# Network Management Configuration Guide, Cisco IOS XE Cupertino 17.8.x (Catalyst 9200 Switches)

**First Published:** 2022-04-09

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2022 Cisco Systems, Inc. All rights reserved.

# CONTENTS


CHAPTER 1 **Configuring Autoconf** 1

Prerequisites for Autoconf 1

Restrictions for Autoconf 1

Information about Autoconf 2

Benefits of Autoconf 2

Identity Session Management and Templates 2

Autoconf Operation 3

Advantages of Using Templates 5

Autoconf Functionality 6

How to Configure Autoconf 7

Applying a Built-In Template to an End Device 7

Applying a Modified Built-In Template to an End Device 11

Migrating from ASP to Autoconf 12

Configuring a Platform Type Filter 13

Configuring a Platform Type Filter for a Class Map 14

Configuring a Platform Type Filter for a Parameter Map 14

Configuring a Device Type Filter for a Class Map 15

Configuration Examples for Autoconf 16

Example: Applying a Built-In Template to an End Device 17

Example: Applying a Modified Built-In Template to an End Device 17

Example: Migrating from ASP Macros to Autoconf 17

Example: Configuring a Platform Type Filter 17

Additional References for Autoconf 18

Feature History for Autoconf 18

CHAPTER 2 **Configuring Interface Templates** 21

Restrictions for Interface Templates 21
Information About Interface Templates 21
Interface Template Overview 21
Binding an Interface Template to a Target 23
Priority for Configurations Using Interface Templates 24
How to Configure Interface Templates 24
Configuring Interface Templates 24
Configuring Static Binding for Interface Templates 25
Configuring Dynamic Binding of Interface Templates 26
Verifying Interface Templates 28
Configuration Examples for Interface Templates 32
Example: Configuring User Interface Templates 32
Example: Sourcing Interface Templates 32
Example: Dynamically Binding Interface Templates 33
Feature History for Interface Templates 33

CHAPTER 3 **Configuring Cisco Plug and Play** 35
Configuring Cisco Plug and Play 35
Feature History for Cisco Plug and Play 35

CHAPTER 4 **Configuring Cisco Discovery Protocol** 37
Information about Cisco Discovery Protocol 37
Default Cisco Discovery Protocol Configuration 37
Cisco Discovery Protocol Overview 37
How to Configure Cisco Discovery Protocol 38
Configuring Cisco Discovery Protocol Characteristics 38
Disabling Cisco Discovery Protocol 40
Enabling Cisco Discovery Protocol 41
Disabling Cisco Discovery Protocol on an Interface 42
Enabling Cisco Discovery Protocol on an Interface 43
Monitoring and Maintaining Cisco Discovery Protocol 45
Feature History for Cisco Discovery Protocol 45

CHAPTER 5 **Configuring Cisco Discovery Protocol Bypass** 47

Restrictions for Cisco Discovery Protocol Bypass 47
Information about Cisco Discovery Protocol Bypass 47
How to configure Cisco Discovery Protocol Bypass 48
Configuration Examples for Cisco Discovery Protocol Bypass 49
Example: Enabling Cisco Discovery Protocol Bypass 49
Displaying Cisco Discovery Protocol neighbours 49
Example:Disabling Cisco Discovery Protocol Bypass 50
Feature History for Cisco Discovery Protocol Bypass 50

CHAPTER 6 **Configuring Simple Network Management Protocol 51**
Prerequisites for SNMP 51
Restrictions for SNMP 53
Information About SNMP 54
SNMP Overview 54
SNMP Manager Functions 54
SNMP Agent Functions 55
SNMP Community Strings 55
SNMP MIB Variables Access 55
SNMP Flash MIB 56
SNMP Notifications 56
SNMP ifIndex MIB Object Values 57
SNMP ENTITY-MIB Identifiers 57
SNMP and Syslog Over IPv6 57
Default SNMP Configuration 58
SNMP Configuration Guidelines 58
How to Configure SNMP 59
SNMP Community Strings 59
Configuring SNMP Groups and Users 59
Opening or Closing SNMP UDP Ports 63
SNMP Notifications 64
Setting the Agent Contact and Location Information 64
Limiting TFTP Servers Used Through SNMP 65
Disabling the SNMP Agent 66
SNMP Examples 68

Monitoring SNMP Status 69
Feature History for Simple Network Management Protocol 69

CHAPTER 7 **Configuring Service Level Agreements** 71
Restrictions on SLAs 71
Information About Service Level Agreements 71
Cisco IOS IP Service Level Agreements (SLAs) 71
Network Performance Measurement with Cisco IOS IP SLAs 73
IP SLA Responder and IP SLA Control Protocol 73
Response Time Computation for IP SLAs 74
IP SLAs Operation Scheduling 75
IP SLA Operation Threshold Monitoring 75
UDP Jitter 76
How to Configure IP SLAs Operations 76
Default Configuration 76
Configuration Guidelines 77
Configuring the IP SLA Responder 77
Implementing IP SLA Network Performance Measurement 79
Analyzing IP Service Levels by Using the UDP Jitter Operation 82
Analyzing IP Service Levels by Using the ICMP Echo Operation 86
Monitoring IP SLA Operations 89
Monitoring IP SLA Operation Examples 90
Additional References 91
Feature History for Service Level Agreements 92

CHAPTER 8 **Configuring SPAN and RSPAN** 93
Prerequisites for SPAN and RSPAN 93
Restrictions for SPAN and RSPAN 93
Information About SPAN and RSPAN 95
SPAN and RSPAN 95
Local SPAN 95
Remote SPAN 96
SPAN and RSPAN Concepts and Terminology 97
SPAN and RSPAN Interaction with Other Features 102

SPAN and RSPAN and Device Stacks 103
Flow-Based SPAN 103
Default SPAN and RSPAN Configuration 104
Configuring SPAN and RSPAN 104
SPAN Configuration Guidelines 104
RSPAN Configuration Guidelines 104
FSPAN and FRSPAN Configuration Guidelines 105
How to Configure SPAN and RSPAN 105
Creating a Local SPAN Session 105
Creating a Local SPAN Session and Configuring Incoming Traffic 108
Specifying VLANs to Filter 110
Configuring a VLAN as an RSPAN VLAN 112
Creating an RSPAN Source Session 113
Specifying VLANs to Filter 115
Creating an RSPAN Destination Session 117
Creating an RSPAN Destination Session and Configuring Incoming Traffic 119
Configuring an FSPAN Session 121
Configuring an FRSPAN Session 124
Monitoring SPAN and RSPAN Operations 127
Configuration Examples for SPAN and RSPAN 127
Example: Configuring Local SPAN 127
Examples: Creating an RSPAN VLAN 128
Feature History for SPAN and RSPAN 129

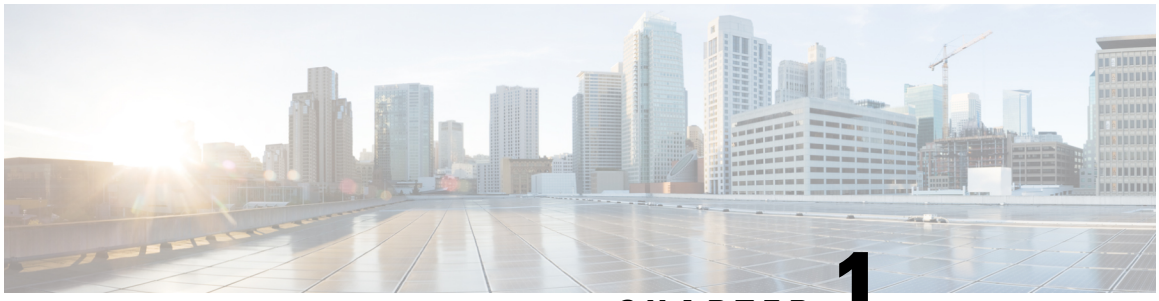
CHAPTER 9 **Configuring Packet Capture** 131
Prerequisites for Configuring Packet Capture 131
Prerequisites for Configuring Embedded Packet Capture 131
Restrictions for Configuring Embedded Packet Capture 131
Information About Packet Capture 132
About Embedded Packet Capture 133
Benefits of Embedded Packet Capture 133
Packet Data Capture 133
How to Implement Embedded Packet Capture 133
Managing Packet Data Capture 134

Monitoring and Maintaining Captured Data 135
Configuration Examples for Embedded Packet Capture 136
Example: Managing Packet Data Capture 136
Example: Monitoring and Maintaining Captured Data 136
Feature History for Packet Capture 138

CHAPTER 10 **Configuring Flexible NetFlow** 141
Prerequisites for Flexible NetFlow 141
Restrictions for Flexible NetFlow 142
Information About Flexible Netflow 144
Flexible Netflow Overview 144
Original NetFlow and Benefits of Flexible NetFlow 144
Flexible NetFlow Components 145
Flow Records 145
Flow Exporters 150
Flow Monitors 151
Flow Samplers 153
Supported Flexible NetFlow Fields 153
Default Settings 157
Flexible NetFlow—Ingress VRF Support Overview 158
Flexible Netflow—Egress VRF Support Overview 158
How to Configure Flexible Netflow 158
Creating a Flow Record 158
Creating a Flow Exporter 159
Creating a Customized Flow Monitor 162
Creating a Flow Sampler 164
Applying a Flow to an Interface 166
Configuring a Bridged NetFlow on a VLAN 167
Configuring Layer 2 NetFlow 168
Monitoring Flexible NetFlow 169
Configuration Examples for Flexible NetFlow 169
Example: Configuring a Flow 169
Example: Monitoring IPv4 ingress traffic 170
Example: Monitoring IPv4 egress traffic 171

Example: Configuring Flexible NetFlow for Ingress VRF Support 172
Example: Configuring Flexible NetFlow for Egress VRF Support 172
Feature History for Flexible NetFlow 173

CHAPTER 11 **Configuring Network Detection and Response** 175
Prerequisites for Network Detection and Response 175
Restrictions for Network Detection and Response 175
Information About Network Detection and Response 175
How to Configure Network Detection and Response 176
Configuring a Certificate for Registration 176
Configuring a Certificate for File Upload 177
Configuring Stealthwatch Cloud on a Device 179
How to Integrate Flexible NetFlow with the Stealthwatch Cloud Portal 180
Creating a Flow Record 180
Creating a Flow Exporter 182
Configuring a Flow Monitor 183
Applying a Flow to an Interface 183
Verifying Network Detection and Response Configuration 184
Configuration Examples for Network Detection and Response 185
Example: Configuring and Integrating Stealthwatch Cloud on a Device 185
Example: Verifying Stealthwatch Cloud Configuration 185
Feature History for Network Detection and Response 188



CHAPTER 1

# Configuring Autoconf

The following sections provide information about Autoconf and how to configure Autoconf:


- Prerequisites for Autoconf, on page 1
- Restrictions for Autoconf, on page 1
- Information about Autoconf , on page 2
- How to Configure Autoconf, on page 7
- Configuration Examples for Autoconf, on page 16
- Additional References for Autoconf, on page 18
- Feature History for Autoconf, on page 18


## Prerequisites for Autoconf

- Before enabling Autoconf, disable the Auto SmartPort (ASP) macro, device classifier, and then access the session monitor.

## Restrictions for Autoconf

- ASP macro and Autoconf are not supported on the same interface at the same time. Either Autoconf or ASP must be disabled on a per-interface level.
- Interface templates are not applicable for wireless sessions.
- When the Autoconf feature is enabled using the **autoconf enable** command, the default Autoconf service policy is applied to all the interfaces. No other service policy can be applied globally using the **service-policy** command. To apply a different service policy, you must disable Autoconf on that interface. When a service policy is applied globally, you must disable it before enabling the Autoconf feature.
- When both local (interface level) and global service policies exist, the local policy takes precedence. The global service policy comes into effect only when the local policy is removed.
- Service templates cannot be applied to interfaces, and interface templates cannot be applied to service instances.
- Only one service template can be nested inside an interface template.
- Autoconf does not support the switchover feature.

# Information about Autoconf

The following sections provide information about Autoconf.

## Benefits of Autoconf

The Autoconf feature permits hardbinding between an end device and an interface. Autoconf falls under the umbrella of the Cisco Smart Operations solution. Smart Operations is a comprehensive set of capabilities that can simplify and improve LAN switch deployment, and help organizations deliver operational excellence and scale services on the network.

The Autoconf feature automatically applies the necessary configurations on the device ports to enable the efficient performance of each directly connected end device using a set of interface configurations that are configured inside an interface template:

- Autoconf efficiently applies commands to an interface because the parser does not need to parse each command each time.
- Configurations that are applied through the Autoconf feature can be reliably removed from a port without impacting previous or subsequent configurations on the port.
- The Autoconf feature provides built-in and user-defined configurations using interface and service templates. Configurations applied through templates can be centrally updated with a single operation.
- Using the Autoconf feature, a configuration can be applied to ports and access sessions.
- The Autoconf feature reduces ongoing maintenance for devices and attached end devices by making them intuitive and autoconfigurable. This reduces operation expenses (OPEX) and lowers the total cost of ownership (TCO).

## Identity Session Management and Templates

A key advantage of the Autoconf feature is that the core session management capability is decoupled from the application-specific logic, allowing the same framework to be used regardless of the criteria for policy determination or the nature of the policies applied.

The identity session management infrastructure allows configurations or policies or both to be applied as templates.

Both service and interface templates are named as containers of configuration and policy. Service templates can be applied only to access sessions, while interface templates can be applied only to ports. When a service template is applied to an access session, the contained configuration and policy are applied only to the target session, and has no impact on other sessions that may be hosted on the same access port. Similarly, when an interface template is applied to an access port, it impacts all the traffic exchanged on the port.

The Autoconf feature uses a set of built-in maps and built-in templates. The built-in templates are designed based on best practices for interface configurations. Built-in templates can be modified by users to include customized configurations, limiting the need to create a new template.

The templates created by users are referred to as user-defined templates. These templates can be defined on a device and can be mapped to any built-in or user-defined trigger.

Use the **show derived-config** command, to view the overall applied configurations applied by Autoconf template and manual configuration. The interface commands shown in the output of the **show running-config interface** *type number* command are not necessarily the operational configuration. The Autoconf feature dynamically applies a template to the interface, and overrides any conflicting static configuration that is already applied.

# Autoconf Operation

Autoconf uses the Device Classifier to identify the end devices that are connected to a port.

The Autoconf feature uses the device classification information gleaned from Cisco Discovery Protocol, LLDP, DHCP, MAC addresses, and the Organizationally Unique Identifier (OUI) that is identified by the Device Classifier.

The Device Classifier provides improved device classification capabilities and accuracy, and increased device visibility for enhanced configuration management.

Device classification is enabled when you enable the Autoconf feature using the **autoconf enable** command in global configuration mode.

The device detection acts as an event trigger, which in turn applies the appropriate automatic template to the interface.

The Autoconf feature is based on a three-tier hierarchy.

- A policy map identifies the trigger type for applying the Autoconf feature.
- A parameter map identifies the appropriate template that must be applied, based on the end device.
- The templates contain the configurations to be applied.

The Autoconf built-in templates and triggers perform the above tasks automatically.

The Autoconf feature provides the following built-in templates:

- AP_INTERFACE_TEMPLATE
- DMP_INTERFACE_TEMPLATE
- IP_CAMERA_INTERFACE_TEMPLATE
- IP_PHONE_INTERFACE_TEMPLATE
- LAP_INTERFACE_TEMPLATE
- MSP_CAMERA_INTERFACE_TEMPLATE
- MSP_VC_INTERFACE_TEMPLATE
- PRINTER_INTERFACE_TEMPLATE
- ROUTER_INTERFACE_TEMPLATE
- SWITCH_INTERFACE_TEMPLATE
- TP_INTERFACE_TEMPLATE

**Note** By default, built-in templates are not displayed under running configuration. The built-in templates are displayed in the running configuration only if you edit them.

The template that is selected is based on parameter map information applied to an interface. This information can be based on the following criteria:

- End Device type
- MAC address
- OUI
- Platform type
- User role
- Username

The Autoconf feature provides one built-in parameter map (BUILTIN_DEVICE_TO_TEMPLATE) with the following configuration:

```
Parameter-map name: BUILTIN_DEVICE_TO_TEMPLATE
 Map: 10 map device-type regex "Cisco-IP-Phone"
  Action(s):
   20 interface-template IP_PHONE_INTERFACE_TEMPLATE
 Map: 20 map device-type regex "Cisco-IP-Camera"
  Action(s):
   20 interface-template IP_CAMERA_INTERFACE_TEMPLATE
 Map: 30 map device-type regex "Cisco-DMP"
  Action(s):
   20 interface-template DMP_INTERFACE_TEMPLATE
 Map: 40 map oui eq "00.0f.44"
  Action(s):
   20 interface-template DMP_INTERFACE_TEMPLATE
 Map: 50 map oui eq "00.23.ac"
  Action(s):
   20 interface-template DMP_INTERFACE_TEMPLATE
 Map: 60 map device-type regex "Cisco-AIR-AP"
  Action(s):
   20 interface-template AP_INTERFACE_TEMPLATE
 Map: 70 map device-type regex "Cisco-AIR-LAP"
  Action(s):
   20 interface-template LAP_INTERFACE_TEMPLATE
 Map: 80 map device-type regex "Cisco-TelePresence"
  Action(s):
   20 interface-template TP_INTERFACE_TEMPLATE
 Map: 90 map device-type regex "Surveillance-Camera"
  Action(s):
   10 interface-template MSP_CAMERA_INTERFACE_TEMPLATE
 Map: 100 map device-type regex "Video-Conference"
  Action(s):
   10 interface-template MSP_VC_INTERFACE_TEMPLATE
```

**Note** Use the **show parameter-map type subscriber attribute-to-service All** command to view the configuration for the built-in parameter map.

