence #10, specify the destination IP address 10.10.10.10/32 as a match parameter, and define the action to drop when matched:

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# match destination-ip 10.10.10.10/32
Device(config-match)# exit
Device(config-sequence-10)# action drop
```

The following example shows how to configure a localized access control policy to include tags in the matching attributes:

```
Device(config)# policy
Device(config-policy)# access-list acl1
Device(config-access-list-acl1)# sequence 100
Device(config-sequence-100)# match
Device(config-match)# tag-instance orange
Device(config-match)# source-tag-instance red
Device(config-match)# action accept
Device(config-action)# count acl_input_wc
```

The following example shows how to remove destination IP address 10.10.10.10/32 as a match parameter from the access control list ACL-TEST-1, and sequence #10:

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# no match destination-ip 10.10.10.10/32
```

Table 4: Related Commands

Commands	Description
action	Specifies action for matched parameters.
access-list	Configures localized access list policy match.
app-route-policy	Configures centralized application route policy.
data-policy	Configures centralized data policy.
sequence	Configures the sequence number for a match-action pair in an access control list.

match as-path

To match a Border Gateway Protocol (BGP) autonomous system (AS) path access list, use the **match as-path** command. To remove a path list entry, use the **no** form of this command.

match as-path *name*

no match as-path *name*

Syntax Description

name	Autonomous system path access list. You can configure up to 32 access list names.

Command Default

No path lists are defined.

Command Modes

Route-map configuration mode (config-route-map)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

The values set by the **match as-path** command overrides global values.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command is ignored; that is, the route is not advertised for outbound route maps and is not accepted for inbound route maps. If you want to modify some particular data, you must configure a second route-map section with an explicit match specified.

Examples

This example sets the autonomous system path to match BGP autonomous system path access list:

```
Device(config)# route-map rmap1 permit 10
Device(config-route-map)# match as-path 120
```

match (data policy)

To configure matching attributes in a data policy, use the **match** command in data policy sequence configuration mode. To remove match parameters, use the **no** form of this command.

match [**app-list** *app-list-name* | **destination-data-ipv6-prefix-list** *ipv6-prefix-list-name* | **destination-data-prefix-list** *ipv4-prefix-list-name* | **destination-ip** *ip/length* | **destination-port** *number* | **destination-tag-instance** *dest-tag-name* | **dscp** *number* | **packet-length** *number* | **plp** { **high** | **low** } | **protocol** *number* | **source-data-prefix-list** *list-name* | **source-ip** *ip/length* | **source-port** *number* | **source-tag-instance** *src-tag-name* | **tag-instance** *tag-name* | **tcp** **syn**]
no match [**app-list** *app-list-name* | **destination-data-ipv6-prefix-list** *ipv6-prefix-list-name* | **destination-data-prefix-list** *list-name* | **destination-ip** *ip/length* | **destination-port** *number* | **destination-tag-instance** *dest-tag-name* | **dscp** *number* | **packet-length** *number* | **plp** { **high** | **low** } | **protocol** *number* | **source-data-prefix-list** *list-name* | **source-ip** *ip/length* | **source-port** *number* | **source-tag-instance** *src-tag-name* | **tag-instance** *tag-name* | **tcp** **syn**]

Syntax Description

app-list *app-list-name*	(Optional) Matches the specified application list name. The application list name character range is from 1 to 32.
destination-data-ipv6-prefix-list *ipv6-prefix-list-name*	(Optional) Matches the specified destination ipv6 prefix list name. The destination ipv6 prefix list name character range is from 1 to 32.
destination-data-prefix-list *ipv4-prefix-list-name*	(Optional) Matches the specified destination prefix list name. The destination ipv4 prefix list name character range is from 1 to 32.

destination-ip *ipv4 prefix (ip/length)*	(Optional) Matches the specified destination IP.
destination-port *number*	(Optional) Matches the specified destination port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). Range: 0 to 65535
dscp *number*	(Optional) Matches the specified DSCP. The range is from 0 to 63.
packet-length *number*	(Optional) Matches the specified packet length. The range is from 0 to 65535. You can enter a range of values.
plp {**high** | **low** }	(Optional) Matches the specified packet's loss priority (PLP).
protocol *number*	(Optional) Matches the TCP or IP protocol number. The range is from 0 to 255.
source-data-prefix-list *list-name*	(Optional) Matches the specified source prefix list name.
source-ip *IP/length*	(Optional) Matches the specified source IP.
source-port *number*	(Optional) Matches the specified source port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
tcpsyn	(Optional) Matches the TCP SYN flag.
traffic-to	(Optional) Matches the specified traffic-to service or access or core.
source-tag-instance *src-tag-name*	(Optional) Matches the specified source tag instance name. The character range is from 1 to 127.
destination-tag-instance *dest-tag-name*	(Optional) Matches the specified destination tag instance name. The character range is from 1 to 127.
tag-instance *tag-name*	(Optional) Matches the specified tag instance name. The character range is from 1 to 127.

Command Default

No match criterion is specified.

Command Modes

Data policy sequence configuration (config-sequence)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

When a packet matches one of the match conditions, the defined action is taken. Or if no match occurs, the default action is taken.

The **match** command can be used to enter the match configuration mode or to define match parameters.