The Autoconf feature provides one built-in policy map (BUILTIN_AUTOCONF_POLICY) with the following configuration:

```
BUILTIN_AUTOCONF_POLICY
  event identity-update match-all
    10 class always do-until-failure
      10 map attribute-to-service table BUILTIN_DEVICE_TO_TEMPLATE
```

**Note** Use the **show policy-map type control subscriber BUILTIN_AUTOCONF_POLICY** command to view the configuration for the built-in policy map.

You can also manually create policy maps, parameter maps, and templates.

When a trigger is created that is based on specific user information, a local 802.1X Cisco Identity Services Engine (ISE) server authenticates it, ensuring the security of the operation.

An interface template can be dynamically activated (on an interface) using any of the following methods:

- RADIUS CoA: While Change of Authorization (CoA) commands are targeted at one or more access sessions, any referenced template must be applied to the interface that is hosting the referenced session.
- RADIUS Access-Accept for client authentication or authorization: Any referenced interface template returned in an Access-Accept must be applied to the port that is hosting the authorized access session.
- Service template: If an interface template is referenced in a service template that is either locally defined or sourced from the AAA server, the interface template must be applied to the interface hosting an access-session on which the service template is applied. (Add a new command for interface template reference from within a locally defined service template.)
- Subscriber control-policy action: A mapping action under the subscriber control policy activates service or interface template (as referenced in a parameter map) or both based on the type of filter, and removes templates, if any, associated with a previous policy.
- Device-to-template parameter map: A subscriber parameter map that allows the filter type-to-service or interface template mappings or both to be specified in an efficient and readable manner.

# Advantages of Using Templates

Using templates for auto configuration has the following benefits:

- Templates are parsed once when they are being defined. This makes the dynamic application of the templates very efficient.
- Templates can be applied to an Ethernet interface that is connected to an end device, based on the type of end device.
- Service templates allow the activation of session-oriented features, whereas interface templates apply configurations to the interface that is hosting a session.
- Service templates are applied to access sessions and hence only impact the traffic exchanged with a single endpoint on a port.
- Startup and running configurations of a device are not modified by the dynamic application of a template.
- Policy application is synchronized with the access-session life cycle. This is tracked by the framework by using all the available techniques, including link-up or link-down.

- Templates can be updated with a single operation. All the applied instances of templates are also updated during this operation.
- Constituent commands of templates do not appear in the running configuration.
- Templates can be removed with no impact on previous or subsequent configurations.
- Template application is acknowledged, allowing for synchronization and performance of remedial actions when failures occur.
- Data VLAN, quality of service (QoS) parameters, storm control, and MAC-based port security are configured automatically based on the end device that is connected to the switch.
- The switch port is cleaned up completely by removing configurations when the device is disconnected from a port.
- Human error is reduced in the installation and configuration process.

# Autoconf Functionality

The Autoconf feature is disabled by default in global configuration mode. When you enable the Autoconf feature in global configuration mode, it is enabled by default at the interface level. The built-in template configurations are applied based on the end devices detected on all the interfaces.

Use the **access-session inherit disable autoconf** command to manually disable Autoconf at the interface level, even when Autoconf is enabled at the global level.

If you disable Autoconf at the global level, all the interface-level configurations are disabled.

***Table 1: Autoconf Functionality***

| Global | Interface Level | AutoConf Status |
|---|---|---|
| Disable | Disable | No automatic configurations are applied when an end device is connected. |
| Enable | Enable | If Autoconf is enabled at the global level, it is also enabled at the interface level by default. Built-in template configurations are applied based on the end devices that are detected on all the interfaces. |
| Enable | Disable | Enabled at global level. Disabled at interface level. No automatic configurations are applied when an end device is connected to the interface on which Autoconf is disabled. |

Autoconf allows you to retain the template even when the link to the end device is down or the end device is disconnected, by configuring the autoconf sticky feature **access-session interface-template sticky** command in global configuration mode. The Autoconf sticky feature avoids the need for detecting the end device and applying the template every time the link flaps or the device is removed and connected back.

The **access-session interface-template sticky** command is mandatory to apply an inbuilt template that contains **access-session** commands on an interface. Configure the **access-session interface-template sticky** command to apply interface template on a port using a service policy.

To disable the Autoconf feature on a specific interface, use the **access-session inherit disable interface-template-sticky** command in interface configuration mode.

# How to Configure Autoconf

The following sections provide information about how to configure Autoconf.

## Applying a Built-In Template to an End Device

The following task shows how to apply a built-in template on an interface that is connected to an end device, for example, a Cisco IP phone.

### Before you begin

Make sure that the end device, for example, a Cisco IP phone, is connected to a switch port.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device(config)# configure terminal` | Enters global configuration mode. |
| **Step 3** | **autoconf enable**<br>**Example:**<br>`Device(config)# autoconf enable` | Enables the Autoconf feature. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and enters privileged EXEC mode. |
| **Step 5** | **show device classifier attached interface** *interface-type interface-number*<br>**Example:**<br>`Device# show device classifier attached interface Gi3/0/26` | (Optional) Displays whether the end device is classified by the device classifier with correct attributes. |
| **Step 6** | **show template binding target** *interface-type interface-number*<br>**Example:**<br>`Device# show template binding target gi3/0/26` | Displays the configuration applied through the template on the interface. |

### Example

The following example shows that an IP phone is classified by the device classifier with correct attributes:

```
Device# show device classifier attached interface GigabitEthernet 3/0/26

Summary:

MAC_Address       Port_Id       Profile Name                        Device Name
==============    ==========    ==================                  ==================
0026.0bd9.7bbb    Gi3/0/26      Cisco-IP-Phone-7962                 Cisco IP Phone 7962
```

The following example shows that a built-in interface template is applied on an interface:

```
Device# show template binding target GigabitEthernet 3/0/26

Interface Templates
===================
Interface: Gi4/0/11
Method              Source            Template-Name
------              ------            -------------
dynamic             Built-in          IP_PHONE_INTERFACE_TEMPLATE
```

The following example shows how to verify the interface configuration after the interface template is applied to an IP phone connected to the GigabitEthernet interface 3/0/26:

```
Device# show running-config interface GigabitEthernet 3/0/26
Building configuration...

Current configuration : 624 bytes
!
interface GigabitEthernet3/0/26
!
End

Device# show derived-config interface GigabitEthernet 3/0/26

Building configuration...

Derived configuration : 649 bytes
!
interface GigabitEthernet3/0/26
 switchport mode access
 switchport block unicast
 switchport port-security maximum 3
 switchport port-security maximum 2 vlan access
 switchport port-security violation restrict
 switchport port-security aging time 2
 switchport port-security aging type inactivity
 switchport port-security
 load-interval 30
 storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AutoConf-4.0-CiscoPhone-Input-Policy
 service-policy output AutoConf-4.0-Output-Policy
 ip dhcp snooping limit rate 15
```

```
end
```

The following example shows how to verify the global configuration after configuring Autoconf:

```
Device# show running config
class-map match-any AutoConf-4.0-Scavenger-Queue
 match dscp cs1
 match cos  1
 match access-group name AutoConf-4.0-ACL-Scavenger
class-map match-any AutoConf-4.0-VoIP
 match dscp ef
 match cos  5
class-map match-any AutoConf-4.0-Control-Mgmt-Queue
 match cos  3
 match dscp cs7
 match dscp cs6
 match dscp cs3
 match dscp cs2
 match access-group name AutoConf-4.0-ACL-Signaling
class-map match-any AutoConf-4.0-Multimedia-Conf
 match dscp af41
 match dscp af42
 match dscp af43
class-map match-all AutoConf-4.0-Broadcast-Vid
 match dscp cs5
class-map match-any AutoConf-4.0-Bulk-Data
 match dscp af11
 match dscp af12
 match dscp af13
class-map match-all AutoConf-4.0-Realtime-Interact
 match dscp cs4
class-map match-any AutoConf-4.0-VoIP-Signal
 match dscp cs3
 match cos  3
class-map match-any AutoConf-4.0-Trans-Data-Queue
 match cos  2
 match dscp af21
 match dscp af22
 match dscp af23
 match access-group name AutoConf-4.0-ACL-Transactional-Data
class-map match-any AutoConf-4.0-VoIP-Data
 match dscp ef
 match cos  5
class-map match-any AutoConf-4.0-Multimedia-Stream
 match dscp af31
 match dscp af32
 match dscp af33
class-map match-all AutoConf-4.0-Internetwork-Ctrl
 match dscp cs6
class-map match-all AutoConf-4.0-VoIP-Signal-Cos
 match cos  3
class-map match-any AutoConf-4.0-Multimedia-Stream-Queue
 match dscp af31
 match dscp af32
 match dscp af33
class-map match-all AutoConf-4.0-Network-Mgmt
 match dscp cs2
class-map match-all AutoConf-4.0-VoIP-Data-Cos
 match cos  5
class-map match-any AutoConf-4.0-Priority-Queue
 match cos  5
 match dscp ef
 match dscp cs5
 match dscp cs4
```

```
class-map match-any AutoConf-4.0-Bulk-Data-Queue
 match cos  1
 match dscp af11
 match dscp af12
 match dscp af13
 match access-group name AutoConf-4.0-ACL-Bulk-Data
class-map match-any AutoConf-4.0-Transaction-Data
 match dscp af21
 match dscp af22
 match dscp af23
class-map match-any AutoConf-4.0-Multimedia-Conf-Queue
 match cos  4
 match dscp af41
 match dscp af42
 match dscp af43
 match access-group name AutoConf-4.0-ACL-Multimedia-Conf
class-map match-all AutoConf-4.0-Network-Ctrl
 match dscp cs7
class-map match-all AutoConf-4.0-Scavenger
 match dscp cs1
class-map match-any AutoConf-4.0-Signaling
 match dscp cs3
 match cos  3
!
!
policy-map AutoConf-4.0-Cisco-Phone-Input-Policy
 class AutoConf-4.0-VoIP-Data-Cos
  set dscp ef
  police cir 128000 bc 8000
   exceed-action set-dscp-transmit cs1
   exceed-action set-cos-transmit 1
 class AutoConf-4.0-VoIP-Signal-Cos
  set dscp cs3
  police cir 32000 bc 8000
   exceed-action set-dscp-transmit cs1
   exceed-action set-cos-transmit 1
 class class-default
  set dscp default
  set cos 0
policy-map AutoConf-4.0-Output-Policy
 class AutoConf-4.0-Scavenger-Queue
  bandwidth remaining percent 1
 class AutoConf-4.0-Priority-Queue
  priority
  police cir percent 30 bc 33 ms
 class AutoConf-4.0-Control-Mgmt-Queue
  bandwidth remaining percent 10
 class AutoConf-4.0-Multimedia-Conf-Queue
  bandwidth remaining percent 10
 class AutoConf-4.0-Multimedia-Stream-Queue
  bandwidth remaining percent 10
 class AutoConf-4.0-Trans-Data-Queue
  bandwidth remaining percent 10
    dbl
 class AutoConf-4.0-Bulk-Data-Queue
  bandwidth remaining percent 4
    dbl
 class class-default
  bandwidth remaining percent 25
    dbl
policy-map AutoConf-DMP
 class class-default
  set dscp cs2
policy-map AutoConf-IPVSC
```

```
 class class-default
  set cos dscp table AutoConf-DscpToCos
policy-map AutoConf-4.0-Input-Policy
 class AutoConf-4.0-VoIP
 class AutoConf-4.0-Broadcast-Vid
 class AutoConf-4.0-Realtime-Interact
 class AutoConf-4.0-Network-Ctrl
 class AutoConf-4.0-Internetwork-Ctrl
 class AutoConf-4.0-Signaling
 class AutoConf-4.0-Network-Mgmt
 class AutoConf-4.0-Multimedia-Conf
 class AutoConf-4.0-Multimedia-Stream
 class AutoConf-4.0-Transaction-Data
 class AutoConf-4.0-Bulk-Data
 class AutoConf-4.0-Scavenger
```

# Applying a Modified Built-In Template to an End Device

The following task shows how to modify a built-in template when multiple wireless access points and IP cameras are connected to a switch.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device(config)# configure terminal` | Enters global configuration mode. |
| **Step 3** | **template** *template-name*<br>**Example:**<br>`Device(config)# template AP_INTERFACE_TEMPLATE` | Enters template configuration mode for the built-in template. |
| **Step 4** | **switchport access vlan** *vlan-id*<br>**Example:**<br>`Device(config-template)# switchport access vlan 20` | Sets the VLAN when the interface is in access mode. |
| **Step 5** | **description** *description*<br>**Example:**<br>`Device(config-template)# description modifiedAP` | Modifies the description of the built-in template. |
| **Step 6** | **exit**<br>**Example:** | Exits template configuration mode and enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-template)# exit` | |
| **Step 7** | **autoconf enable**<br>**Example:**<br>`Device(config)# autoconf enable` | Enables the Autoconf feature. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and enters privileged EXEC mode. |
| **Step 9** | **show template interface binding all**<br>**Example:**<br>`Device# show template interface binding all` | Displays whether the template is applied on the interface. |

### Example

The following example shows that an IP camera and access points are classified by the device classifier with correct attributes:

```
Device# show device classifier attached detail

DC default profile file version supported = 1

Detail:
MAC_Address     Port_Id    Cert Parent Proto    ProfileType     Profile Name
Device_Name
=============================================================================================================
001d.a1ef.23a8  Gi1/0/7     30    3    C     M    Default      Cisco-AIR-AP-1130      cisco
 AIR-AP1131AG-A-K9
001e.7a26.eb05  Gi1/0/30    70    2    C     M    Default      Cisco-IP-Camera        Cisco
 IP Camera
```

The following example shows that the built-in interface template is applied on an interface:

```
Device# show template interface binding all

Template-Name                   Source            Method          Interface
-------------                   ------            ------          ---------
IP_CAMERA_INTERFACE_TEMPLATE     Built-in          dynamic         Gi1/0/30
AP_INTERFACE_TEMPLATE          Modified-Built-in   dynamic         Gi1/0/7
```

# Migrating from ASP to Autoconf

### Before you begin

Verify that the AutoSmart Port (ASP) macro is running by using the **show running-config | include macro auto global** command.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **no macro auto global processing**<br>**Example:**<br>`Device(config)# no macro auto global processing` | Disables ASP on a global level. |
| **Step 4** | **exit**<br>**Example:**<br>`Device(config)# exit` | Exits global configuration mode and returns to privileged EXEC mode. |
| **Step 5** | **clear macro auto configuration all**<br>**Example:**<br>`Device# clear macro auto configuration all` | Clears macro configurations for all interfaces. |
| **Step 6** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 7** | **autoconf enable**<br>**Example:**<br>`Device(config)# autoconf enable` | Enables the Autoconf feature. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuring a Platform Type Filter

The following tasks shows how to configure a platform type filter for class maps and parameter maps.

# Configuring a Platform Type Filter for a Class Map

A control class defines the conditions under which the actions of a control policy are executed. You should define whether all, any, or none of the conditions must be evaluated to execute the actions of the control policy. Platform types are evaluated based on the specified platform name in the control policy.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **class-map type control subscriber** {**match-all** \| **match-any** \| **match-none**} *control-class-name*<br>**Example:**<br>`Device(config)# class-map type control subscriber match-all DOT1X_NO_AGENT` | Creates a control class and enters control class-map filter mode.<br>• **match-all**: Must match all the conditions in the control class.<br>• **match-any**: Must match at least one condition in the control class.<br>• **match-none**: Must not match any of the conditions in the control class. |
| **Step 4** | **match platform-type** *platform-name*<br>**Example:**<br>`Device(config-filter-control-classmap)# match platform-type C3850` | Creates a condition to evaluate control classes based on the specified platform type. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-filter-control-classmap)# end` | Exits control class-map filter mode and returns to privileged EXEC mode. |
| **Step 6** | **show class-map type control subscriber** {**all** \| **name** *control-class-name*}<br>**Example:**<br>`Device# show class-map type control subscriber all` | (Optional) Displays information about control policies for all the class maps or a specific class map. |

# Configuring a Platform Type Filter for a Parameter Map

We recommend that you use the parameter map.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **parameter-map type subscriber attribute-to-service** *parameter-map-name*<br>**Example:**<br>`Device(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para` | Specifies the parameter map type and name, and enters parameter-map filter mode. |
| **Step 4** | *map-index* **map platform-type** {{**eq** \| **not-eq** \| **regex**} *filter-name*}<br>**Example:**<br>`Device(config-parameter-map-filter)# 10 map platform-type eq C9xxx` | Specifies the parameter map attribute filter criteria to the platform type. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-parameter-map-filter-submode)# end` | Exits parameter-map filter mode and returns to privileged EXEC mode. |
| **Step 6** | **show parameter-map type subscriber attribute-to-service**{**all \| name** *parameter-map-name*}<br>**Example:**<br>`Device# show parameter-map type subscriber attribute-to-service` | (Optional) Displays the parameter map attributes. |

# Configuring a Device Type Filter for a Class Map

A control class defines the conditions under which the actions of a control policy are executed. You should define whether all, any, or none of the conditions must be evaluated to execute the actions of the control policy. Device types are evaluated based on the specified device name in the control policy.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **class-map type control subscriber** {**match-all** \| **match-any** \| **match-none**} *control-class-name*<br>**Example:**<br>`Device(config)# class-map type control subscriber match-all Device-Type-Match` | Creates a control class and enters control class-map filter mode.<br>• **match-all**: Must match all the conditions in the control class.<br>• **match-any**: Must match at least one condition in the control class.<br>• **match-none**: Must not match any of the conditions in the control class. |
| **Step 4** | **match device-type** {*device-name*\|**regex** *regular-expression*}<br>**Example:**<br>`Device(config-filter-control-classmap)# match device-type laptop`<br>`Device(config-filter-control-classmap)# match device-type regex cis*` | Creates a condition to evaluate control classes based on the specified device type.<br>• *device-name*: Enter a device name for the class map attribute filter criteria.<br>• **regex** *regular-expression*: Enter a regular expression to specify the filter type. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-filter-control-classmap)# end` | Exits control class-map filter mode and returns to privileged EXEC mode. |
| **Step 6** | **show class-map type control subscriber** {**all** \| **name** *control-class-name*}<br>**Example:**<br>`Device# show class-map type control subscriber all` | (Optional) Displays information about control policies for all the class maps or a specific class map. |

# Configuration Examples for Autoconf

The following sections provide configuration examples for the Autoconf feature.

# Example: Applying a Built-In Template to an End Device

The following example shows how to apply a built-in template to an end device connected to an interface:

```
Device> enable
Device(config)# configure terminal
Device(config)# autoconf enable
Device(config)# end
Device# show device classifier attached interface Gi3/0/26
Device# show template binding target GigabitEthernet 3/0/26
```

# Example: Applying a Modified Built-In Template to an End Device

The following example shows how to apply a modified built-in template to an end device and verify the configuration:

```
Device> enable
Device(config)# configure terminal
Device(config)# template AP_INTERFACE_TEMPLATE
Device(config-template)# switchport access vlan 20
Device(config-template)# description modifiedAP
Device(config-template)# exit
Device(config)# autoconf enable
Device(config)# end
Device# show template interface binding all
```

# Example: Migrating from ASP Macros to Autoconf

The following example shows how to migrate from ASP to Autoconf:

```
Device> enable
Device# configure terminal
Device(config)# no macro auto global processing
Device(config)# exit
Device# clear macro auto configuration all
Device# configure terminal
Device(config)# autoconf enable
Device(config)# end
```

# Example: Configuring a Platform Type Filter

The following example shows how to configure a platform type filter for a class map:

```
Device> enable
Device# configure terminal
Device(config)# class-map type control subscriber match-all DOT1X_NO_AGENT
Device(config-filter-control-classmap)# match platform-type C9xxx
Device(config-filter-control-classmap)# end
Device#
```

The following example shows how to configure a platform type filter for a parameter map:

```
Device> enable
Device# configure terminal
```

```
Device(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para
Device(config-parameter-map-filter)# 10 map platform-type eq C9xxx
Device(config-parameter-map-filter-submode)# end
Device#
```

# Additional References for Autoconf

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco identity-based networking services commands | Cisco IOS Identity-Based Networking Services Command Reference |
| Interface Templates | "Interface Templates" chapter in Identity-Based Networking Services Configuration Guide. |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| IEEE 802.1X | *Port Based Network Access Control* |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

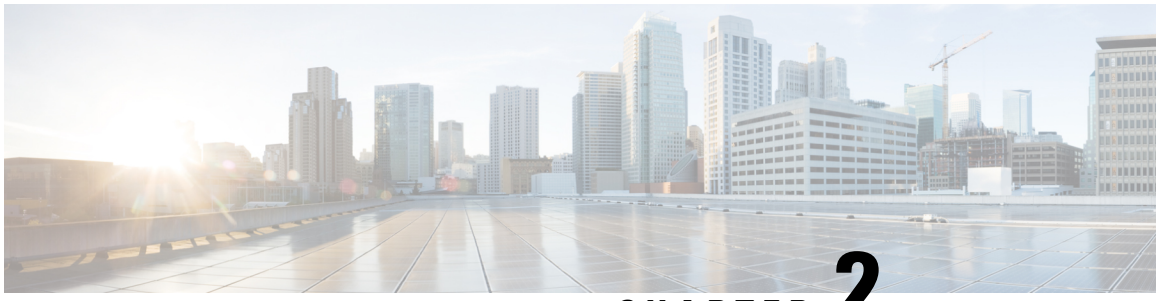
# Feature History for Autoconf

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless notedotherwise.

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Fuji 16.9.2 | Autoconf | The Autoconf feature permits hardbinding between an end device and an interface. In Autoconf the core session management capability is decoupled from the application-specific logic, allowing the same framework to be used regardless of the criteria for policy determination or the nature of the policies applied. |
| Cisco IOS XE Gibraltar 16.12.1 | AutoConf Device Granularity to PID of Cisco Switch | The **platform type** filter option was introduced for class map and parameter map configurations. |

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.



CHAPTER 2

# Configuring Interface Templates

The following sections provide information about Interface Templates and how to configure and bind Interface Templates to a target:


- Restrictions for Interface Templates, on page 21
- Information About Interface Templates, on page 21
- How to Configure Interface Templates, on page 24
- Configuration Examples for Interface Templates, on page 32
- Feature History for Interface Templates, on page 33


## Restrictions for Interface Templates

- Remote storing and downloading of templates is not supported.
- To dynamically bind an interface template, the interface template with the same name as referred by AAA Authorization has to be configured on the device.
- Source template configurations are not supported on port channel interface.

## Information About Interface Templates

This section describes an interface template, its types and usage.

### Interface Template Overview

An interface template is a container of configurations or policies that can be applied to specific ports. When an interface template is applied to an access port, it impacts all traffic that is exchanged on the port.

There are two types of interface templates; user and builtin templates. Builtin templates are created by the system.

You can modify builtin templates. If you delete a modified builtin template, the system restores the original definition of the template.

The following are the available builtin templates:

- AP_INTERFACE_TEMPLATE (Access Point)

- DMP_INTERFACE_TEMPLATE (Digital Media Player)
- IP_CAMERA_INTERFACE_TEMPLATE
- IP_PHONE_INTERFACE_TEMPLATE
- LAP_INTERFACE_TEMPLATE (Lightweight Access Point)
- MSP_CAMERA_INTERFACE_TEMPLATE
- MSP_VC_INTERFACE_TEMPLATE (Video Conferencing)
- PRINTER_INTERFACE_TEMPLATE
- ROUTER_INTERFACE_TEMPLATE
- SWITCH_INTERFACE_TEMPLATE
- TP_INTERFACE_TEMPLATE (TelePresence)

Following is an example of a builtin interface template:

```
Template Name       : IP_CAMERA_INTERFACE_TEMPLATE
Modified            : No
Template Definition :
 spanning-tree portfast
 spanning-tree bpduguard enable
 switchport mode access
 switchport block unicast
 switchport port-security
 mls qos trust dscp
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
!
```

You can also create specific user templates with the commands that you want to include.

**Note** The template name must not contain spaces.

You can create an interface template using the **template** command in global configuration mode. In template configuration mode, enter the required commands. The following commands can be entered in template configuration mode:

| Command | Description |
|---|---|
| **access-session** | Configures access session-specific interface commands.<br>This is applicable to Identity-Based Networking Services (IBNS) 2.0 |
| **authentication** | Configures authentication manager Interface Configuration commands.<br>This is applicable to IBNS1.0 |
| **carrier-delay** | Configures delay for interface transitions. |
| **default** | Sets a command to its defaults. |

| Command | Description |
|---|---|
| **description** | Configures interface-specific description. |
| **dot1x** | Configures interface configuration commands for IEEE 802.1X. |
| **ip** | Configures IP template. |
| **keepalive** | Enables keepalive. |
| **load-interval** | Specifies interval for load calculation for an interface. |
| **mab** | Configures MAC authentication bypass Interface. |
| **peer** | Configures peer parameters for point to point interfaces. |
| **service-policy** | Configures CPL service policy. |
| **source** | Gets configurations from another source. |
| **spanning-tree** | Configures spanning tree subsystem |
| **storm-control** | Configures storm control. |
| **subscriber** | Configures subscriber inactivity timeout value. |
| **switchport** | Sets switching mode configurations |

**Note** System builtin templates aren't displayed in the running configuration. These templates show up in the running configuration only if you edit them.

# Binding an Interface Template to a Target

Each template can be bound to a target, like an interface or a sub-interface. A template can be attached to a target either statically or dynamically. Static binding of a template involves binding the template to a target, like an interface. Only one template can be bound at a time using static binding. Static binding of another template to the same target will unbind the previously bound template. To configure static binding, use the **source template** command in interface configuration mode.

Any number of templates can be bound dynamically to a target. To configure dynamic binding using builtin policy maps and parameter maps, enable the Autoconf feature using the **autoconf enable** command.

**Note** You can have statically and dynamically bound templates on the same interface at a time.

# Priority for Configurations Using Interface Templates

Configuration applied through dynamically-bound templates has the highest priority, followed by configuration applied directly on the interface, and then configuration applied through statically-bound templates. When similar commands are present at different priority levels, the one at the highest priority is applied. If a configuration at a higher priority level is not applied, then the configuration with the next highest priority is applied to the target.

Multiple templates can be dynamically bound to a target. When multiple templates are dynamically bound, the template that is applied last has the highest priority.

To delete a template, you must remove the binding to all targets. If you bind a template that does not exist, a new template is created with no configurations.

# How to Configure Interface Templates

Perform the following tasks to configure a user interface template and bind it to a target.

# Configuring Interface Templates

Perform the following task to create user interface templates:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **template** *name*<br>**Example:**<br>`Device(config)# template user-template1` | Creates a user template and enters template configuration mode.<br>**Note**<br>Builtin templates are system-generated. |
| **Step 4** | **load-interval** *interval*<br>**Example:**<br>`Device(config-template)# load-interval 60` | Configures the sampling interval for statistics collections on the template.<br>**Note**<br>Builtin templates are system-generated. |
| **Step 5** | **description** *description*<br>**Example:** | Configures the description for the template. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-template)# description This is a user template` | |
| **Step 6** | **keepalive** *number*<br>**Example:**<br>`Device(config-template)# Keepalive 60` | Configures the keepalive timer. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuring Static Binding for Interface Templates

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 1/0/12` | Specifies the interface type and number and enters interface configuration mode. |
| **Step 4** | **source template** *name*<br>**Example:**<br>`Device(config-if)# source template user-template1` | Statically applies an interface template to a target. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-if)# end` | Exits interface configuration mode and returns to privileged EXEC mode. |

### Example

To verify static binding use the **show running-config interface** *int-name* and the **show derived-config interface** *int-name* commands.

```
Device# show running-config interface GigabitEthernet 1/0/12

Building configuration...

Current configuration : 71 bytes
!
interface GigabitEthernet1/0/12
source template user-template1
end
```

```
Device# show derived-config interface GigabitEthernet 1/0/12
Building configuration...

Derived configuration : 108 bytes
!
interface GigabitEthernet1/0/12
description This is a user template
load-interval 60
keepalive 60
end
```

# Configuring Dynamic Binding of Interface Templates

To configure dynamic binding of interface templates, perform the following tasks:

### Before you begin

Ensure that 802.1x port-based authentication is configured on the device. When you are using the ISE server to download and assign a template that includes **switchport mode** and vlan change commands, the **access-session interface-template sticky** command is used, which is available only in IBNS 2.0. Hence, VLAN changes using a template require IBNS 2.0.

### Procedure

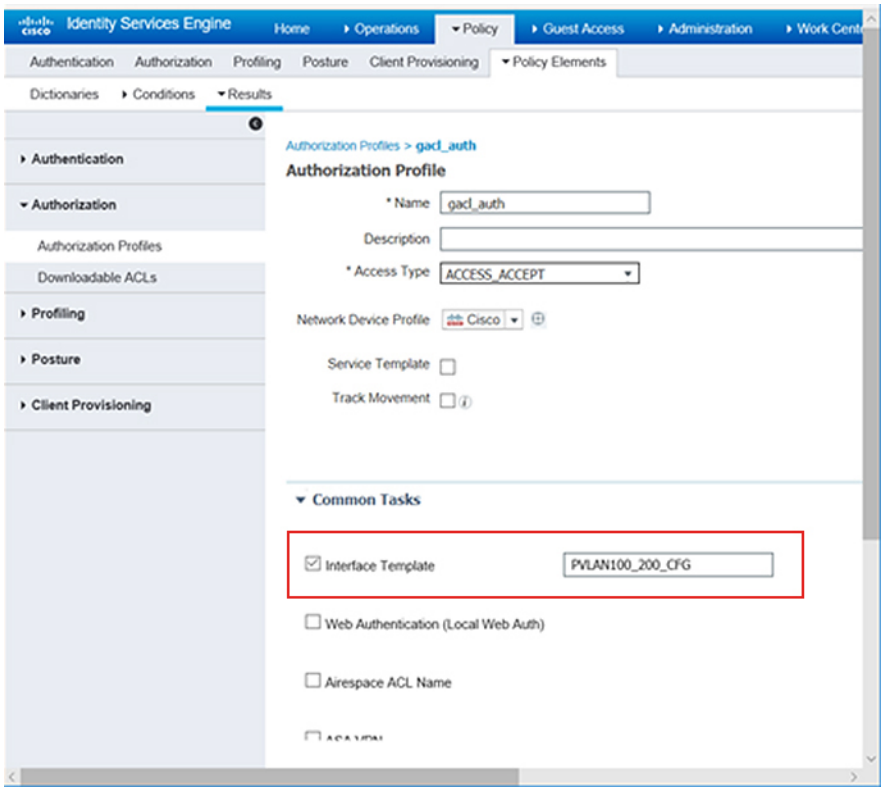
**Step 1** Create a template on the device, as specified in the Configuring Interface Templates, on page 24 procedure.

**Step 2** Configure the Identity Services Engine (ISE) or any other RADIUS server to download the template name to the device interface. The template is assigned after the device is authenticated successfully.

If you're using ISE, go to the **Policy** > **Policy Elements** > **Authorization** > **Authorization Profile** page.

Check the **Interface Template** check box and enter the name of the template to be assigned to the client interface.

*Figure 1: Configure ISE to Assign Interface Template*




If you're using a different RADIUS server, configure the attribute **Cisco-AVpair="interface:template=*name*"** with the name of the template. This configuration pushes the template to the device after the initial client authentication is completed.

**Step 3** To verify that the template name is downloaded to the interface, use the **show authentication sessions interface** *interface-id* **details** or **show access-session interface** *interface-id* **details** command. To verify that the interface template commands are applied to the interface, use the **show derived-config interface** *interface-id* command.

## Example

The following example shows how to verify that a template named del_template is downloaded and applied to the TwentyFiveGigE1/0/3 interface on the device:

```
Device# show running-config | section del_template
template del_template
access-session port-control auto
no access-session monitor
authentication periodic

Device# show authentication sessions interface tw1/0/3 details
Interface: TwentyFiveGigE1/0/3
IIF-ID: 0x1F9EBBA9
MAC Address: 002f.0100.0001
IPv6 Address: Unknown
IPv4 Address: Unknown
```

```
User-Name: NOAS
Device-type: Un-Classified Device
Device-name: Unknown Device
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 0404140B00004E1C6E569E0B
Acct Session ID: Unknown
Handle: 0xdb000e24
Current Policy: DOT1x

Server Policies:
Interface Template: del_template

Method status list:
Method State
dot1x Authc Success


Device# show derived-config interface tw1/0/3
Building configuration...

Derived configuration : 321 bytes
!
interface TwentyFiveGigE1/0/3
switchport access vlan 44
switchport mode access
switchport port-security violation restrict
switchport port-security
authentication periodic
access-session port-control auto
no access-session monitor
mab
dot1x pae authenticator
service-policy type control subscriber DOT1x
end
```

# Verifying Interface Templates

Use one or more of the commands listed below to verify the interface template configuration.

***Table 2: Show commands to verify Interface Template Configuration***

| Command | Purpose |
|---|---|
| **show template interface all** {**all** \| **binding** {*temp-name* \| **all** \| **target** *int-name*} \| **brief** } | Shows all interface template configurations. |
| **show template interface source** {**built-in** [**original**] \| **user**}{*temp-name* \| **all**}} | Shows interface template source configurations. |
| **show template service**{**all** \| **binding target** *int-name* \| **brief** \| **source** {**aaa** \| **built-in** \| **user** {**temp-name** \| **all**}} | Shows all interface template service configurations. |

### Example: Verifying Interface User Template

```
Device# show template interface source user all
    Template Name : TEST-1
    Template Definition:
    load-interval 60
    description TEST_1_TEMPLATE
    keepalive 200
    !
    Template Name : TEST-2
    Template Definition:
    load-interval 60
    description TEST-1_TEMPLATE
    keepalive 200
```

### Example: Verifying all Builtin Templates

```
Device#  show template interface source built-in all

Building configuration...

Template Name : AP_INTERFACE_TEMPLATE
Modified : No
Template Definition :
switchport mode trunk
switchport nonegotiate
service-policy input AutoConf-4.0-Trust-Cos-Input-Policy
service-policy output AutoConf-4.0-Output-Policy
!
Template Name : DMP_INTERFACE_TEMPLATE
Modified : No
Template Definition :
switchport mode access
switchport block unicast
switchport port-security
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input AutoConf-4.0-Trust-Dscp-Input-Policy
service-policy output AutoConf-4.0-Output-Policy
!
Template Name : IP_CAMERA_INTERFACE_TEMPLATE
Modified : No
Template Definition :
switchport mode access
switchport block unicast
switchport port-security
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input AutoConf-4.0-Trust-Dscp-Input-Policy
service-policy output AutoConf-4.0-Output-Policy
!
Template Name : IP_PHONE_INTERFACE_TEMPLATE
Modified : No
Template Definition :
switchport mode access
switchport block unicast
switchport port-security maximum 3
switchport port-security maximum 2 vlan access
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security
storm-control broadcast level pps 1k
storm-control multicast level pps 2k
```

```
storm-control action trap
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input AutoConf-4.0-CiscoPhone-Input-Policy
service-policy output AutoConf-4.0-Output-Policy
ip dhcp snooping limit rate 15
load-interval 30
!
Template Name : LAP_INTERFACE_TEMPLATE
Modified : No
Template Definition :
switchport mode access
switchport block unicast
switchport port-security violation protect
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security
storm-control broadcast level pps 1k
storm-control multicast level pps 2k
storm-control action trap
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
load-interval 30
!
Template Name : MSP_CAMERA_INTERFACE_TEMPLATE
Modified : No
Template Definition :
switchport mode access
switchport block unicast
switchport port-security
spanning-tree portfast
spanning-tree bpduguard enable
!
Template Name : MSP_VC_INTERFACE_TEMPLATE
Modified : No
Template Definition :
switchport mode access
switchport port-security
spanning-tree portfast
spanning-tree bpduguard enable
load-interval 30
!
Template Name : PRINTER_INTERFACE_TEMPLATE
Modified : No
Template Definition :
switchport mode access
switchport port-security maximum 2
switchport port-security
spanning-tree portfast
spanning-tree bpduguard enable
load-interval 60
!
Template Name : ROUTER_INTERFACE_TEMPLATE
Modified : No
Template Definition :
switchport mode trunk
spanning-tree portfast trunk
spanning-tree bpduguard enable
service-policy input AutoConf-4.0-Trust-Cos-Input-Policy
service-policy output AutoConf-4.0-Output-Policy
!
Template Name : SWITCH_INTERFACE_TEMPLATE
Modified : No
```

```
Template Definition :
switchport mode trunk
service-policy input AutoConf-4.0-Trust-Cos-Input-Policy
service-policy output AutoConf-4.0-Output-Policy
!
Template Name : TP_INTERFACE_TEMPLATE
Modified : No
Template Definition :
switchport mode access
switchport port-security maximum 3
switchport port-security maximum 2 vlan access
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
switchport port-security
storm-control broadcast level pps 1k
storm-control multicast level pps 2k
storm-control action trap
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input AutoConf-4.0-Trust-Dscp-Input-Policy
service-policy output AutoConf-4.0-Output-Policy
ip dhcp snooping limit rate 15
load-interval 30
!
end
```