Examples

The following example shows how to configure centralized data policy to include tags in matching attributes:

```
vSmart(config)# policy
vSmart(config-policy)# data-policy DP1
vSmart(config-data-policy-DP1)# vpn-list vpn1
vSmart(config-vpn-list-vpn1)# sequence 100
vSmart(config-sequence-100)# match
vSmart(config-match)# tag-instance orange
vSmart(config-match)# source-tag-instance red
vSmart(config-match)# destination-tag-instance blue
vSmart(config-match)# action accept
vSmart(config-action)# count count1
```

Table 5: Related Commands

Commands	Description
action	Specifies action for matched parameters.
sequence	To configure the sequence number for a match-action pair in an access control list.
access-list	To configure localized access list policy match.
match (access-control-list)	To configure match attributes in an access list policy.

match ip address

To distribute any routes that have a destination IP network number address that is permitted by a standard access list, an expanded access list, or a prefix list, use the **match ip address** command. To remove the **match ip address** entry, use the **no** form of this command.

match ip address { **prefix-list** | [*prefix-list-name*] }

no match ip address { **prefix-list** | [*prefix-list-name*] }

Syntax Description

prefix-list*prefix-list-name*	Distributes routes based on a prefix list. The prefix list name can be any alphanumeric string up to 63 characters. The ellipsis indicates that multiple values can be entered, up to 32 prefix lists.

Note In Cisco Catalyst SD-WAN Manager Release 20.15.1, when pushing a CLI template to a device running a version earlier than Cisco Catalyst SD-WAN Manager Release 20.15.1, the CLI template must include the following configuration lines under route-map:

```
match ip address prefix-list xyz
match ip address prefix-list-deprecated xyz
match ip address 33
match ip address access-list 33
```

Command Default

No prefix lists are specified.

Command Modes

Route-map configuration mode (config-route-map)

Command History

Note In Cisco Catalyst SD-WAN Manager Release 20.15.1, when pushing a CLI template to a device running a version earlier than Cisco Catalyst SD-WAN Manager Release 20.15.1, the CLI template must include the following configuration lines under route-map:

```
description SET COMMUNITY FOR EDGE ROUTES
description-deprecated SET COMMUNITY FOR EDGE ROUTES
```

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

This example shows how to match routes that have addresses specified by an access list test:

```
Device(config)# route-map rmap1 deny 10
Device(config-route-map)# match ip address prefix-list prfx1
```

match protocol attribute application-group

To configure the match criterion for a class map based on the specified application group, use the **match protocol attribute application-group** command in class-map configuration mode. To remove the application-group match criterion from the class map, use the **no** form of this command.

Supported Parameters

application-group	Name of the application group as a matching criterion. See the "Usage Guidelines" section for a list of application groups supported by most routers.
application-name	(Optional) Name of the application. When the application name is specified, the application is configured as the match criterion instead of the application group.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE `match protocol attribute application-group` command.

Examples

```
class-map match-any ART_APPLICATIONS
 match protocol attribute application-group ms-cloud-group
```

parameter-map type inspect

To configure an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action, use the **parameter-map type inspect** command in global configuration mode. To delete an inspect-type parameter map, use the **no** form of this command.

Syntax Description

parameter-map-name	Name of the inspect parameter map.
global	Defines a global inspect parameter map.
default	Defines a default inspect parameter map.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE parameter-map type inspect command.

Examples

The following example shows the inspect type parameter map configuration:

```
Device(config)# parameter-map type inspect parameter-map type inspect aip
Device(config)# parameter-map type inspect parameter-map type global
```

policer

To define a policer profile and to enter the policer configuration mode, use the **policer** command in policy configuration mode. To remove the policer profile, use the **no** form of this command.

policer *policer-name*
no policer *policer-name*

Syntax Description

policer-name	Name of policer.

Command Default

None

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

This command can be used to define a policer profile and enter the policer configuration mode where further configurations can be done.

Example

The following example defines a policer profile named pol1. It sets the rate to 500,000,000 bps, and burst size to 15,000 bytes, and configures to drop the traffic if the burst size or traffic rate is exceeded.

```
Device(config)# policy
Device(config-policy)# policer pol1
Device(config-policy-pol1)# rate 500000000
Device(config-policy-pol1)# burst 15000
Device(config-policy-pol1)# exceed drop
```

The following example applies a policer using an Access List named ACL-TEST-1.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 1
Device(config-sequence-1)# action drop
Device(config-action)# policer pol1
```

Note Rate, burst, and exceed must be defined before committing, otherwise the commit is aborted.

Table 6: Related Commands

Commands	Description
burst	Maximum traffic burst size, in bytes. The range is from 15000 to 10000000.
exceed	Action to take when the burst size or traffic rate is exceeded.

Commands	Description
rate	Bandwidth for 1G interfaces, the range is from 8 to 1000000000 bps; for 10G interfaces, the range is from 8 to 10000000000 bps.

policy

To enter policy configuration mode or configure policies, use the **policy** command in global configuration mode. To remove policy configurations, use the **no** form of this command.

policy [**access-list** | **app-visibility** | **class-map** | **cloud-qos-service-side** | **flow-visibility** | **flow-stickiness-disable** | **implicit-acl-logging** | **ipv6** | **lists** | **log-frequency** | **mirror** | **policer** | **qos-map** | **qos-scheduler** | **rewrite-rule** | **route-policy** | **utd-tls-decrypt**]
no policy [**access-list** | **app-visibility** | **class-map** | **cloud-qos-service-side** | **flow-visibility** | **implicit-acl-logging** | **ipv6** | **lists** | **log-frequency** | **mirror** | **policer** | **qos-map** | **qos-scheduler** | **rewrite-rule** | **route-policy** | **utd-tls-decrypt**]

Syntax Description

access-list	(Optional) Configures ACLs.
app-visibility	(Optional) Enables/disables application visibility.
class-map	(Optional) Configures class map.
cloud-qos	(Optional) Enables/Disables QoS for cEdge Cloud.
cloud-qos-service-side	(Optional) Enables/Disables QoS for cEdge Cloud on service side.
flow-visibility	(Optional) Enables/Disables flow visibility.
flow-stickiness-disable	(Optional) Enables/Disables flow stickiness.
implicit-acl-logging	(Optional) Enables/Disables logging of implicit acl packet drops.
ipv6	(Optional) Configures IPv6 policy.
lists	(Optional) Configures lists.
log-frequency	(Optional) Logs frequency as packet counts.
mirror	(Optional) Configures traffic mirror.
policer	(Optional) Configures policer.
qos-map	(Optional) Configures QoS map.
qos-scheduler	(Optional) Configures QoS scheduler.
rewrite-rule	(Optional) Configures rewrite rule.
route-policy	(Optional) Configures route policies

utd-tls-decrypt	(Optional) Configures TLS Decryption policies.

Command Default

Default behavior or values vary based on optional arguments or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Release 17.6.1a	The **flow-stickiness-disable** keyword is added.
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	The **flow-stickiness-disable** keyword is added for NAT66 DIA.

Usage Guidelines

Policy influences the flow of data traffic and routing information among Cisco devices in the overlay network. This command can be used to enter the policy configuration mode where further configurations can be done or to configure policies with optional arguments or keywords.

Example

The following example enters the policy configuration mode. It defines a policer profile named pol1 and sets the burst size to 15,000 bytes, and rate to 500,000,000 bps, and configures to drop the traffic if the burst size or traffic rate is exceeded.