### Example: Verifying Interface Template Binding for all templates

```
Device# show template interface binding all
    Template-name               Source      Method          Interface
    =============               ====      ==========      ==========
IP_PHONE_INTERFACE_TEMPLATE    Built-in    Dynamic        Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                          Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                          Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                          Gi1/0/10, Gi1/0/11, Gi1/0/12
                                                          Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                          Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                          Gi1/0/19, Gi1/0/20, Gi1/0/21
                                                          Gi1/0/22, Gi1/0/23, Gi1/0/24
                                                          Gi1/1/1, Gi1/1/2, Gi1/1/3

IP_PHONE_INTERFACE_TEMPLATE    Built-in     Static        Gi4/0/4
```

### Example: Verifying Static Template Binding for a Target Interface

```
Device# show template interface binding target GigabitEthernet 1/0/4
    Interface            Method       Source             Template
    =========           ==========    =====              =========
    Gi1/0/4              Dynamic      built-in           IP_PHONE_INTERFACE_TEMPLATE
                         Static       user               TEST
                         Dynamic      Modified-built-in TEST
```

### Example: Verifying Dynamic Template Binding for all templates

```
Device# show template service all

    User-defined template:
    ======================

    Template Name      : SVC-1
    Template Definition:
    vlan 100
```

```
access-group acl1

built-in template:
======================

Template Name      : SVC-2
Template Definition:
vlan 100
access-group acl1

aaa downloaded template:
==========================
Template Name      : SVC-2
Template Definition:
vlan 100
access-group acl1
```

### Example: Verifying Template Binding for a Target Interface

```
Device# show template binding target GigabitEthernet 1/0/4

  Interface Templates:
    Interface            method       Source            Template
    =========           ==========    =====             =========
    Gi1/0/4              Dynamic      built-in          IP_PHONE_INTERFACE_TEMPLATE
                         Static       user              TEST
                         Dynamic      Modified-built-in TEST
  Service Templates:
   Template            Source         Session-Mac
   ========            ====           ================
   SVC1                user           aa-bb-cc-dd-ee-ff
   SVC2                built-in       ab-ab-ab-ab-ab-ab
   SVC3                aaa            ac-ac-ac-ac-ac-ac
```

# Configuration Examples for Interface Templates

## Example: Configuring User Interface Templates

### Example: Configuring User Templates

```
Device# enable
Device (config)# configure terminal
Device(config)# template user-template1
Device(config-template)# load-interval 60
Device(config-template)# description This is a user template
Device(config-template)# Keepalive 60
Device(config)# end
```

## Example: Sourcing Interface Templates

```
Device> enable
Device# configure terminal
Device(config)# interface fastethernet 4/0/0
```

```
Device(config-if)# source template user-template1
Device(config-if)# end
```

# Example: Dynamically Binding Interface Templates

Configure a template on the device:

```
Device# configure terminal
Device(config)# tempalte user_template
Device(config-template)# access-session port-control auto
Device(config-template)# no access-session monitor
Device(config-template)# authentication periodic
```

Configure RADIUS Server attribute with the template name:

```
Cisco-AVpair="interface:template=user_template"
```

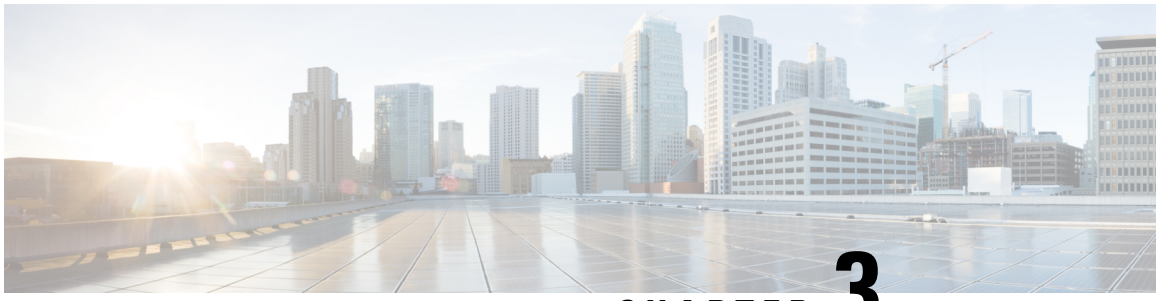
# Feature History for Interface Templates

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless notedotherwise.

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Fuji 16.9.2 | Interface Templates | An interface template provides a mechanism to configure multiple commands at the same time and associate it with a target such as an interface. |
| Cisco IOS XE Bengaluru 17.5.1 | Interface Templates - **cts manual** command | The command **cts manual** was introduced. It can be configured in the template configuration mode. |

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.



CHAPTER 3

# Configuring Cisco Plug and Play


- Configuring Cisco Plug and Play, on page 35
- Feature History for Cisco Plug and Play, on page 35


## Configuring Cisco Plug and Play

For information about configuring Plug and Play, see

- Cisco Plug and Play Feature Guide
- Configuration Guide for Cisco Network Plug and Play on APIC-EM

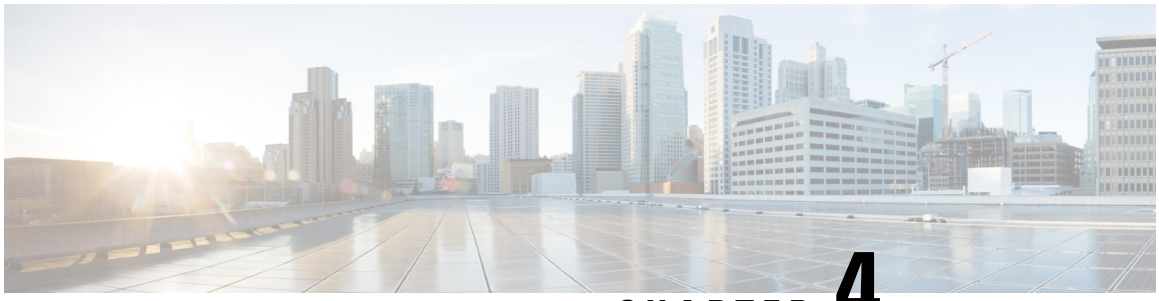
## Feature History for Cisco Plug and Play

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless notedotherwise.

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Fuji 16.9.2 | Cisco Plug and Play | The Cisco Plug and Play solution is a converged solution that provides a highly secure, scalable, seamless, and unified zero-touch deployment experience. |

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.



CHAPTER 4

# Configuring Cisco Discovery Protocol

Cisco Discovery Protocol is a Layer 2, media-independent, and network-independent protocol that runs on Cisco devices and enables networking applications to learn about directly connected devices nearby. This protocol facilitates the management of Cisco devices by discovering these devices, determining how they are configured, and allowing systems using different network-layer protocols to learn about each other.

This module describes Cisco Discovery Protocol Version 2 and how it functions with SNMP.


- Information about Cisco Discovery Protocol, on page 37
- How to Configure Cisco Discovery Protocol, on page 38
- Monitoring and Maintaining Cisco Discovery Protocol, on page 45
- Feature History for Cisco Discovery Protocol, on page 45


# Information about Cisco Discovery Protocol

The following sections provide information about Cisco Discovery Protocol

## Default Cisco Discovery Protocol Configuration

This table shows the default Cisco Discovery Protocol configuration.

| Feature | Default Setting |
|---|---|
| Cisco Discovery Protocol global state | Enabled |
| Cisco Discovery Protocol interface state | Enabled |
| Cisco Discovery Protocol timer (packet update frequency) | 60 seconds |
| Cisco Discovery Protocol holdtime (before discarding) | 180 seconds |
| Cisco Discovery Protocol Version-2 advertisements | Enabled |

## Cisco Discovery Protocol Overview

Cisco Discovery Protocol is a device discovery protocol that runs over Layer 2 (the data-link layer) on all Cisco-manufactured devices (routers, bridges, access servers, controllers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. With Cisco

Discovery Protocol, network management applications can learn the device type and the SNMP agent address of neighboring devices running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices.

Cisco Discovery Protocol runs on all media that support Subnetwork Access Protocol (SNAP). Because Cisco Discovery Protocol runs over the data-link layer only, two systems that support different network-layer protocols can learn about each other.

Each Cisco Discovery Protocol-configured device sends periodic messages to a multicast address, advertising at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime information, which is the length of time a receiving device holds Cisco Discovery Protocol information before discarding it. Each device also listens to the messages sent by other devices to learn about neighboring devices.

On the device, Cisco Discovery Protocol enables Network Assistant to display a graphical view of the network. The device uses Cisco Discovery Protocol to find cluster candidates and maintain information about cluster members and other devices up to three cluster-enabled devices away from the command device by default.

The following applies to a device and connected endpoint devices:

- Cisco Discovery Protocol identifies connected endpoints that communicate directly with the device.
- To prevent duplicate reports of neighboring devices, only one wired device reports the location information.
- The wired device and the endpoints both send and receive location information.

# How to Configure Cisco Discovery Protocol

The following sections provide information about how to configure Cisco Discovery Protocol.

## Configuring Cisco Discovery Protocol Characteristics

You can configure these Cisco Discovery Protocol characteristics:

- Frequency of Cisco Discovery Protocol updates
- Amount of time to hold the information before discarding it
- Whether or not to send Version 2 advertisements

**Note** Steps 3 through 5 are all optional and can be performed in any order.

Follow these steps to configure the Cisco Discovery Protocol characteristics.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:** | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device>enable` | |
| **Step 2** | **configureterminal**<br>**Example:**<br>`Device# configure terminal` | |
| **Step 3** | **cdp timer** *seconds*<br>**Example:**<br>`Device(config)# cdp timer 20` | (Optional) Sets the transmission frequency of Cisco Discovery Protocol updates in seconds.<br>The range is 5 to 254; the default is 60 seconds. |
| **Step 4** | **cdp holdtime** *seconds*<br>**Example:**<br>`Device(config)# cdp holdtime 60` | (Optional) Specifies the amount of time a receiving device should hold the information sent by your device before discarding it.<br>The range is 10 to 255 seconds; the default is 180 seconds. |
| **Step 5** | **cdp advertise-v2**<br>**Example:**<br>`Device(config)# cdp advertise-v2` | (Optional) Configures Cisco Discovery Protocol to send Version 2 advertisements.<br>This is the default state. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 8** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### What to do next

Use the **no** form of the Cisco Discovery Protocol commands to return to the default settings.

# Disabling Cisco Discovery Protocol

Cisco Discovery Protocol is enabled by default.

**Note** Device clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange Cisco Discovery Protocol messages. Disabling Cisco Discovery Protocol can interrupt cluster discovery and device connectivity.

Follow these steps to disable the Cisco Discovery Protocol device discovery capability.

## Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device>enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configureterminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **no cdp run**<br>**Example:**<br>`Device(config)# no cdp run` | Disables Cisco Discovery Protocol. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 5** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 6** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### What to do next

You must reenable Cisco Discovery Protocol to use it.

# Enabling Cisco Discovery Protocol

Cisco Discovery Protocol is enabled by default.

**Note** Device clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange Cisco Discovery Protocol messages. Disabling Cisco Discovery Protocol can interrupt cluster discovery and device connectivity.

Follow these steps to enable Cisco Discovery Protocol when it has been disabled.

### Before you begin

Cisco Discovery Protocol must be disabled, or it cannot be enabled.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device>enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configureterminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **cdp run**<br>**Example:**<br>`Device(config)# cdp run` | Enables Cisco Discovery Protocol if it has been disabled. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 5** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### What to do next

Use the **show run all** command to show that Cisco Discovery Protocol has been enabled. If you enter only **show run**, the enabling of Cisco Discovery Protocol may not be displayed.

# Disabling Cisco Discovery Protocol on an Interface

Cisco Discovery Protocol is enabled by default on all supported interfaces to send and to receive Cisco Discovery Protocol information.

**Note** Device clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange Cisco Discovery Protocol messages. Disabling Cisco Discovery Protocol can interrupt cluster discovery and device connectivity.

**Note** Cisco Discovery Protocol bypass is not supported and may cause a port go into err-disabled state.

Follow these steps to disable Cisco Discovery Protocol on a port.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device>enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configureterminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *interface-id*<br>**Example:**<br>`Device(config)# interface gigabitethernet 1/0/1` | Specifies the interface on which you are disabling Cisco Discovery Protocol, and enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **no cdp enable**<br>**Example:**<br>`Device(config-if)# no cdp enable` | Disables Cisco Discovery Protocol on the interface specified in Step 3. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 7** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Enabling Cisco Discovery Protocol on an Interface

Cisco Discovery Protocol is enabled by default on all supported interfaces to send and to receive Cisco Discovery Protocol information.

**Note** Device clusters and other Cisco devices (such as Cisco IP Phones) regularly exchange Cisco Discovery Protocol messages. Disabling Cisco Discovery Protocol can interrupt cluster discovery and device connectivity.

**Note** Cisco Discovery Protocol bypass is not supported and may cause a port go into err-disabled state.

Follow these steps to enable Cisco Discovery Protocol on a port on which it has been disabled.

### Before you begin

Cisco Discovery Protocol must be disabled on the port that you are trying to Cisco Discovery Protocol enable on, or it cannot be enabled.

## Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device>enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configureterminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *interface-id*<br>**Example:**<br>`Device(config)# interface gigabitethernet1/0/1` | Specifies the interface on which you are enabling Cisco Discovery Protocol, and enters interface configuration mode. |
| **Step 4** | **cdp enable**<br>**Example:**<br>`Device(config-if)# cdp enable` | Enables Cisco Discovery Protocol on a disabled interface. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 7** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Monitoring and Maintaining Cisco Discovery Protocol

*Table 3: Commands for Displaying Cisco Discovery Protocol Information*

| Command | Description |
|---|---|
| **clear cdp counters** | Resets the traffic counters to zero. |
| **clear cdp table** | Deletes the Cisco Discovery Protocol table of information about |
| **show cdp** | Displays global information, such as frequency of transmissions an for packets being sent. |
| **show cdp entry** *entry-name* [**version**] [**protocol**] | Displays information about a specific neighbor.<br>You can enter an asterisk (*) to display all Cisco Discovery Proto or you can enter the name of the neighbor about which you want<br>You can also limit the display to information about the protocols the specified neighbor or information about the version of softwa the device. |
| **show cdp interface** [*interface-id*] | Displays information about interfaces where Cisco Discovery Proto<br>You can limit the display to the interface about which you want i |
| **show cdp neighbors** [*interface-id*] [*detail*] | Displays information about neighbors, including device type, inte number, holdtime settings, capabilities, platform, and port ID.<br>You can limit the display to neighbors of a specific interface or e display to provide more detailed information. |
| **show cdp traffic** | Displays Cisco Discovery Protocol counters, including the numb sent and received and checksum errors. |
| **show ap cdp neighbors** | Displays information regarding the access point's Cisco Discove neighbors. |
| **show ap cdp neighbors detail** | Displays detailed information regarding the access point's Cisco Protocol neighbors. |
| **show ap name** *ap-name* **cdp neighbors** | Displays the Cisco Discovery Protocol information for an access |
| **show ap name** *ap-name* **cdp neighbors detail** | Displays details about a specific access point neighbor that is usi Discovery Protocol. |

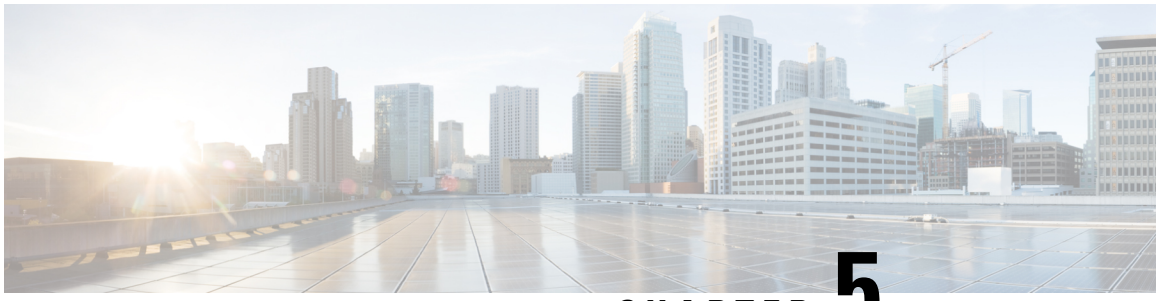
# Feature History for Cisco Discovery Protocol

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Fuji 16.9.2 | Cisco Discovery Protocol | Cisco Discovery Protocol is a Layer 2, media-independent, and network-independent protocol that runs on Cisco devices and enables networking applications to learn about directly connected devices nearby. |

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com.



CHAPTER 5

# Configuring Cisco Discovery Protocol Bypass

In Cisco Discovery Protocol Bypass mode Cisco Discovery Protocol packets are received and transmitted unchanged. Received packets are not processed. No packets are generated. In this mode, 'bump-in-the-wire' behavior is applied to Cisco Discovery Protocol packets. This is a backward compatible mode, equivalent to not having Cisco Discovery Protocol support.


- Restrictions for Cisco Discovery Protocol Bypass, on page 47
- Information about Cisco Discovery Protocol Bypass, on page 47
- How to configure Cisco Discovery Protocol Bypass, on page 48
- Configuration Examples for Cisco Discovery Protocol Bypass, on page 49
- Feature History for Cisco Discovery Protocol Bypass, on page 50


## Restrictions for Cisco Discovery Protocol Bypass

Cisco Discovery Protocol Bypass does not support standard ACLs on the switch port.

## Information about Cisco Discovery Protocol Bypass

When a Cisco IP Phone is plugged into a port that is configured with a Voice VLAN and single-host mode, the phone will be silently allowed onto the network by way of a feature known as Cisco Discovery Protocol Bypass. The phone (or any device) that sends the appropriate Type Length Value (TLV) in a Cisco Discovery Protocol message will be allowed access to the voice VLAN.

In Cisco Discovery Protocol Bypass mode, Cisco Disocvery Protocol packets are received and transmitted unchanged. Received packets are not processed. No packets are generated. In this mode, 'bump-in-the-wire' behaviour is applied to Cisco Discovery Protocol packets. This is a backward compatible mode, equivalent to not having Cisco Discovery Protocol support.

In Cisco Discovery Protocol Bypass mode authentication sessions are established in single and multi-host modes for IP Phones. However, if voice VLAN and 802.1x on an interface port is enabled, then Cisco Discovery Protocol Bypass is enabled when the host mode is set to single or multi-host mode.

It is possible to use the Multi-Domain Authentication (MDA) feature instead of Cisco Discovery Protocol Bypass feature as it provides better Access Control, Visibility and Authorization.

**Note** By default the host mode is set to single mode in legacy mode and multi-authentication in the edge mode.

Cisco Discovery Protocol Enhancement for Second Port Disconnect—Allows a Cisco IP phone to send a Cisco Discovery Protocol message to the switch when a host unplugs from behind the phone. The switch is then able to clear any authenticated session for the indirectly connected host, the same as if the host had been directly connected and the switch had detected a link down event. This is supported in latest IP telephones.

Cisco Discovery Protocol Bypass provides no support for third-party phones—Cisco Discovery Protocol Bypass works only with Cisco phones.

# How to configure Cisco Discovery Protocol Bypass

Follow these steps to enable Cisco Discovery Protocol Bypass:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`# configure terminal` | Enters the global configuration mode. |
| **Step 3** | **interface** *interface-id*<br>**Example:**<br>`(config)# interface GigabitEthernet1/0/12` | Specifies a physical port, and enters interface configuration mode.<br>• Valid interfaces are physical ports. |
| **Step 4** | **switchport mode access**<br>**Example:**<br>`(config-if)# switchport mode access` | Specifies that the interface is in access mode. |
| **Step 5** | **switchport access vlan** *vlan id*<br>**Example:**<br>`(config-if)# switchport access vlan 10` | Assigns all ports as static-access ports in the same VLAN<br>• If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094. |
| **Step 6** | **switchport voice vlan** *vlan-id*<br>**Example:**<br>`(config-if)# switchport voice vlan 3` | Instruct the Cisco IP phone to forward all voice traffic through the specified VLAN. By default, the Cisco IP phone forwards the voice traffic with an 802.1Q priority of 5. |

| | Command or Action | Purpose |
|---|---|---|
| | | Valid VLAN IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image is installed. Do not enter leading zeros. |
| **Step 7** | **authentication port-control auto**<br>**Example:**<br>`(config-if)# authentication port-control auto` | Enables 802.1x authentication on the port. |
| **Step 8** | **authentication host-mode** {**single-host** \| **multi-host**}<br>**Example:**<br>`(config-if)# authentication host-mode single \| multi-host` | The keywords allow the following:<br>• single-host-Single host (client) on an IEEE 802.1X-authorized port.<br>• multi-host-Multiple hosts on an 802.1X-authorized port after a authenticating a single host. |
| **Step 9** | **dot1x pae authenticator**<br>**Example:**<br>`(config-if)# dot1x pae authenticator` | Enables 802.1X authentication on the port with default parameters |

# Configuration Examples for Cisco Discovery Protocol Bypass

## Example: Enabling Cisco Discovery Protocol Bypass

Cisco Discovery Protocol Bypass is enabled by default once 'Authetication port-control auto' is configured with dotx1 or MAB or if voice vlan is configured on interface along with single/multiple host mode.

This following configuration example configures Cisco Disovery Protocol Bypass when authenticating using MAB.

```
 (config)# interface GigabitEthernet1/0/12
(config-if)# switchport mode access
(config-if)# switchport access vlan 10
(config-if)# switchport voice vlan 3
(config-if)# authentication port-control auto
(config-if)# mab
```

## Displaying Cisco Discovery Protocol neighbours

The following configuration example displays Cisco Discovery Protocol neighbours.

```
# show cdp neighbors g1/0/37 detail
Device ID: SEP24B657B038DF
```

```
Entry address(es):
Platform: Cisco IP Phone 9971,  Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/37,  Port ID (outgoing port): Port 1
Holdtime : 157 sec
Second Port Status: Down <<<<<<<<<<
Version :
sip9971.9-1-1SR1
advertisement version: 2
Duplex: full
Power drawn: 12.804 Watts
Power request id: 57146, Power management id: 4
Power request levels are:12804 0 0 0 0
Total cdp entries displayed : 1
```

## Example:Disabling Cisco Discovery Protocol Bypass

To disable Cisco Discovery Protocol Bypass,‘Authetication port-control auto’ needs to be removed from the interface.

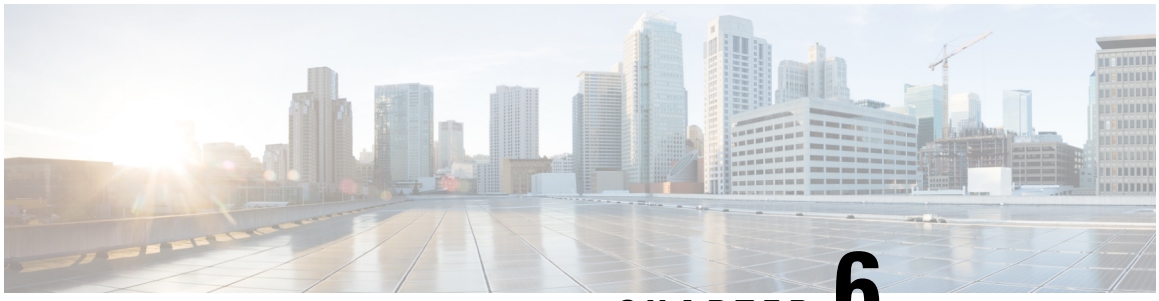
# Feature History for Cisco Discovery Protocol Bypass

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.

***Table 4: Feature History for Cisco Discovery Protocol Bypass***

| Releases | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Fuji 16.9.2 | Cisco Discovery Protocol Bypass | The feature was introduced. |



CHAPTER 6

# Configuring Simple Network Management Protocol


- Prerequisites for SNMP, on page 51
- Restrictions for SNMP, on page 53
- Information About SNMP, on page 54
- How to Configure SNMP, on page 59
- SNMP Examples, on page 68
- Monitoring SNMP Status, on page 69
- Feature History for Simple Network Management Protocol, on page 69


## Prerequisites for SNMP

### Supported SNMP Versions

This software release supports the following SNMP versions:

- SNMPv1—The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.
- SNMPv2C replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the community-string-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic. It has these features:
  - SNMPv2—Version 2 of the Simple Network Management Protocol, a Draft Internet Standard, defined in RFCs 1902 through 1907.
  - SNMPv2C—The community-string-based Administrative Framework for SNMPv2, an Experimental Internet Protocol defined in RFC 1901.
- SNMPv3—Version 3 of the SNMP is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network and includes these security features:
  - Message integrity—Ensures that a packet was not tampered with in transit.
  - Authentication—Determines that the message is from a valid source.
  - Encryption—Mixes the contents of a package to prevent it from being read by an unauthorized source.

**Note** To select encryption, enter the **priv** keyword.

Both SNMPv1 and SNMPv2C use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password.

SNMPv2C includes a bulk retrieval function and more detailed error message reporting to management stations. The bulk retrieval function retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes in SNMPv2C report the error type.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up for a user and the group within which the user resides. A security level is the permitted level of security within a security model. A combination of the security level and the security model determine which security method is used when handling an SNMP packet. Available security models are SNMPv1, SNMPv2C, and SNMPv3.

The following table identifies characteristics and compares different combinations of security models and levels:

***Table 5: SNMP Security Models and Levels***

| Model | Level | Authentication | Encryption | Result |
|---|---|---|---|---|
| SNMPv1 | noAuthNoPriv | Community string | No | Uses a community string match for authentication. |
| SNMPv2C | noAuthNoPriv | Community string | No | Uses a community string match for authentication. |
| SNMPv3 | noAuthNoPriv | Username | No | Uses a username match for authentication. |
| SNMPv3 | authNoPriv | Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) | No | Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. |

| Model | Level | Authentication | Encryption | Result |
|---|---|---|---|---|
| SNMPv3 | authPriv | MD5 or SHA | Data Encryption Standard (DES) or Advanced Encryption Standard (AES) | Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.<br>Allows specifying the User-based Security Model (USM) with these encryption algorithms:<br>• DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.<br>• 3DES 168-bit encryption<br>• AES 128-bit, 192-bit, or 256-bit encryption |

You must configure the SNMP agent to use the SNMP version supported by the management station. Because an agent can communicate with multiple managers, you can configure the software to support communications using SNMPv1, SNMPv2C, or SNMPv3.

# Restrictions for SNMP

### Version Restrictions

- SNMPv1 does not support informs.
- SNMPv3 authentication is not supported in the following scenarios:
  - If there is a change in the switch priority followed by stack reload.
  - If a device with a lower MAC address is added to the stack, the device will be elected as the active switch if all the switches in the stack have the same priority.
- To avoid SNMPv3 authentication failure, you should manually configure SNMP engineID on the device before SNMPv3 user configuration. With this, the user can manage and administer the device as the user is tied to the engineID.

# Information About SNMP

The following sections provide information about SNMP.

## SNMP Overview

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a management information base (MIB). The SNMP manager can be part of a network management system (NMS) such as Cisco Prime Infrastructure. The agent and MIB reside on the device. To configure SNMP on the device, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

## SNMP Manager Functions

The SNMP manager uses information in the MIB to perform the operations described in the following table:

***Table 6: SNMP Operations***

| Operation | Description |
|---|---|
| get-request | Retrieves a value from a specific variable. |
| get-next-request | Retrieves a value from a variable within a table.[1] |
| get-bulk-request[2] | Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. |
| get-response | Replies to a get-request, get-next-request, and set-request sent by an NMS. |
| set-request | Stores a value in a specific variable. |
| trap | An unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred. |

1 With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
2 The get-bulk command only works with SNMPv2 or later.

**Note** We recommend that the SNMP Manager exclude the **ciscoFlashFileDate** MIB object from its query, to avoid performance related issues. This is because, though the **ciscoFlashFileDate** object is published in the MIB, it is not supported on the product.

# SNMP Agent Functions

The SNMP agent can receive requests from one or more SNMP managers. Every request carries the NMS IP address, the number of times an NMS polls the agent, and a timestamp of polling. This information can be tracked for both IPv4 and IPv6 servers.

The SNMP agent responds to SNMP manager requests as follows:

- Get a MIB variable—The SNMP agent begins this function in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Set a MIB variable—The SNMP agent begins this function in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

Use the **show snmp stats hosts** command to display the list of the SNMP managers requests in the queue, and use the **clear snmp stats hosts** command to clear the queue.

The SNMP agent also sends unsolicited trap messages to notify an NMS that a significant event has occurred on the agent. Examples of trap conditions include, but are not limited to, when a port or module goes up or down, when spanning-tree topology changes occur, and when authentication failures occur.

# SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the device, the community string definitions on the NMS must match at least one of the three community string definitions on the device.

A community string can have one of the following attributes:

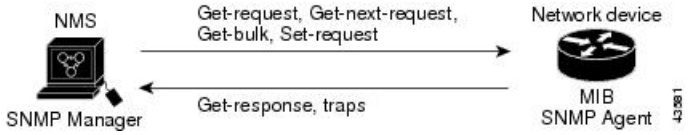
- Read-only (RO)—Gives all objects in the MIB except the community strings read access to authorized management stations, but does not allow write access.
- Read-write (RW)—Gives all objects in the MIB read and write access to authorized management stations, but does not allow access to the community strings.
- When a cluster is created, the command device manages the exchange of messages among member devices and the SNMP application. The Network Assistant software appends the member device number (@esN, where N is the device number) to the first configured RW and RO community strings on the command device and propagates them to the member devices.

# SNMP MIB Variables Access

An example of an NMS is the Cisco Prime Infrastructure network management software. Cisco Prime Infrastructure software uses the device MIB variables to set device variables and to poll devices on the network for specific information. The results of a poll can be displayed as a graph and analyzed to troubleshoot internetworking problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

As shown in the figure, the SNMP agent gathers data from the MIB. The agent can send traps, or notification of certain events, to the SNMP manager, which receives and processes the traps. Traps alert the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in *get-request*, *get-next-request*, and *set-request* format.

*Figure 2: SNMP Network*




# SNMP Flash MIB

The Cisco Flash MIB is used to query flash file data from Cisco devices. Earlier the number of files listed per partition per device in the Flash MIB was limited to 100. Starting with Cisco IOS XE 17.1.1 release, the limitation of Flash MIB listing 100 files per partition per device has been removed. Now Flash MIB will fetch all the files from the flash file system. It is mandatory to use the **snmp mib flash cache** command to perform a Flash MIB walk. The **snmp mib flash cache** command will prefetch all the files into the local Flash MIB cache. Since the 100 file limitation has been removed the Flash MIB walk to retrieve the files will take longer.

**Note** It is recommended that you do not to use the **snmp mib flash cache** command on the Cisco Catalyst 9200/9200L Series Switches due to its impact on the CPU. To prevent SNMP walks from timing out we recommend the snmp walk to have a minimum timeout period of 10 seconds and a default retry of 5 seconds.

# SNMP Notifications

SNMP allows the device to send notifications to SNMP managers when particular events occur. SNMP notifications can be sent as traps or inform requests. In command syntax, unless there is an option in the command to select either traps or informs, the keyword traps refers to either traps or informs, or both. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs.

**Note** SNMPv1 does not support informs.

Traps are unreliable because the receiver does not send an acknowledgment when it receives a trap, and the sender cannot determine if the trap was received. When an SNMP manager receives an inform request, it acknowledges the message with an SNMP response protocol data unit (PDU). If the sender does not receive a response, the inform request can be sent again. Because they can be resent, informs are more likely than traps to reach their intended destination.

The characteristics that make informs more reliable than traps also consume more resources in the device and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request is held in memory until a response is received or the request times out. Traps are sent only once, but an inform might be resent or retried several times. The retries increase traffic and contribute to a higher overhead on the network. Therefore, traps and informs require a trade-off between reliability and resources. If it is important that the SNMP manager receive every notification, use inform requests. If traffic on the network or memory in the device is a concern and notification is not required, use traps.

# SNMP ifIndex MIB Object Values

The SNMP agent's IF-MIB module comes up shortly after reboot. As various physical interface drivers are initialized they register with the IF-MIB module, essentially saying "Give me an ifIndex number". The IF-MIB module assigns the next available ifIndex number on a first-come-first-served basis. That is, minor differences in driver initialization order from one reboot to another can result in the same physical interface getting a different ifIndex number than it had before the reboot (unless ifIndex persistency is enabled of course).

# SNMP ENTITY-MIB Identifiers

ENTITY-MIB contains information for managing physical entities such as field-replaceable units (FRUs), fans. or power supplies on a device. Each entity is identified by a unique index number-*entPhysicalIndex* that is used to access information about the entity in current and other MIBs. An online insertion and removal (OIR) of the entity results in the entity being assigned the next available *entPhysicalIndex* number, irrespective of whether a new entity is inserted or an existing entity is reinserted.

# SNMP and Syslog Over IPv6

To support both IPv4 and IPv6, IPv6 network management requires both IPv6 and IPv4 transports. Syslog over IPv6 supports address data types for these transports.

Simple Network Management Protocol (SNMP) and syslog over IPv6 provide these features:

- Support for both IPv4 and IPv6
- IPv6 transport for SNMP and to modify the SNMP agent to support traps for an IPv6 host
- SNMP- and syslog-related MIBs to support IPv6 addressing
- Configuration of IPv6 hosts as trap receivers

For support over IPv6, SNMP modifies the existing IP transport mapping to simultaneously support IPv4 and IPv6. These SNMP actions support IPv6 transport management:

- Opens User Datagram Protocol (UDP) SNMP socket with default settings
- Provides a new transport mechanism called *SR_IPV6_TRANSPORT*
- Sends SNMP notifications over IPv6 transport
- Supports SNMP-named access lists for IPv6 transport
- Supports SNMP proxy forwarding using IPv6 transport
- Verifies SNMP Manager feature works with IPv6 transport

For information on SNMP over IPv6, including configuration procedures, see the “Managing Cisco IOS Applications over IPv6” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

For information about syslog over IPv6, including configuration procedures, see the “Implementing IPv6 Addressing and Basic Connectivity” chapter in the *Cisco IOS IPv6 Configuration Library* on Cisco.com.

# Default SNMP Configuration

| Feature | Default Setting |
|---|---|
| SNMP agent | Disabled[3]. |
| SNMP trap receiver | None configured. |
| SNMP traps | None enabled except the trap for TCP connections (tty). |
| SNMP version | If no version keyword is present, the default is Version 1. |
| SNMPv3 authentication | If no keyword is entered, the default is the **noauth** (noAuthNoPriv) security level. |
| SNMP notification type | If no type is specified, all notifications are sent. |

[3] This is the default when the device starts and the startup configuration does not have any **snmp-server** global configuration commands.