```
Device(config)# policy
Device(config-policy)# policer pol1
Device(config-policy-pol1)# burst 15000
Device(config-policy-pol1)# rate 500000000
Device(config-policy-pol1)# exceed drop
Device(config-policy-pol1)# flow-stickiness disable
```

The following example enables app-visibility.

```
Device(config)# policy app-visibility
```

The following example disables flow-stickiness.

```
Device(config-policy)# flow-stickiness disable
```

policy ip visibility

To manually enable or disable policy feature fields visibility, use the **ip visibility** command in policy configuration mode. To disable the feature fields visibility, use the **no** form of the command.

ip visibility features [**cxp** | **dre** | **fec** | **multi-sn** | **pktdup** | **probe-saas** | **sslproxy** | **ulogging**] { *enable* | *disable* }
no ip visibility features [**cxp** | **dre** | **fec** | **multi-sn** | **pktdup** | **probe-saas** | **sslproxy** | **ulogging**] { *enable* | *disable* }

Syntax Description

cxp	cloud express feature

dre	APPQOE DRE feature.
fec	FEC feature
multi-sn	APPQOE Multi SN feature
pktdup	Packet duplicate feature
probe-saas	Probe saas feature
sslproxy	SSLProxy feature
ulogging	Unified logging feature

Command Default

Default behavior or values vary based on optional arguments or keywords.

Command Modes

Policy configuration mode (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.9.1a	This command was introduced.

Usage Guidelines

Starting from Cisco IOS XE Release 17.9.1a, you can manually enable or disable the feature fields visibility. Even if the feature fields are enabled automatically due to upgrade, you need to disable fields manually using **ip visibility features** *features***disable** command or use the **no** form of the command.

The disable behavior is same as **no policy ip visibility features**.

The following example shows how to enable the cxp feature fields using the **ip visibility** command:

```
Device(config)# policy ip visibility features cxp enable
```

The following shows how to diable the cxp feature using the **no** form or **disable** command:

```
Device(config)# no policy ip visibility features cxp
Device(config)# policy ip visibility features cxp disable
```

policy log-rate-limit

To limit the number of policy flow logs in a given second, use the **policy log-rate-limit** command in global configuration mode . To disable the limit, use the **no** form of this command.

policy log-rate-limit

This command has no keywords or arguments.

Command Default

The default is 25 messages logged per second.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.11.1a	This command was introduced.

Usage Guidelines

The log-rate-limit range is 1 to 10000. For Cisco IOS XE Release 17.11.1a, a maximum rate limit supported is 500.

Example

The following is an example of this command:

```
Device(config)# policy log-rate-limit

(<1..10000> logs per second. Default is 25) (25):
```

The following example shows how to specify a rate limit:

```
Device# show sdwan running-config policy
policy
no app-visibility
no app-visibility-ipv6
no flow-visibility
no flow-visibility-ipv6
no implicit-acl-logging
log-frequency        1000
log-rate-limit    25
access-list ACL1
  sequence 1
   match
    dscp 10
   !
   action accept
    count CNT2
    log
   !
  !
  default-action drop
!
!
```

queue-limit

To specify or modify the maximum number of packets the queue can hold for a class configured in a policy-map, use the **queue-limit** command in policy-map class configuration mode. To remove the queue packet limit from a class, use the **no** form of this command.

queue-limit { *queue-limit-size* { **bytes** | **ms** | **packets** | **us** } **dscp** *dscp-value* }

no queue-limit { *queue-limit-size* { **bytes** | **ms** | **packets** | **us** } **dscp** *dscp-value* }

Syntax Description

queue-limit-size	The maximum size of the queue. Valid range is a number from 1 to 8192000. The maximum varies according to the optional unit of measure keyword specified (bytes, ms, packets, or us).
bytes	(Optional) Indicates that the unit of measure is bytes. Valid range for bytes is a number from 1 to 64000000.
ms	(Optional) Indicates that the unit of measure is milliseconds. Valid range for milliseconds is a number from 1 to 3400.
packets	(Optional) Indicates that the unit of measure is packets. Valid range for packets is a number from 1 to 8192000.
us	(Optional) Indicates that the unit of measure is microseconds. Valid range for microseconds is a number from 1 to 512000.
dscp *dscp-value*	(Optional) Specify the dscp value. Valid options are 0-63, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, vs6, cs7, default, dscp, ef, precedence.

Command Default

None

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
	Qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Weighted fair queuing (WFQ) creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queuing process. When the maximum packet threshold you defined for the class is reached, queuing of any further packets to the class queue causes tail drop.

You use queue limits to configure Weighted Tail Drop (WTD). WTD ensures the configuration of more than one threshold per queue. Each class of service is dropped at a different threshold value to provide for QoS differentiation.

You can configure the maximum queue thresholds for the different subclasses of traffic.

This command can be used to specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map.

Example

The following example shows defining the maximum queue limit to 108 packets.

```
Router(config)# policy-map POL123
Router(config-pmap)# class CLASS123
Router(config-pmap-c)# bandwidth 1000
Router(config-pmap-c)# queue-limit 108 packets
```

rate

To define the traffic rate for a policer profile, use the **rate** command in policer configuration mode.

rate *bps*

Note Rate is a required parameter in a policer profile. Entering **no rate** *bps* is valid, but causes **commit** to fail.

Syntax Description

bps	Bandwidth for 1G interfaces, the range is from 8 to 1000000000 bps; for 10G interfaces, the range is from 8 to 10000000000 bps.

Command Default

None

Command Modes

Policer configuration (config-policer-{policer-profile-name})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

To configure policing parameters, create a policer that specifies the maximum bandwidth and burst rate for traffic on an interface, and how to handle traffic that exceeds these values.

This command can be used to define the traffic rate for a policer profile.

Example

The following example defines a policer profile named pol1. It sets the rate to 500,000,000 bps, and burst size to 15,000 bytes, and configures to drop the traffic if the burst size or traffic rate is exceeded.

```
Device(config)# policy
Device(config-policy)# policer pol1
Device(config-policy-pol1)# rate 500000000
Device(config-policy-pol1)# burst 15000
Device(config-policy-pol1)# exceed drop
```

The following example applies a policer using an Access List named ACL-TEST-1.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 1
Device(config-sequence-1)# action drop
Device(config-action)# policer pol1
```

Note Rate, burst, and exceed must be defined before committing, otherwise the commit is aborted.

Table 7: Related Commands

Commands	Description
burst	Maximum traffic burst size, in bytes. The range is from 15000 to 10000000.
exceed	Action to take when the burst size or traffic rate is exceeded.

request-data-size

To set the protocol data size in the payload of a Cisco IOS IP Service Level Agreements (SLAs) operation's request packet, use the **request-data-size**command in the appropriate submode of IP SLA configuration, auto IP SLA MPLS configuration, IP SLA monitor configuration, or IP SLA template parameters configuration mode. To return to the default value, use the **no** form of this command.

Syntax Description

bytes	Size of the protocol data in the payload of the request packet of the operation, in bytes. Range is from 0 to the maximum supported by the protocol.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE `request-data-size` command.

IP SLA Configuration

```
ip sla 6001
 udp-jitter 172.31.11.85 44444 source-ip 172.31.17.220 num-packets 100
  request-data-size 64
  tag 6001:UDP64 HNZ-H7Z
  frequency 300
```

rewrite-rule

To configure a rewrite rule to overwrite the DSCP field of a packet's outer IP header, mark transit traffic with an 802.1p CoS value, and apply a rewrite rule on an interface use the **rewrite-rule** command. A rewrite rule is applied to packets that are transmitted out of the interface.

You can apply rewrite rules to both unicast and multicast traffic.

rewrite-rule *rule-name* [**class** *class-name*] { **high** | **low** } **dscp** *dscp-value* **mpls-exp-topmost** *mpls-exp-value*

no rewrite-rule *rule-name* [**class** *class-name*] { **high** | **low** } **dscp** *dscp-value* **mpls-exp-topmost** *mpls-exp-value*

Syntax Description

dscp *dscp-value*	DSCP value: Assign a DSCP value to transit traffic. Range: 0 through 63
mpls-exp-topmost *mpls-exp-value*	Multiprotocol label switching experimental field (MPLS EXP) value: Assign an MPLS EXP value to traffic. **Note** If you use the **dscp** keyword to assign a DSCP value to traffic that uses MPLS, the command maps the DSCP value to an MPLS EXP value using the standard mapping of DSCP to MPLS EXP. For information about this mapping, see the QoS: Classification Configuration Guide, Cisco IOS XE 17. Range: 0 through 7
class *class-name*	Forwarding class name: Name of the forwarding class.
rule-name	Rewrite rule name: Name of the rewrite rule. It can be a text string from 1 through 32 characters long. When you apply a rewrite rule to an interface, the name must match one that you specified when you created the rule with the **policy rewrite-rule** configuration command.

Note Cisco IOS XE SD-WAN supports a maximum number of only 16 rewrite rules and only 64 entries per rewrite rule.

Command Default

None.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Added the **mpls-exp-topmost** keyword.

Usage Guidelines

For traffic using IP, the **rewrite-rule** command assigns a value to the DSCP field of the IP header for outgoing traffic.

In carrier supporting carrier (CSC) scenarios, which use MPLS, the **rewrite-rule** command assigns the MPLS EXP value in the MPLS header for outgoing traffic. Use the **rewrite-rule** command using a CLI template or CLI add-on template, and the **mpls-exp-topmost** keyword. If, in a CSC scenario, you use the **dscp** keyword

instead, such as with legacy configurations created before support of the **mpls-exp-topmost** keyword, the **rewrite-rule** command converts the DSCP value to an MPLS EXP value in accordance with the standard mapping of DSCP to MPLS EXP values. The benefit of using the **mpls-exp-topmost** keyword is that you can set the MPLS EXP value directly, without depending on the mapping of DSCP to MPLS EXP values.

The following example shows how to create a rewrite rule:

```
Device(config)# policy
Device(config-policy)# rewrite-rule Branch-QoS-Rewrite-Template
Device(config-policy)# class BULK low dscp 10
Device(config-policy)# class BULK high dscp 10
```

The following example applies to a CSC scenario. It defines a rewrite rule called rw-exp, which sets the MPLS EXP value for outgoing traffic to 1 and applies the rule to the outbound interface.

Define the rewrite rule using the **mpls-exp-topmost** keyword, as follows:

```
sdwan
  policy
    rewrite-rule rw-exp
      class BULK low mpls-exp-topmost 1
      class BULK high mpls-exp-topmost 1
```

Alternatively, if you define the rewrite rule using the **dscp** keyword, the **rewrite-rule** command converts the value of 10 to an MPLS EXP value of 1, in accordance with the standard mapping of DSCP to MPLS EXP values.

```
sdwan
  policy
    rewrite-rule rw-exp
      class BULK low dscp 10
      class BULK high dscp 10
```

Apply the rule as follows:

```
sdwan
interface GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color public-internet restrict
  exit
  rewrite-rule rw-exp
exit
```

service-area

To classify traffic based on service areas for different Microsoft 365 (M365) cloud services, use the **service-area** command in Policy configuration (config-policy) mode.

service-area *service-area-name*

no service-area *service-area-name*

Syntax Description

service-area name	Specifies one or more service-areas that the M365 cloud application belongs to. The four service areas are: • **Common**: M365 Pro Plus, Office in a browser, Azure AD, and other common network endpoints. • **Exchange**: Exchange Online and Exchange Online Protection. • **SharePoint**: SharePoint Online and OneDrive for Business. • **Skype**: Skype for Business and Microsoft Teams.

Command Default

There are no default values.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

- SD-AVC must be enabled on Cisco vManage.
- You can add only one sequence with a match for a service-area, to a policy configuration in Cisco vManage.

The following example shows how to specify a service area:

```
policy
 app-route-policy test_policy
  vpn-list vpn-list-1
   sequence 111
    match
     source-ip 0.0.0.0/0
     service-area exchange sharepoint skype
     traffic-category optimize-allow
    !
    action
     count count-name
     cloud-saas
    !
   !
  !
```

service-policy

To attach a policy map to an input interface, a virtual circuit (VC), an output interface, or a VC that will be used as the service policy for the interface or VC, use the **service-policy** command in the appropriate configuration mode. To remove a service policy from an input or output interface or from an input or output VC, use the **no** form of this command.

Supported Parameters

type	(Optional) Determines the exact pattern to look for in the protocol stack of interest.
input	Attaches the specified policy map to the input interface or input VC.
policy-map-name	The name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters in length.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `service-policy` command.

Examples

```
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
interface GigabitEthernet0/0/2
 service-policy type epbr input test100
```

set ip vrf

To indicate where to forward packets that pass a match clause of a route map for policy routing when the next hop must be under a specified virtual routing and forwarding (VRF) name, use the **setipvrf** command in policy map class configuration mode. To disable this feature, use the **no** form of this command.

Supported Parameters

vrf-name	Name of the VRF.
next - hop *ip-address*	IP address of the next hop to which packets are forwarded. The next hop must be an adjacent router.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `set ip vrf` command.

Examples

```
ip access-list extended test300
 100 permit ip any 0.0.0.2 255.255.255.0
ip access-list extended test100
 100 permit ip any 0.0.0.2 255.255.255.0
class-map match-any test300
 match access-group name test300
```

```
class-map match-any test100
 match access-group name test100
policy-map type epbr test300
 class test300
  set ipv4 vrf 300 next-hop 203.0.113.255
policy-map type epbr test100
 class test100
  set ipv4 vrf 100 next-hop 203.0.113.255
interface GigabitEthernet0/0/1
 service-policy type epbr input test300
interface GigabitEthernet0/0/2
 service-policy type epbr input test100

ipv6 access-list test300_v6
  sequence 100 permit ipv6 any 2003::2/64
ipv6 access-list test100_v6
 sequence 100 permit ipv6 any 2001::2/64
class-map match-any test300_v6
 match access-group name test300_v6
class-map match-any test100_v6
 match access-group name test100_v6
policy-map type epbr test300_v6
 class test300_v6
  set ipv6 vrf 300 next-hop 2003::2
policy-map type epbr test100_v6
 class test100_v6
  set ipv6 vrf 100 next-hop 2001::2
interface GigabitEthernet0/0/1
 service-policy type epbr input test300_v6
interface GigabitEthernet0/0/2
 service-policy type epbr input test100_v6
```

set ip next-hop verify-availability

To configure policy routing to verify the reachability of a single or multiple IPv4 or IPv6 next hops of a policy map before the router performs policy routing to the next hops, use the **set ipv4 next-hop verify-availability** or **set ipv6 next-hop verify-availability** commands respectively in the policy-map class mode.

To disable this feature, use the **no** form of this command

set [**ipv4** | **ipv6**] [**vrf** *vrf-name* | **global**] **next-hop verify-availability** [*ip-address* ... [*ip-address*]] [*nhop-address sequence* **track** *object-number*]
no [**ipv4** | **ipv6**] [**vrf** *vrf-name* | **global**] **next-hop verify-availability** [*ip-address* ... [*ip-address*]] [*nhop-address sequence* **track** *object-number*]

Syntax Description

vrf *vrf-name*	Specifies that the next hop reachability should be verified for a specific VRF.
global	Specifies that the next hop reachability should be verified at a global level
ip-addresses	Specifies a single or multiple next hops addresses to verify their reachability
nhop-address	Specifies a single next hop address to verify its reachability
sequence	Specifies the sequence to be inserted into the next-hop list. The range is from 1 to 65535.
track	Sets the next hop depending on the state of a tracked object.

object-number	Specifies tracked object number. The range is from 1 to 1000.

Command Default

This command s disabled by default.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	This command was introduced.

Usage Guidelines

Use this command to enable policy routing to verify the reachability of a single or multiple IPv4 or IPv6 next hop addresses. This command can be configured globally or for a vrf. The options after **set [ipv4|ipv6] next-hop verify-availability** can be configured in any order.

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the ip-address argument

Example

The following example shows how to verify the availability of an IPv4 next hop address, and enable tracker for the address.

```
Device(config)# class-map match-any test100

Device(config-cmap)# match acess-group name test100

Device(config-cmap)# policy-map type epbr 1

Device(config-pmap)# class test300

Device(config-pmap-c)# set ipv4 vrf 300 next-hop verify-availability 10.10.0.2 10 track 2
```

The following example shows how to verify the availability of an IPv6 next hop address and enable tracker for the address.

```
Device(config)# class-map match-any test100_v6

Device(config-cmap)# match acess-group name test100_v6

Device(config-cmap)# policy-map type epbr test300_v6

Device(config-pmap)# class test300_v6

Device(config-pmap-c)# set ipv6 vrf 300 next-hop verify-availability 2001:DB8::1 10 track
4
```

sequence

To specify a sequence number for the permit condition in the IP access list, use the **sequence** command in the appropriate configuration mode. To remove a sequence number from an IP access list, use the **no** form of this command.

sequence *sequence-number* { **permit** } { **ipv6** } { **any** *ipv6-address* }

Syntax Description

sequence-number	Permits statements to position the statement in the list.
permit	Sets permit conditions for an IPv6 access list.
ipv6	Sets the IPv6 address to set permit conditions.
any *ipv6-address*	Specifies any source or any destination host as an abbreviation for the *source-addr* or *destination-addr value* and the *source-wildcard* or *destination-wildcard* value of 0.0.0. 255.255.255.255.

Command Default

There are no specific conditions under which a packet passes the access list.

Command Modes

IPv6 access-list configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Examples

```
Device(config)# ipv6 access-list test300_v6
Device(config-ipv6-acl)# sequence 100 permit ipv6 any 2001:DB8::/32
```

sequence (access-control-list)

To define the sequence number for a match-action pair in an access control list, use the **sequence** command in access control list configuration mode. To remove the sequence number and match-action pair, use the **no** form of this command.

sequence *number*
no sequence *number*

Syntax Description

number	Sequence number ranging from 0 to 65535.

Command Default

None

Command Modes

Access Control List configuration (config-access-list-{ACL-name})

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Access control lists (ACLs) perform packet filtering to control which packets move through an interface of a router. The packet filtering provides security by helping to limit the network traffic, restrict the access of

users and devices to a network, and prevent the traffic from leaving a network interface. An access control list is a sequential list consisting of match-action pairs.

The sequence numbering feature applies sequence numbers to match-action pairs. The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when it matches the conditions in one of the pairs.

When a packet matches one of the match conditions, the defined action is taken. Or if no match occurs, the default action is taken.

This command can be used to define the sequence number for a match-action pair in an access control list.

Example

The following example creates an access control list named ACL-TEST-1, defines sequence #10, specifies destination IP 10.10.10.10/32 as a match parameter and defines the action to drop when matched.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# sequence 10
Device(config-sequence-10)# match destination-ip 10.10.10.10/32
Device(config-match)# exit
Device(config-sequence-10)# action drop
```

The following example creates an access control list named ACL-TEST-1 and removes sequence #10 and the match-action pair.

```
Device(config)# policy
Device(config-policy)# access-list ACL-TEST-1
Device(config-access-list-ACL-TEST-1)# no sequence 10
```

Table 8: Related Commands

Commands	Description
default-action	Specifies default action for matched parameters.

sla-class

To configure a Service Level Agreements (SLA) class, use the **sla-class** command in global configuration mode. You can create groups of properties for a policy to use with application-aware routing. You can configure a maximum of six SLA classes for Cisco IOS XE SD-WANs.

sla-class *sla-class-name* **jitter** *jitter* **latency** *latency* **loss** *percentage* **app-probe-class** *app-probe-class-name* [**fallback-to-best-tunnel criteria** *criteria* **jitter** *jitter* **latency** *latency* **loss** *percentage*]

no sla-class *sla-class-name*

Syntax Description

jitter *milliseconds*	Specifies the jitter on the connection. Packets matching the policy for application-aware routing that have the specified jitter or a lower jitter value. *Range:* 1 through 1000 milliseconds

latency *milliseconds*	Specifies the latency on the connection. Packets matching the policy for application-aware routing that have the specified latency or a lower latency value. *Range:* 1 through 1000 milliseconds
loss *percentage*	Specifies the packet loss on the connection. Packets matching the policy for application-aware routing that have the specified packet loss or a lower packet loss value. *Range:* 0 through 100 percentage
app-probe-class *app-probe-class-name*	Specifies the app-probe-class configured on the SLA class.
(Optional) **fallback-to-best-tunnel**	(Optional) Specifies the fallback-to best-tunnel option. When this option is selected, the packet can choose the best path available using the criteria.
criteria	Specifies the criteria. The options are a combination of one or more of loss, latency, and jitter values.

Command Default

There are no default values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates. A app-probe-class keyword is added.
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	A fallback-best-tunnel and criteria keywords are added.

The following example shows the SLA configuration for a latency of 50 millisecond and a app-probe-class along with the fallback-best-tunnel option:

```
Device(config)# policy
Device(config-policy)# sla-class 50ms-sla
Device(config-policy))# latency 50
Device(config-policy))# app-probe-class real-time-video
Device(config-policy))# fallback-best-tunnel
Device(config-policy))# criteria loss jitter
```

sig

To enable VPN multiplexing and demultiplexing, use the **sig** command in the action configuration mode. The SIG tunnel is created in the VPN 0 (global) space. The SIG tunnel configuration is identical to other

IPSEc tunnel configurations, excluding the inclusion of the **tunnel vrf multiplexing** command. To remove the multiplexing, use the **no sig** form of this command.

sig

no sig

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes action configuration (config-action)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

```
vSmart(config)# policy
vSmart(config-policy)# data-policy sig_ha_zscaler_data_policy_cedge
vSmart(config-data-policy-sig_ha_zscaler_data_policy_cedge)# vpn-list vpn_1
vSmart(config-vpn-list-vpn_1)# sequence 100
vSmart(config-sequence-100)# match destination-ip 10.10.10.10/32
vSmart(config-match)# protocol 17
vsmart(config-match)# !
vsmart(config-match)# action accept
vsmart(config-action)# count sig_ha_zscaler_datapolicycnt100
vsmart(config-action)# sig
vsmart(config-action)# exit
vsmart(config-action)# exit
```

site-list

To list of one or more identifiers of sites in the Cisco SD-WAN overlay network, use the **site-list** command in the policy lists configuration mode. To remove the listing of sites, use the **no site-list** form of this command.

site-list *list-name*

no site-list *list-name*

Syntax Description

list-name	List of sites to which to apply the policy. The *list-name* must match a list name that you configured in the **policy lists site-list** part of the configuration.

Command Default None

Command Modes policy lists configuration (config-lists)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

The following example configures site lists to use for control and data policies that contain overlapping site identifiers, and apply the policies to this site lists on a Cisco vSmart Controller.

```
vSmart(config)# policy
vSmart(config-policy)# lists
vSmart(config-lists)# site-list us-control-list
vSmart(config-lists)# site-id 1-200
vSmart(config-lists)# site-list emea-control-site-list
vSmart(config-lists)# site-id 201-300
vSmart(config-lists)# site-list apac-control-site-list
vSmart(config-lists)# site-id 301-400
```

tag (IP SLA)

To create a user-specified identifier for a Cisco IOS IP Service Level Agreements (SLAs) operation, use the **tag** (IP SLA) command in the appropriate submode of IP SLA configuration, auto IP SLA MPLS configuration, or IP SLA monitor configuration mode. To remove a tag from an operation, use the **no** form of this command.

Syntax Description

text	Name of a group to which the operation belongs from 0 to 16 ASCII characters.

Command Default

No tag identifier is specified.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see the Cisco IOS XE `tag` command.

```
ip sla responder
ip sla 6001
 udp-jitter 172.31.11.85 44444 source-ip 172.31.17.220 num-packets 100
  request-data-size 64
  tag 6001:UDP64 HNZ-H7Z
  frequency 300
ip sla schedule 6001 life forever start-time now
ip sla 7001
 icmp-echo 172.31.17.222 source-ip 172.31.17.216
  request-data-size 64
  tag 7001:AVAILABILITY DSO-D7S
  frequency 30
ip sla schedule 7001 life forever start-time now
ip sla reaction-configuration 6001 react rtt threshold-value 40 40 threshold-type immediate
 action-type trapAndTrigger
ip sla reaction-configuration 6001 react timeout threshold-type immediate action-type
trapAndTrigger
ip sla reaction-configuration 6001 react packetLossDS threshold-value 1 1 threshold-type
immediate action-type trapAndTrigger
```

```
ip sla reaction-configuration 7001 react timeout threshold-type immediate action-type
trapAndTrigger
```

tag-instances

To configure tag instances with member attributes, use the **tag-instances** command in global configuration mode. To delete the tag instances, use the **no** form of this command.

tag-instances tag-instance *tag-instance-name* [**app-list** *app-list-name*] [**data-prefix-list** *data-prefix-list-name*] [**data-ipv6-prefix-list** *ipv6-prefix-list-name*] [**id** *tag-id*]
no tag-instances tag-instance *tag-instance-name*

Syntax Description

tag-instance	Specifies the tag instance information.
tag-instance-name	Specifies the tag instance name.
app-list-name	Specify the list of app list names of 1 to 32 characters.
data-prefix-list-name	Specify the list of data prefix list names of 1 to 32 characters.
data-ipv6-prefix-list-name	Specify the list of data IPv6 prefix list names of 1 to 32 characters.
tag-id	Global unique ID assigned to each of the tag instances. Range: 1 to 4294967295.

Command Default

No tag identifier is specified.

Command Modes

Global configuration mode (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

You cannot modify the tag ID after the tag name is provided. To modify a tag ID, delete the tag and create a new tag with a new tag ID.

Examples

The following example shows how to configure tag-instances red and blue with unique tag-ids and data-prefix-list names:

```
tag-instances
 tag-instance red
  tag-id 1000
  data-prefix-list pfx1 pfx2
!
 tag-instance blue
  tag-id 2000
  data-ipv6-prefix-list v6_pfx1 v6_pfx2
!
```

Related Commands

Command	Description
lists	To create groupings of similar objects, such as IP prefixes, data-prefixes, and app-lists for use when configuring tag-instances. Note that the lists configured under tag-instances is not same as the lists configured under policy. Tag-instances requires its own lists configured.

track ip sla

To track the state of a Cisco IOS IP Service Level Agreements (SLAs) operation and to enter tracking configuration mode, use the **track ip sla** command in global configuration mode. To remove the tracking, use the **no** form of this command.

track ip *jitter* **sla**

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE track ip sla command.

Note In Cisco Catalyst SD-WAN Manager Release 20.15.1, when pushing a CLI template to a device running a version earlier than Cisco Catalyst SD-WAN Manager Release 20.15.1, the CLI template must add another command, **track tracked-object** *track-id* **ip sla** *ip sla-id* **state**.

```
track 1 ip sla 2 state
track tracked-object 1 ip sla 2 state
```

Examples

The following example shows how to configure the tracking process to track the state of IP SLAs operation 2:

```
Device(config)# track 1 ip sla 2 state
Device(config-track)
```

The following example shows how to configure the tracking process to track the reachability of IP SLAs operation 3:

```
Device(config)# track 2 ip sla 3 reachability
Device(config-track)
```

udp-jitter

To configure a Cisco IOS IP Service Level Agreements (SLAs) User Datagram Protocol (UDP) jitter operation or a IP SLAs multicast UDP jitter operation and enter UDP jitter or multicast UDP jitter configuration mode, use the **udp-jitter**command in IP SLA configuration mode.

Syntax Description

destination-ip-address | *destination-hostname*	Destination IPv4 or IPv6 address or hostname. • For a multicast UDP jitter operation, this must be a multicast IP address.
destination-port	Specifies the destination port number. The range is from 1 to 65535.
source-ip {*ip-address* | *hostname*}	(Optional) Specifies the source IPv4 or IPv6 address or hostname. When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
num-packets *number-of-packets*	(Optional) Specifies the number of packets. The default is 10.

Command Default

No IP SLAs operation type is configured for the operation being configured.

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates..

Usage Guidelines

For more information about this command, see the Cisco IOS XE `udp-jitter` command.

Examples

```
ip sla responder
ip sla 6001
 udp-jitter 172.31.11.85 44444 source-ip 172.31.17.220 num-packets 100
  request-data-size 64
  tag 6001:UDP64 HNZ-H7Z
  frequency 300
ip sla schedule 6001 life forever start-time now
ip sla 7001
 icmp-echo 172.31.17.222 source-ip 172.31.17.216
  request-data-size 64
  tag 7001:AVAILABILITY DSO-D7S
  frequency 30
ip sla schedule 7001 life forever start-time now
ip sla reaction-configuration 6001 react rtt threshold-value 40 40 threshold-type immediate
 action-type trapAndTrigger
ip sla reaction-configuration 6001 react timeout threshold-type immediate action-type
trapAndTrigger
ip sla reaction-configuration 6001 react packetLossDS threshold-value 1 1 threshold-type
immediate action-type trapAndTrigger
ip sla reaction-configuration 7001 react timeout threshold-type immediate action-type
trapAndTrigger
```

utd-policy

To attach an Unified Threat Defense (UTD) action to a policy, use the **utd-policy** command in profile configuration mode.The UTD action contains both the UTD profile and a UTD policy that will be applied, and along with the TLS decryption action.

utd-policy *policy-name*

Syntax Description

policy-name	Enter a name for the UTD policy.

Command Modes

Profile configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Qualified for use in Cisco vManage CLI templates

The following example shows how to attach a profile for a Unified Security Policy.

```
Device(config)# parameter-map type inspect aip
Device(config-profile)# utd-policy united
```

vpn-list

To list the VPNs on Cisco vSmart Controllers for which a policy is applicable such as, data-policy and app-route-policy, use the **vpn-list** command in data policy configuration mode. To remove the list of VPNs, use the **no** form of this command.

vpn-list { *list-name* }

no vpn-list { *list-name* }

Syntax Description

list-name	Specifies the name of the policy-related list that the Cisco vSmart Controller saves on the Cisco IOS XE Catalyst SD-WAN device.

Command Default

None

Command Modes

data policy configuration (config-data-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For more information about this command, see Centralized Policy.

```
vSmart(config)# policy
vSmart(config-policy)# data-policy sig_ha_zscaler_data_policy_cedge
vSmart(config-data-policy-sig_ha_zscaler_data_policy_cedge)# vpn-list vpn_1
vSmart(config-vpn-list-vpn_1)# sequence 100
vSmart(config-sequence-100)# match destination-ip 10.10.10.10/32
vSmart(config-match)# protocol 17
vsmart(config-match)# !
vsmart(config-match)# action accept
vsmart(config-action)# count sig_ha_zscaler_datapolicycnt100
vsmart(config-action)# sig
vsmart(config-action)# exit
vsmart(config-action)# exit
vSmart(config-vpn-list-vpn_1)# sequence 110
vSmart(config-sequence-110)# match app-list googel_app
vSmart(config-match)# destination-data-prefix-list dest_prefix_list
vsmart(config-match)# !
vsmart(config-match)# action accept
vsmart(config-action)# count sig_ha_zscaler_datapolicycnt110
vsmart(config-action)# sig
vsmart(config-action)# exit
vsmart(config-action)# exit
vSmart(config-vpn-list-vpn_1)# sequence 120
vSmart(config-sequence-110)# match app-list amazon
vSmart(config-match)# destination-data-prefix-list dest_prefix_list
vsmart(config-match)# !
vsmart(config-match)# action accept
vsmart(config-action)# count sig_ha_zscaler_datapolicycnt120
vsmart(config-action)# sig
vsmart(config-action)# exit
vsmart(config-action)# exit
vSmart(config-sequence-120)# default-action accept
```

vrf (IP SLA)

To allow monitoring within Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) using Cisco IOS IP Service Level Agreements (SLAs) operations, use the **vrf** command in the appropriate submode of IP SLA configuration, IP SLA monitor configuration, or IP SLA template configuration mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE vrf (IP SLA) command.

Examples

The following examples show how to configure an IP SLAs operation for an MPLS VPN. These examples show how test traffic can be sent in an already existing VPN tunnel between two endpoints.

IP SLA Configuration

```
Device# config-transaction
Device(config)# ip sla 1
Device(config-ip-sla)# icmp-echo 10.1.1.1
```

```
Device(config-ip-sla-echo)# vrf vpn1
Device(config-ip-sla-echo)#
```