# SNMP Configuration Guidelines

The device requires one of the following global configuration commands configured in order to open SNMP UDP ports 161 and 162 and enable the SNMP agent: **snmp-server host**, or **snmp-server user**, or **snmp-server community**, or **snmp-server manager**.

An SNMP *group* is a table that maps SNMP users to SNMP views. An SNMP *user* is a member of an SNMP group. An SNMP *host* is the recipient of an SNMP trap operation. An SNMP *engine ID* is a name for the local or remote SNMP engine.

When configuring SNMP, follow these guidelines:

- When configuring an SNMP group, do not specify a notify view. The **snmp-server host** global configuration command auto-generates a notify view for the user and then adds it to the group associated with that user. Modifying the group's notify view affects all users associated with that group.
- To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides.
- Before you configure remote users for a particular agent, configure the SNMP engine ID, using the **snmp-server engineID** global configuration command with the **remote** option. The remote agent's SNMP engine ID and user password are used to compute the authentication and privacy digests. If you do not configure the remote engine ID first, the configuration command fails.
- When configuring SNMP informs, you need to configure the SNMP engine ID for the remote agent in the SNMP database before you can send proxy requests or informs to it.
- If a local user is not associated with a remote host, the device does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.
- Changing the value of the SNMP engine ID has significant results. A user's password (entered on the command line) is converted to an MD5 or SHA security digest based on the password and the local engine ID. The command-line password is then destroyed, as required by RFC 2274. Because of this deletion, if the value of the engine ID changes, the security digests of SNMPv3 users become invalid, and you need to reconfigure SNMP users by using the **snmp-server user** *username* global configuration command. Similar restrictions require the reconfiguration of community strings when the engine ID changes.

- When you configure the SNMP server host with the default UDP port, 162, the output of the **show running-config** command does not display the UDP port value. If you specify a UDP port value other than the default by using the **snmp-server host** {*host-addr*} *community-string* **udp-port** *value* command, the UDP port number will be displayed in the **show running-config** command output. You can configure the **snmp-server host** command with or without the default UDP port 162; however, you cannot configure both simultaneously.

  The following examples are correct:

```
Device(config)# snmp-server host 10.10.10.10 community udp-port 163
Device(config)# snmp-server host 10.10.10.10 community

Device(config)# snmp-server host 10.10.10.10 community udp-port 163
Device(config)# snmp-server host 10.10.10.10 community udp-port 162
```

  The following examples are incorrect:

```
Device(config)# snmp-server host 10.10.10.10 community udp-port 163
Device(config)# snmp-server host 10.10.10.10 community
Device(config)# snmp-server host 10.10.10.10 community udp-port 162

Device(config)# snmp-server host 10.10.10.10 community udp-port 163
Device(config)# snmp-server host 10.10.10.10 community udp-port 162
Device(config)# snmp-server host 10.10.10.10 community
```

# How to Configure SNMP

The following sections provide information on how to configure SNMP.

## SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the device, the community string definitions on the NMS must match at least one of the three community string definitions on the device.

A community string can have one of the following attributes:

- Read-only (RO)—Gives all objects in the MIB except the community strings read access to authorized management stations, but does not allow write access.
- Read-write (RW)—Gives all objects in the MIB read and write access to authorized management stations, but does not allow access to the community strings.
- When a cluster is created, the command device manages the exchange of messages among member devices and the SNMP application. The Network Assistant software appends the member device number (@esN, where N is the device number) to the first configured RW and RO community strings on the command device and propagates them to the member devices.

## Configuring SNMP Groups and Users

You can specify an identification name (engine ID) for the local or remote SNMP server engine on the device. You can configure an SNMP server group that maps SNMP users to SNMP views, and you can add new users to the SNMP group.

Follow these steps to configure SNMP groups and users on the device.

## Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server engineID** {**local** *engineid-string* \| **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}<br>**Example:**<br>`Device(config)# snmp-server engineID local 1234` | Configures a name for either the local or remote copy of SNMP.<br>• The *engineid-string* is a 24-character ID string with the name of the copy of SNMP. You need not specify the entire 24-character engine ID if it has trailing zeros. Specify only the portion of the engine ID up to the point where only zeros remain in the value. The Step Example configures an engine ID of 123400000000000000000000.<br>• If you select **remote**, specify the *ip-address* of the device that contains the remote copy of SNMP and the optional User Datagram Protocol (UDP) port on the remote device. The default is 162. |
| **Step 4** | **snmp-server group** *group-name* {**v1** \| **v2c** \| **v3** {**auth** \| **noauth** \| **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]<br>**Example:**<br>`Device(config)# snmp-server group public v2c access lmnop` | Configures a new SNMP group on the remote device.<br>For *group-name*, specify the name of the group.<br>Specify one of the following security models:<br>• **v1** is the least secure of the possible security models.<br>• **v2c** is the second least secure model. It allows transmission of informs and integers twice the normal width.<br>• **v3**, the most secure, requires you to select one of the following authentication levels: |

| | Command or Action | Purpose |
|---|---|---|
| | | **auth**—Enables the Message Digest 5 (MD5) and the Secure Hash Algorithm (SHA) packet authentication.<br>**noauth**—Enables the noAuthNoPriv security level. This is the default if no keyword is specified.<br>**priv**—Enables Data Encryption Standard (DES) packet encryption (also called privacy).<br>(Optional) Enter **read** *readview* with a string (not to exceed 64 characters) that is the name of the view in which you can only view the contents of the agent.<br>(Optional) Enter **write** *writeview* with a string (not to exceed 64 characters) that is the name of the view in which you enter data and configure the contents of the agent.<br>(Optional) Enter **notify** *notifyview* with a string (not to exceed 64 characters) that is the name of the view in which you specify a notify, inform, or trap.<br>(Optional) Enter **access** *access-list* with a string (not to exceed 64 characters) that is the name of the access list. |
| **Step 5** | **snmp-server user** *username group-name* {**remote** *host* [ **udp-port** *port*] } {**v1** [**access** *access-list*] \| **v2c** [**access** *access-list*] \| **v3** [**encrypted**] [**access** *access-list*] [**auth** {**md5** \| **sha**} *auth-password*] } [*priv* {**des** \| **3des** \| **aes** {**128** \| **192** \| **256**}} *priv-password*]<br>**Example:**<br>`Device(config)# snmp-server user Pat public v2c` | Adds a new user for an SNMP group.<br>The *username* is the name of the user on the host that connects to the agent.<br>The *group-name* is the name of the group to which the user is associated.<br>Enter **remote** to specify a remote SNMP entity to which the user belongs and the hostname or IP address of that entity with the optional UDP port number. The default is 162.<br>Enter the SNMP version number (**v1**, **v2c**, or **v3**). If you enter **v3**, you have these additional options:<br>• **encrypted** specifies that the password appears in encrypted format. This keyword is available only when the **v3** keyword is specified.<br>• **auth** is an authentication level setting session that can be either the |

| | Command or Action | Purpose |
|---|---|---|
| | | HMAC-MD5-96 (**md5**) or the HMAC-SHA-96 (**sha**) authentication level and requires a password string *auth-password* (not to exceed 64 characters).<br><br>If you enter **v3** you can also configure a private (**priv**) encryption algorithm and password string *priv-password* using the following keywords (not to exceed 64 characters):<br>• **priv** specifies the User-based Security Model (USM).<br>• **des** specifies the use of the 56-bit DES algorithm.<br>• **3des** specifies the use of the 168-bit DES algorithm.<br>• **aes** specifies the use of the DES algorithm. You must select either 128-bit, 192-bit, or 256-bit encryption.<br><br>(Optional) Enter **access** *access-list* with a string (not to exceed 64 characters) that is the name of the access list. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 8** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Opening or Closing SNMP UDP Ports

The SNMP process uses ports 161 and 162 where port 161 is used for polling the device and port 162 is used for sending notifications from the agent to the server. The SNMP UDP ports remain closed unless one of the requisite commands is configured. This design provides additional security by opening the ports only when needed and prevents a device from listening to a port unnecessarily.

Beginning in user EXEC mode, follow these steps to open the SNMP UDP ports.

## Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server** {**host** \| **user** \| **community** \| **manager**}<br>**Example:**<br>`Device(config)# snmp-server host` | Opens SNMP UDP ports 161 and 162. Configuring any one of the options (**host**, **user**, **community**, **manager**) opens both ports. To close the ports, enter the **no** form of all the options that you have configured. The ports remain open as long as even one of the keywords is configured.<br>If you enter the **no snmp-server** command, without any of the keywords, the SNMP process is shut down and not just the SNMP UDP ports. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 5** | **show udp**<br>**Example:**<br>`Device# show udp` | Displays the SNMP UDP ports. If one of the requisite commands is configured, ports 161 and 162 will display value `listen` under the remote field. |
| **Step 6** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# SNMP Notifications

SNMP allows the device to send notifications to SNMP managers when particular events occur. SNMP notifications can be sent as traps or inform requests. In command syntax, unless there is an option in the command to select either traps or informs, the keyword traps refers to either traps or informs, or both. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs.

**Note** SNMPv1 does not support informs.

Traps are unreliable because the receiver does not send an acknowledgment when it receives a trap, and the sender cannot determine if the trap was received. When an SNMP manager receives an inform request, it acknowledges the message with an SNMP response protocol data unit (PDU). If the sender does not receive a response, the inform request can be sent again. Because they can be resent, informs are more likely than traps to reach their intended destination.

The characteristics that make informs more reliable than traps also consume more resources in the device and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request is held in memory until a response is received or the request times out. Traps are sent only once, but an inform might be resent or retried several times. The retries increase traffic and contribute to a higher overhead on the network. Therefore, traps and informs require a trade-off between reliability and resources. If it is important that the SNMP manager receive every notification, use inform requests. If traffic on the network or memory in the device is a concern and notification is not required, use traps.

# Setting the Agent Contact and Location Information

Follow these steps to set the system contact and location of the SNMP agent so that these descriptions can be accessed through the configuration file.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server contact** *text*<br>**Example:**<br>`Device(config)# snmp-server contact Dial System Operator at beeper 21555` | Sets the system contact string. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **snmp-server location** *text*<br>**Example:**<br>`Device(config)# snmp-server location Building 3/Room 222` | Sets the system location string. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 7** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Limiting TFTP Servers Used Through SNMP

Follow these steps to limit the TFTP servers used for saving and loading configuration files through SNMP to the servers specified in an access list.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **snmp-server tftp-server-list** *access-list-number*<br>**Example:** | Limits the TFTP servers used for configuration file copies through SNMP to the servers in the access list. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# snmp-server tftp-server-list 44` | For *access-list-number*, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999. |
| **Step 4** | **access-list** *access-list-number* {**deny** \| **permit**} *source* [*source-wildcard*]<br>**Example:**<br>`Device(config)# access-list 44 permit 10.1.1.2` | Creates a standard access list, repeating the command as many times as necessary.<br>For *access-list-number*, enter the access list number specified in Step 3.<br>The **deny** keyword denies access if the conditions are matched. The **permit** keyword permits access if the conditions are matched.<br>For *source*, enter the IP address of the TFTP servers that can access the device.<br>(Optional) For *source-wildcard*, enter the wildcard bits, in dotted decimal notation, to be applied to the source. Place ones in the bit positions that you want to ignore.<br>The access list is always terminated by an implicit deny statement for everything. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 7** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Disabling the SNMP Agent

The **no snmp-server** global configuration command disables all running versions (Version 1, Version 2C, and Version 3) of the SNMP agent on the device and shuts down the SNMP process. You reenable all versions of the SNMP agent by entering one of the following commands in global configuration mode: **snmp-server host**, or **snmp-server user**, or **snmp-server community**, or **snmp-server manager**. There is no Cisco IOS command specifically designated for enabling SNMP.

Follow these steps to disable the SNMP agent.

### Before you begin

The SNMP Agent must be enabled before it can be disabled. The SNMP agent is enabled by the first **snmp-server** global configuration command entered on the device.

## Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **no snmp-server**<br>**Example:**<br>`Device(config)# no snmp-server` | Disables the SNMP agent operation. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 5** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 6** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# SNMP Examples

This example shows how to enable all versions of SNMP. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string *public*. This configuration does not cause the device to send any traps.

```
Device(config)# snmp-server community public
```

This example shows how to permit any SNMP manager to access all objects with read-only permission using the community string *public*. The device also sends VTP traps to the hosts 192.180.1.111 and 192.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string *public* is sent with the traps.

```
Device(config)# snmp-server community public
Device(config)# snmp-server enable traps vtp
Device(config)# snmp-server host 192.180.1.27 version 2c public
Device(config)# snmp-server host 192.180.1.111 version 1 public
Device(config)# snmp-server host 192.180.1.33 public
```

This example shows how to allow read-only access for all objects to members of access list 4 that use the *comaccess* community string. No other SNMP managers have access to any objects. SNMP Authentication Failure traps are sent by SNMPv2C to the host *cisco.com* using the community string *public*.

```
Device(config)# snmp-server community comaccess ro 4
Device(config)# snmp-server enable traps snmp authentication
Device(config)# snmp-server host cisco.com version 2c public
```

This example shows how to send Entity MIB traps to the host *cisco.com*. The community string is restricted. The first line enables the device to send Entity MIB traps in addition to any traps previously enabled. The second line specifies the destination of these traps and overwrites any previous **snmp-server** host commands for the host *cisco.com*.

```
Device(config)# snmp-server enable traps entity
Device(config)# snmp-server host cisco.com restricted entity
```

This example shows how to enable the device to send all traps to the host *myhost.cisco.com* using the community string *public*:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com public
```

This example shows how to associate a user with a remote host and to send **auth** (authNoPriv) authentication-level informs when the user enters global configuration mode:

```
Device(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Device(config)# snmp-server group authgroup v3 auth
Device(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5 mypassword
Device(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Device(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Device(config)# snmp-server enable traps
Device(config)# snmp-server inform retries 0
```

This example shows how to display the entries of SNMP Managers polled to an SNMP Agent:

```
Device# show snmp stats host
Request Count                  Last Timestamp              Address
2                               00:00:01 ago               3.3.3.3
1                               1w2d ago                   2.2.2.2
```

# Monitoring SNMP Status

To display SNMP input and output statistics, including the number of illegal community string entries, errors, and requested variables, use the **show snmp** privileged EXEC command. You also can use the other privileged EXEC commands listed in the table to display SNMP information.

***Table 7: Commands for Displaying SNMP Information***

| Command | Purpose |
|---|---|
| **show snmp** | Displays SNMP statistics. |
| | Displays information on the local SNMP engine and all remote e have been configured on the device. |
| **show snmp group** | Displays information on each SNMP group on the network. |
| **show snmp pending** | Displays information on pending SNMP requests. |
| **show snmp sessions** | Displays information on the current SNMP sessions. |
| **show snmp user** | Displays information on each SNMP user name in the SNMP us<br>**Note**<br>You must use this command to display SNMPv3 configuration in **auth** \| **noauth** \| **priv** mode. This information is not displayed in t **running-config** output. |

# Feature History for Simple Network Management Protocol

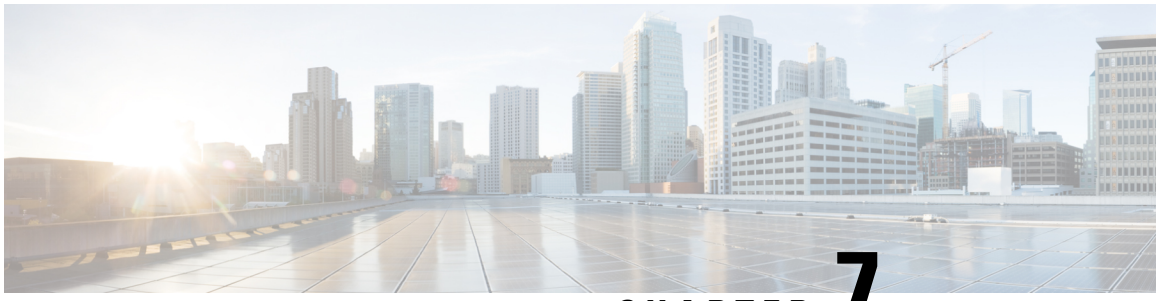
This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless notedotherwise.

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Fuji 16.9.2 | SNMP | SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a management information base (MIB) |

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Amsterdam 17.1.1 | Opening or Closing SNMP UDP ports | The SNMP UDP ports are opened only if one of the requisite commands is configured. This design provides additional security by opening the ports only when needed and prevents a device from listening to a port unnecessarily. |
| | Tracking NMS Polling | The details of the SNMP Manager polled to an SNMP Agent can be displayed. Use the show snmp server stats hosts command to display the NMS IP address, the number of times an NMS polls the agent, and a timestamp of polling. |

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.



CHAPTER 7

# Configuring Service Level Agreements

This chapter describes how to use Cisco IOS IP Service Level Agreements (SLAs) on the switch.

Unless otherwise noted, the term *switch* refers to a standalone switch or a switch stack.


- Restrictions on SLAs, on page 71
- Information About Service Level Agreements, on page 71
- How to Configure IP SLAs Operations, on page 76
- Monitoring IP SLA Operations, on page 89
- Monitoring IP SLA Operation Examples, on page 90
- Additional References, on page 91
- Feature History for Service Level Agreements, on page 92


## Restrictions on SLAs

This section lists the restrictions on SLAs.

The following are restrictions on IP SLAs network performance measurement:

- The device does not support VoIP service levels using the gatekeeper registration delay operations measurements.
- Only a Cisco IOS device can be a source for a destination IP SLAs responder.
- You cannot configure the IP SLAs responder on non-Cisco devices and Cisco IOS IP SLAs can send operational packets only to services native to those devices.

## Information About Service Level Agreements

The following sections provide information about Service Level Agreements.

### Cisco IOS IP Service Level Agreements (SLAs)

Cisco IOS IP SLAs send data across the network to measure performance between multiple network locations or across multiple network paths. They simulate network data and IP services and collect network performance information in real time. Cisco IOS IP SLAs generate and analyze traffic either between Cisco IOS devices or from a Cisco IOS device to a remote IP device such as a network application server. Measurements provided

by the various Cisco IOS IP SLA operations can be used for troubleshooting, for problem analysis, and for designing network topologies.

Depending on the specific Cisco IOS IP SLA operations, various network performance statistics are monitored within the Cisco device and stored in both command-line interface (CLI) and Simple Network Management Protocol (SNMP) MIBs. IP SLA packets have configurable IP and application layer options such as source and destination IP address, User Datagram Protocol (UDP)/TCP port numbers, a type of service (ToS) byte (including Differentiated Services Code Point [DSCP] and IP Prefix bits), Virtual Private Network (VPN) routing/forwarding instance (VRF), and URL web address.

Because Cisco IP SLAs are Layer 2 transport independent, you can configure end-to-end operations over disparate networks to best reflect the metrics that an end user is likely to experience. IP SLAs collect and analyze the following performance metrics:

- Delay (both round-trip and one-way)
- Jitter (directional)
- Packet loss (directional)
- Packet sequencing (packet ordering)
- Path (per hop)
- Connectivity (directional)
- Server or website download time

Because Cisco IOS IP SLAs is SNMP-accessible, it can also be used by performance-monitoring applications like Cisco Prime Internetwork Performance Monitor (IPM) and other third-party Cisco partner performance management products.

Using IP SLAs can provide the following benefits:

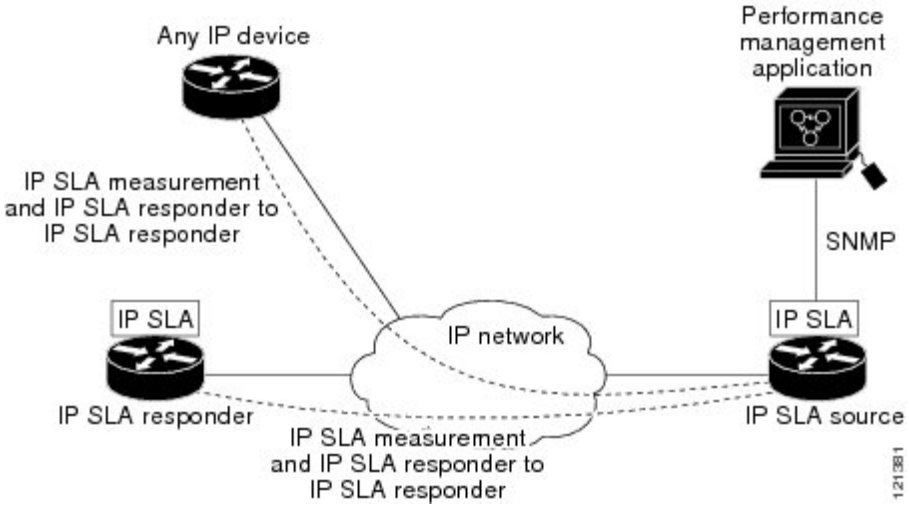
- Service-level agreement monitoring, measurement, and verification.
- Network performance monitoring
  - Measurement of jitter, latency, or packet loss in the network.
  - Continuous, reliable, and predictable measurements.
- IP service network health assessment to verify that the existing QoS is sufficient for new IP services.
- Edge-to-edge network availability monitoring for proactive verification and connectivity testing of network resources (for example, shows the network availability of an NFS server used to store business critical data from a remote site).
- Network operation troubleshooting by providing consistent, reliable measurement that immediately identifies problems and saves troubleshooting time.
- Multiprotocol Label Switching (MPLS) performance monitoring and network verification (if the device supports MPLS).

# Network Performance Measurement with Cisco IOS IP SLAs

You can use IP SLAs to monitor the performance between any area in the network—core, distribution, and edge—without deploying a physical probe. It uses generated traffic to measure network performance between two networking devices.

***Figure 3: Cisco IOS IP SLAs Operation***

The following figure shows how IP SLAs begin when the source device sends a generated packet to the destination device. After the destination device receives the packet, depending on the type of IP SLAs operation, it responds with time-stamp information for the source to make the calculation on performance metrics. An IP SLAs operation performs a network measurement from the source device to a destination in the network using a specific protocol such as UDP.



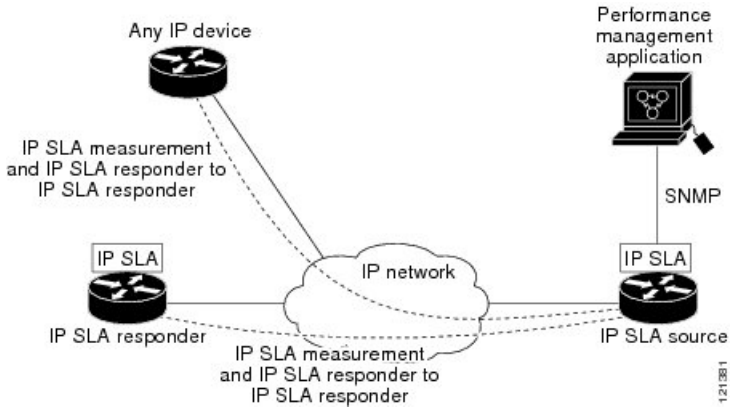

# IP SLA Responder and IP SLA Control Protocol

The IP SLA responder is a component embedded in the destination Cisco device that allows the system to anticipate and respond to IP SLA request packets. The responder provides accurate measurements without the need for dedicated probes. The responder uses the Cisco IOS IP SLA Control Protocol to provide a mechanism through which it can be notified on which port it should listen and respond.

**Note** The IP SLA responder can be a Cisco IOS Layer 2, responder-configurable device. The responder does not need to support full IP SLA functionality.

The following figure shows where the Cisco IOS IP SLA responder fits in the IP network. The responder listens on a specific port for control protocol messages sent by an IP SLA operation. Upon receipt of the control message, it enables the specified UDP or TCP port for the specified duration. During this time, the responder accepts the requests and responds to them. It disables the port after it responds to the IP SLA packet, or when the specified time expires. MD5 authentication for control messages is available for added security.

*Figure 4: Cisco IOS IP SLAs Operation*




You do not need to enable the responder on the destination device for all IP SLA operations. For example, a responder is not required for services that are already provided by the destination router (such as Telnet or HTTP).

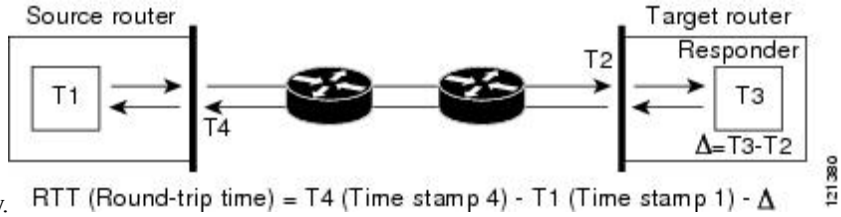
# Response Time Computation for IP SLAs

Switches, controllers, and routers can take tens of milliseconds to process incoming packets due to other high priority processes. This delay affects the response times because the test-packet reply might be in a queue while waiting to be processed. In this situation, the response times would not accurately represent true network delays. IP SLAs minimize these processing delays on the source device as well as on the target device (if the responder is being used) to determine true round-trip times. IP SLA test packets use time stamping to minimize the processing delays.

When the IP SLA responder is enabled, it allows the target device to take time stamps when the packet arrives on the interface at interrupt level and again just as it is leaving, eliminating the processing time. This time stamping is made with a granularity of sub-milliseconds (ms).

*Figure 5: Cisco IOS IP SLA Responder Time Stamping*

The following figure demonstrates how the responder works. Four time stamps are taken to make the calculation for round-trip time. At the target router, with the responder functionality enabled, time stamp 2 (TS2) is subtracted from time stamp 3 (TS3) to produce the time spent processing the test packet as represented by delta. This delta value is then subtracted from the overall round-trip time. Notice that the same principle is applied by IP SLAs on the source router where the incoming time stamp 4 (TS4) is also taken at the interrupt level to allow for greater accuracy.




An additional benefit of the two time stamps at the target device is the ability to track one-way delay, jitter, and directional packet loss. Because much network behavior is asynchronous, it is critical to have these statistics. However, to capture one-way delay measurements, you must configure both the source router and target router with Network Time Protocol (NTP) so that the source and target are synchronized to the same clock source. One-way jitter measurements do not require clock synchronization.

# IP SLAs Operation Scheduling

When you configure an IP SLAs operation, you must schedule the operation to begin capturing statistics and collecting error information. You can schedule an operation to start immediately or to start at a certain month, day, and hour. You can use the *pending* option to set the operation to start at a later time. The pending option is an internal state of the operation that is visible through SNMP. The pending state is also used when an operation is a reaction (threshold) operation waiting to be triggered. You can schedule a single IP SLAs operation or a group of operations at one time.

You can schedule several IP SLAs operations by using a single command through the Cisco IOS CLI or the CISCO RTTMON-MIB. Scheduling the operations to run at evenly distributed times allows you to control the amount of IP SLAs monitoring traffic. This distribution of IP SLA operations helps minimize the CPU utilization and thus improves network scalability.

For more details about the IP SLA multi-operations scheduling functionality, see the "IP SLAs—Multiple Operation Scheduling" chapter of the *Cisco IOS IP SLAs Configuration Guide*.

# IP SLA Operation Threshold Monitoring

To support successful service level agreement monitoring, you must have mechanisms that notify you immediately of any possible violation. IP SLAs can send SNMP traps that are triggered by events such as the following:

- Connection loss
- Timeout
- Round-trip time threshold
- Average jitter threshold
- One-way packet loss
- One-way jitter
- One-way mean opinion score (MOS)
- One-way latency

An IP SLA threshold violation can also trigger another IP SLA operation for further analysis. For example, the frequency could be increased or an Internet Control Message Protocol (ICMP) path echo or ICMP path jitter operation could be initiated for troubleshooting.

### ICMP Echo

The ICMP echo operation measures the end-to-end response time between a Cisco device and any other device that uses IP. The response time is computed by measuring the time it takes to send an ICMP echo request message to a destination and receive an ICMP echo reply. Many customers use IP SLA ICMP-based operations, in-house ping testing, or ping-based dedicated probes to measure this response time. The IP SLA ICMP echo operation conforms to the same specifications as ICMP ping testing, and both methods result in the same response times.

# UDP Jitter

Jitter is a simple term that describes interpacket delay variance. When multiple packets are sent consecutively at an interval of 10 ms from source to destination, the destination should receive them 10 ms apart (if the network is behaving correctly). However, if there are delays in the network (such as queuing, arriving through alternate routes, and so on), the time interval between packet arrivals might be more or less than 10 ms. A positive jitter value indicates that the packets arrived more than 10 ms apart. A negative jitter value indicates that the packets arrived less than 10 ms apart. If the packets arrive 12 ms apart, the positive jitter is 2 ms; if the packets arrive 8 ms apart, the negative jitter is 2 ms. For delay-sensitive networks, positive jitter values are undesirable, and a jitter value of 0 is ideal.

In addition to monitoring jitter, the IP SLA UDP jitter operation can be used as a multipurpose data gathering operation. The packets generated by IP SLAs carry sequence information and time stamps from the source and operational target that include packet sending and receiving data. Based on this data, UDP jitter operations measure the following:

- Per-direction jitter (source to destination and destination to source)
- Per-direction packet-loss
- Per-direction delay (one-way delay)
- Round-trip delay (average round-trip time)

Because the paths for the sending and receiving of data can be different (asymmetric), you can use the per-direction data to more readily identify where congestion or other problems are occurring in the network.

The UDP jitter operation generates synthetic (simulated) UDP traffic and sends a number of UDP packets, each of a specified size, sent a specified number of milliseconds apart, from a source router to a target router, at a given frequency. By default, ten packet-frames, each with a payload size of 10 bytes are generated every 10 ms, and the operation is repeated every 60 seconds. You can configure each of these parameters to best simulate the IP service you want to provide.

To provide accurate one-way delay (latency) measurements, time synchronization (as provided by NTP) is required between the source and the target device. Time synchronization is not required for the one-way jitter and packet loss measurements. If the time is not synchronized between the source and target devices, one-way jitter and packet loss data is returned, but values of 0 are returned for the one-way delay measurements provided by the UDP jitter operation.

# How to Configure IP SLAs Operations

This section does not include configuration information for all available operations as the configuration information details are included in the *Cisco IOS IP SLAs Configuration Guide*. It does include several operations as examples, including configuring the responder, configuring a UDP jitter operation, which requires a responder, and configuring an ICMP echo operation, which does not require a responder. For details about configuring other operations, see the *Cisco IOS IP SLAs Configuration Guide*.

## Default Configuration

No IP SLAs operations are configured.

# Configuration Guidelines

For information on the IP SLA commands, see the *Cisco IOS IP SLAs Command Reference, Release 12.4T* .

For detailed descriptions and configuration procedures, see the *Cisco IOS IP SLAs Configuration Guide, Release 12.4TL*.

Not all of the IP SLA commands or operations described in the referenced guide are supported on the device. The device supports IP service level analysis by using UDP jitter, UDP echo, HTTP, TCP connect, ICMP echo, ICMP path echo, ICMP path jitter, FTP, DNS, and DHCP, as well as multiple operation scheduling and proactive threshold monitoring. It does not support VoIP service levels using the gatekeeper registration delay operations measurements.

Before configuring any IP SLAs application, you can use the **show ip sla application** privileged EXEC command to verify that the operation type is supported on your software image. This is an example of the output from the command:

```
Device# show ip sla application

        IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 33299323
Estimated system max number of entries: 24389

Estimated number of configurable operations: 24389
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *13:04:37.668 UTC Wed Dec 19 2012
```

# Configuring the IP SLA Responder

The IP SLA responder is available only on Cisco IOS software-based devices, including some Layer 2 devices that do not support full IP SLA functionality.

Follow these steps to configure the IP SLA responder on the target device (the operational target):

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode. Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# config t` | Enters the global configuration mode. |
| **Step 3** | **ip sla responder** {**tcp-connect** \| **udp-echo**} **ipaddress** *ip-address* **port** *port-number*<br>**Example:**<br>`Device(config)# ip sla responder udp-echo 172.29.139.134 5000` | Configures the device as an IP SLA responder.<br>The keywords have these meanings:<br>• **tcp-connect**—Enables the responder for TCP connect operations.<br>• **udp-echo**—Enables the responder for User Datagram Protocol (UDP) echo or jitter operations.<br>• **ipaddress** *ip-address*—Enter the destination IP address.<br>• **port** *port-number*—Enter the destination port number.<br>**Note** The IP address and port number must match those configured on the source device for the IP SLA operation. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 7** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Implementing IP SLA Network Performance Measurement

Follow these steps to implement IP SLA network performance measurement on your device:

### Before you begin

Use the **show ip sla application** privileged EXEC command to verify that the desired operation type is supported on your software image.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# config t` | Enters the global configuration mode. |
| **Step 3** | **ip sla** *operation-number*<br>**Example:**<br>`Device(config)# ip sla 10` | Creates an IP SLA operation, and enters IP SLA configuration mode. |
| **Step 4** | **udp-jitter** {*destination-ip-address* \| *destination-hostname*} *destination-port* [**source-ip** {*ip-address* \| *hostname*}] [**source-port** *port-number*] [**control** {**enable** \| **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]<br>**Example:**<br>`Device(config-ip-sla)# udp-jitter 172.29.139.134 5000 source-ip 172.29.139.140 source-port 4000` | Configures the IP SLA operation as the operation type of your choice (a UDP jitter operation is used in the example), and enters its configuration mode (UDP jitter configuration mode is used in the example).<br>• *destination-ip-address* \| *destination-hostname*: Specifies the destination IP address or hostname.<br>• *destination-port*: Specifies the destination port number in the range from 1 to 65535.<br>• (Optional) **source-ip** {*ip-address* \| *hostname*}: Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLA chooses the IP address nearest to the destination<br>• (Optional) **source-port** *port-number*: Specifies the source port number in the range from 1 to 65535. When a port number is not specified, IP SLA chooses an available port. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** If the **udp-jitter** command does not have the source port configured, UDP chooses any random port for control packets. In case UDP chooses the reserved port 1967, it may result in high CPU utilisation by the IP SLA responder.<br>• (Optional) **control**: Enables or disables sending of IP SLA control messages to the IP SLA responder. By default, IP SLA control messages are sent to the destination device to establish a connection with the IP SLA responder<br>• (Optional) **num-packets** *number-of-packets*: Enters the number of packets to be generated. The range is 1 to 6000; the default is 10.<br>• (Optional) **interval** *inter-packet-interval*: Enters the interval between sending packets in milliseconds. The range is 1 to 6000; the default value is 20 ms. |
| **Step 5** | **frequency** *seconds*<br>**Example:**<br>`Device(config-ip-sla-jitter)# frequency 45` | (Optional) Configures options for the SLA operation. This example sets the rate at which a specified IP SLA operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds. |
| **Step 6** | **threshold** *milliseconds*<br>**Example:**<br>`Device(config-ip-sla-jitter)# threshold 200` | (Optional) Configures threshold conditions. This example sets the threshold of the specified IP SLA operation to 200. The range is from 0 to 60000 milliseconds. |
| **Step 7** | **exit**<br>**Example:**<br>`Device(config-ip-sla-jitter)# exit` | Exits the SLA operation configuration mode (UDP jitter configuration mode in this example), and returns to global configuration mode. |
| **Step 8** | **ip sla schedule** *operation-number* [**life** {**forever** \| *seconds*}] [**start-time** {*hh:mm* [:*ss*] [*month day* \| *day month*] \| **pending** \| **now** \| **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]<br>**Example:** | Configures the scheduling parameters for an individual IP SLA operation.<br>• *operation-number*: Enter the RTR entry number. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# ip sla schedule 10 start-time now life forever` | • (Optional) **life**: Sets the operation to run indefinitely (**forever**) or for a specific number of *seconds*. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour).<br>• (Optional) **start-time**: Enters the time for the operation to begin collecting information:<br>To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month.<br>Enter **pending** to select no information collection until a start time is selected.<br>Enter **now** to start the operation immediately.<br>Enter **after** *hh:mm:ss* to show that the operation should start after the entered time has elapsed.<br>• (Optional) **ageout** *seconds*: Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds, the default is 0 seconds (never ages out).<br>• (Optional) **recurring**: Set the operation to automatically run every day. |
| **Step 9** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 10** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 11** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config` | (Optional) Saves your entries in the configuration file. |

| | Command or Action | Purpose |
|---|---|---|
| | `startup-config` | |

### UDP Jitter Configuration

This example shows how to configure a UDP jitter IP SLA operation:

```
Device(config)# ip sla 10
Device(config-ip-sla)# udp-jitter 172.29.139.134 5000 source-ip 172.29.139.140 source-port
 4000
Device(config-ip-sla-jitter)# frequency 30
Device(config-ip-sla-jitter)# exit
Device(config)# ip sla schedule 10 start-time now life forever
Device(config)# end
Device# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

# Analyzing IP Service Levels by Using the UDP Jitter Operation

Follow these steps to configure a UDP jitter operation on the source device:

### Before you begin

You must enable the IP SLA responder on the target device (the operational target) to configure a UDP jitter operation on the source device.

## Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# config t` | Enters the global configuration mode. |
| **Step 3** | **ip sla** *operation-number*<br>**Example:**<br>`Device(config)# ip sla 10` | Creates an IP SLA operation, and enters IP SLA configuration mode. |
| **Step 4** | **udp-jitter** {*destination-ip-address* \| *destination-hostname*} *destination-port* [**source-ip** {*ip-address* \| *hostname*}] [**source-port** *port-number*] [**control** {**enable** \| **disable**}] [**num-packets** *number-of-packets*] [**interval** *interpacket-interval*]<br>**Example:**<br>`Device(config-ip-sla)# udp-jitter 172.29.139.134 5000 source-ip 172.29.139.140 source-port 4000` | Configures the IP SLA operation as a UDP jitter operation, and enters UDP jitter configuration mode.<br>• *destination-ip-address* \| *destination-hostname*: Specifies the destination IP address or hostname.<br>• *destination-port*: Specifies the destination port number in the range from 1 to 65535.<br>• (Optional) **source-ip** {*ip-address* \| *hostname*}: Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLA chooses the IP address nearest to the destination.<br>• (Optional) **source-port** *port-number*: Specifies the source port number in the range from 1 to 65535. When a port number is not specified, IP SLA chooses an available port.<br>**Note** If the **udp-jitter** command does not have the source port configured, UDP chooses any random port for control packets. In case UDP chooses the reserved port 1967, it may result in high CPU utilisation by the IP SLA responder.<br>• (Optional) **control**: Enables or disables sending of IP SLA control messages to |

| | Command or Action | Purpose |
|---|---|---|
| | | the IP SLA responder. By default, IP SLA control messages are sent to the destination device to establish a connection with the IP SLA responder.<br>• (Optional) **num-packets** *number-of-packets*: Enters the number of packets to be generated. The range is 1 to 6000; the default is 10.<br>• (Optional) **interval** *inter-packet-interval*: Enters the interval between sending packets in milliseconds. The range is 1 to 6000; the default value is 20 ms. |
| **Step 5** | **frequency** *seconds*<br>**Example:**<br>`Device(config-ip-sla-jitter)# frequency 45` | (Optional) Sets the rate at which a specified IP SLA operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-ip-sla-jitter)# exit` | Exits UDP jitter configuration mode, and returns to global configuration mode. |
| **Step 7** | **ip sla schedule** *operation-number* [**life** {**forever** \| *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* \| *day month*] \| **pending** \| **now** \| **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]<br>**Example:**<br>`Device(config)# ip sla schedule 10 start-time now life forever` | Configures the scheduling parameters for an individual IP SLA operation.<br>• *operation-number*: Enter the RTR entry number.<br>• (Optional) **life**: Sets the operation to run indefinitely (**forever**) or for a specific number of *seconds*. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour).<br>• (Optional) **start-time**: Enters the time for the operation to begin collecting information:<br>To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month.<br>Enter **pending** to select no information collection until a start time is selected. |

| | Command or Action | Purpose |
|---|---|---|
| | | Enter **now** to start the operation immediately.<br>Enter **after** *hh:mm:ss* to show that the operation should start after the entered time has elapsed.<br>• (Optional) **ageout** *seconds*: Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds, the default is 0 seconds (never ages out).<br>• (Optional) **recurring**: Set the operation to automatically run every day. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 9** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 10** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### Configuring a UDP Jitter IP SLA Operation

This example shows how to configure a UDP jitter IP SLA operation:

```
Device(config)# ip sla 10
Device(config-ip-sla)# udp-jitter 172.29.139.134 5000 source-ip 172.29.139.140 source-port
 4000
Device(config-ip-sla-jitter)# frequency 30
Device(config-ip-sla-jitter)# exit
Device(config)# ip sla schedule 10 start-time now life forever
Device(config)# end
Device# show ip sla configuration 10
IP SLAs, Infrastructure Engine-II.

Entry number: 10
```

```
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 1.1.1.1/0.0.0.0
Target port/Source port: 2/0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

# Analyzing IP Service Levels by Using the ICMP Echo Operation

Follow these steps to configure an ICMP echo operation on the source device:

### Before you begin

This operation does not require the IP SLA responder to be enabled.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# config terminal` | Enters the global configuration mode. |
| **Step 3** | **ip sla** *operation-number*<br>**Example:**<br>`Device(config)# ip sla 10` | Creates an IP SLA operation and enters IP SLA configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **icmp-echo** {*destination-ip-address* \| *destination-hostname*} [**source-ip** {*ip-address* \| *hostname*} \| **source-interface** *interface-id*]<br>**Example:**<br>`Device(config-ip-sla)# icmp-echo 172.29.139.134` | Configures the IP SLA operation as an ICMP Echo operation and enters ICMP echo configuration mode.<br>• *destination-ip-address* \| *destination-hostname*—Specifies the destination IP address or hostname.<br>• (Optional) **source-ip** {*ip-address* \| *hostname*}—Specifies the source IP address or hostname. When a source IP address or hostname is not specified, IP SLA chooses the IP address nearest to the destination.<br>• (Optional) **source-interface** *interface-id*—Specifies the source interface for the operation. |
| **Step 5** | **frequency** *seconds*<br>**Example:**<br>`Device(config-ip-sla-echo)# frequency 30` | (Optional) Sets the rate at which a specified IP SLA operation repeats. The range is from 1 to 604800 seconds; the default is 60 seconds. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-ip-sla-echo)# exit` | Exits UDP echo configuration mode, and returns to global configuration mode. |
| **Step 7** | **ip sla schedule** *operation-number* [**life** {**forever** \| *seconds*}] [**start-time** {*hh:mm* [*:ss*] [*month day* \| *day month*] \| **pending** \| **now** \| **after** *hh:mm:ss*] [**ageout** *seconds*] [**recurring**]<br>**Example:**<br>`Device(config)# ip sla schedule 10 start-time now life forever` | Configures the scheduling parameters for an individual IP SLA operation.<br>• *operation-number*—Enter the RTR entry number.<br>• (Optional) **life**—Sets the operation to run indefinitely (**forever**) or for a specific number of *seconds*. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour)<br>• (Optional) **start-time**—Enter the time for the operation to begin collecting information:<br>To start at a specific time, enter the hour, minute, second (in 24-hour notation), and day of the month. If no month is entered, the default is the current month. |

| | Command or Action | Purpose |
|---|---|---|
| | | Enter **pending** to select no information collection until a start time is selected.<br>Enter **now** to start the operation immediately.<br>Enter **after** *hh:mm:ss* to indicate that the operation should start after the entered time has elapsed.<br>• (Optional) **ageout** *seconds*—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The range is 0 to 2073600 seconds; the default is 0 seconds (never ages out).<br>• (Optional) **recurring**—Sets the operation to automatically run every day. |
| **Step 8** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 9** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 10** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### Configuring an ICMP Echo IP SLA Operation

This example shows how to configure an ICMP echo IP SLA operation:

```
Device(config)# ip sla 10
Device(config-ip-sla)# icmp-echo 172.29.139.134
Device(config-ip-sla-echo)# frequency 30
Device(config-ip-sla-echo)# exit
Device(config)# ip sla schedule 10 start-time now life forever
Device(config)# end
Device# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.
```

```
Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 2.2.2.2
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Vrf Name:
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

# Monitoring IP SLA Operations

The following table describes the commands used to display IP SLA operation configurations and results:

***Table 8: Monitoring IP SLA Operations***

| | |
|---|---|
| **show ip sla application** | Displays global informatio |
| **show ip sla authentication** | Displays IP SLA authentic |
| **show ip sla configuration** [*entry-number*] | Displays configuration val operations or a specific op |
| **show ip sla enhanced-history** {**collection-statistics** \| **distribution statistics**} [*entry-number*] | Displays enhanced history or distribution statistics fo operation. |
| **show ip sla ethernet-monitor configuration** [*entry-number*] | Displays IP SLA automati |
| **show ip sla group schedule** [*schedule-entry-number*] | Displays IP SLA group sc |
| **show ip sla history** [*entry-number* \| **full** \| **tabular**] | Displays history collected |

| | |
|---|---|
| **show ip sla mpls-lsp-monitor** {**collection-statistics** \| **configuration** \| **ldp operational-state** \| **scan-queue** \| **summary** [*entry-number*] \| **neighbors**} | Displays MPLS label switche operations. |
| **show ip sla reaction-configuration** [*entry-number*] | Displays the configured proact all IP SLA operations or a spe |
| **show ip sla reaction-trigger** [*entry-number*] | Displays the reaction trigger i or a specific operation. |
| **show ip sla responder** | Displays information about th |
| **show ip sla statistics** [*entry-number* \| **aggregated** \| **details**] | Displays current or aggregate |

# Monitoring IP SLA Operation Examples

The following example shows all IP SLAs by application:

```
Device# show ip sla application

        IP Service Level Agreements
Version: Round Trip Time MIB 2.2.0, Infrastructure Engine-III

Supported Operation Types:
        icmpEcho, path-echo, path-jitter, udpEcho, tcpConnect, http
        dns, udpJitter, dhcp, ftp, udpApp, wspApp

Supported Features:
        IPSLAs Event Publisher

IP SLAs low memory water mark: 33299323
Estimated system max number of entries: 24389

Estimated number of configurable operations: 24389
Number of Entries configured  : 0
Number of active Entries      : 0
Number of pending Entries     : 0
Number of inactive Entries    : 0
Time of last change in whole IP SLAs: *13:04:37.668 UTC Wed Dec 19 2012
```

The following example shows all IP SLA distribution statistics:

```
Device# show ip sla enhanced-history distribution-statistics

Point by point Enhanced History
Entry    = Entry Number
Int      = Aggregation Interval
BucI     = Bucket Index
StartT   = Aggregation Start Time
Pth      = Path index
Hop      = Hop in path index
Comps    = Operations completed
OvrTh    = Operations completed over thresholds
SumCmp   = Sum of RTT (milliseconds)
SumCmp2L = Sum of RTT squared low 32 bits (milliseconds)
SumCmp2H = Sum of RTT squared high 32 bits (milliseconds)
TMax     = RTT maximum (milliseconds)
TMin     = RTT minimum (milliseconds)
```

```
Entry Int BucI StartT     Pth Hop Comps OvrTh SumCmp     SumCmp2L   SumCmp2H   T
Max    TMin
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco Medianet Metadata Guide | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mdata/configuration/15-sy/mdata-15sy-book/metadata-framework.pdf |
| Cisco Media Services Proxy Configuration Guide | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/msp/configuration/15-mt/msp-15-mt-book.pdf |
| Cisco Mediatrace and Cisco Performance Monitor Configuration Guide | http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/media_monitoring/configuration/15-mt/mm-15-mt-book/mm-mediatrace.html |

### Error Message Decoder

| Description | Link |
|---|---|
| To help you research and resolve system error messages in this release, use the Error Message Decoder tool. | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi |

### MIBs

| MIB | MIBs Link |
|---|---|
| All supported MIBs for this release. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

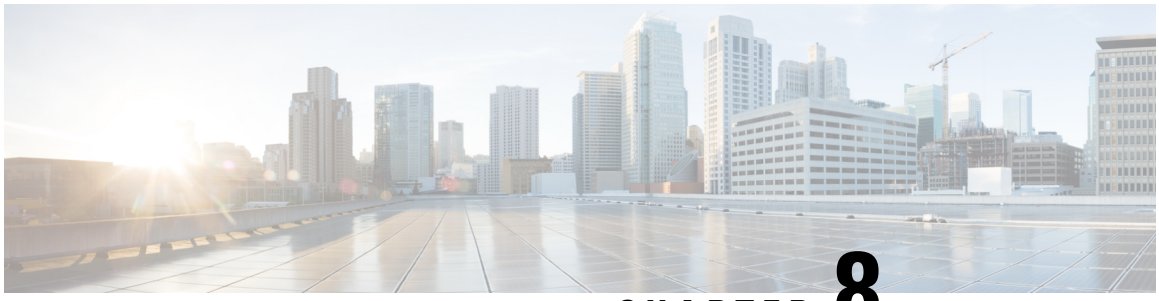
# Feature History for Service Level Agreements

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless notedotherwise.

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Fuji 16.9.2 | Service Level Agreements | Cisco IOS IP Service Level Agreements send data across the network to measure performance between multiple network locations or across multiple network paths. They simulate network data and IP services and collect network performance information in real time. |

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.



CHAPTER 8

# Configuring SPAN and RSPAN


- Prerequisites for SPAN and RSPAN, on page 93
- Restrictions for SPAN and RSPAN, on page 93
- Information About SPAN and RSPAN, on page 95
- Configuring SPAN and RSPAN, on page 104
- How to Configure SPAN and RSPAN, on page 105
- Monitoring SPAN and RSPAN Operations, on page 127
- Configuration Examples for SPAN and RSPAN, on page 127
- Feature History for SPAN and RSPAN, on page 129


## Prerequisites for SPAN and RSPAN

### SPAN

You can limit SPAN traffic to specific VLANs by using the **filter vlan** keyword. If a trunk port is being monitored, only traffic on the VLANs specified with this keyword is monitored. By default, all VLANs are monitored on a trunk port.

### RSPAN

We recommend that you configure an RSPAN VLAN before you configure an RSPAN source or a destination session.

## Restrictions for SPAN and RSPAN

### SPAN

The restrictions for SPAN are as follows:

- On each device, you can configure 66 sessions. A maximum of 8 source sessions can be configured and the remaining sessions can be configured as RSPAN destinations sessions. A source session is either a local SPAN session or an RSPAN source session.
- For SPAN sources, you can monitor traffic for a single port or VLAN or a series or range of ports or VLANs for each session. You cannot mix source ports and source VLANs within a single SPAN session.

- The destination port cannot be a source port; a source port cannot be a destination port.
- You cannot have two SPAN sessions using the same destination port.
- When you configure a device port as a SPAN destination port, it is no longer a normal device port; only monitored traffic passes through the SPAN destination port.
- Entering SPAN configuration commands does not remove previously configured SPAN parameters. You must enter the **no monitor session** {*session_number* | **all** | **local** | **remote**} global configuration command to delete configured SPAN parameters.
- For local SPAN, outgoing packets through the SPAN destination port carry the original encapsulation headers—untagged, ISL, or IEEE 802.1Q—if the **encapsulation replicate** keywords are specified. If the keywords are not specified, the packets are sent in native form.
- You can configure a disabled port to be a source or destination port, but the SPAN function does not start until the destination port and at least one source port or source VLAN are enabled.
- You cannot mix source VLANs and filter VLANs within a single SPAN session.

Traffic monitoring in a SPAN session has the following restrictions:

- Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.
- Wireshark does not capture egress packets when egress span is active.
- You can run both a local SPAN and an RSPAN source session in the same device or device stack. The device or device stack supports a total of 66 source and RSPAN destination sessions.
- You can configure two separate SPAN or RSPAN source sessions with separate or overlapping sets of SPAN source ports and VLANs. Both switched and routed ports can be configured as SPAN sources and destinations.
- You can have multiple destination ports in a SPAN session, but no more than 64 destination ports per device stack .
- SPAN sessions do not interfere with the normal operation of the device. However, an oversubscribed SPAN destination, for example, a 10-Mb/s port monitoring a 100-Mb/s port, can result in dropped or lost packets.
- When SPAN or RSPAN is enabled, each packet being monitored is sent twice, once as normal traffic and once as a monitored packet. Monitoring a large number of ports or VLANs could potentially generate large amounts of network traffic.
- You can configure SPAN sessions on disabled ports; however, a SPAN session does not become active unless you enable the destination port and at least one source port or VLAN for that session.
- The device does not support a combination of local SPAN and RSPAN in a single session.
  - An RSPAN source session cannot have a local destination port.
  - An RSPAN destination session cannot have a local source port.
  - An RSPAN destination session and an RSPAN source session that are using the same RSPAN VLAN cannot run on the same device or device stack.
- SPAN sessions capture only Dynamic Host Configuration Protocol (DHCP) ingress packets when DHCP snooping is enabled on the device.

### RSPAN

The restrictions for RSPAN are as follows:

- RSPAN does not support BPDU packet monitoring or other Layer 2 device protocols.
- The RSPAN VLAN is configured only on trunk ports and not on access ports. To avoid unwanted traffic in RSPAN VLANs, make sure that the VLAN remote-span feature is supported in all the participating devices.
- RSPAN VLANs are included as sources for port-based RSPAN sessions when source trunk ports have active RSPAN VLANs. RSPAN VLANs can also be sources in SPAN sessions. However, since the device does not monitor spanned traffic, it does not support egress spanning of packets on any RSPAN VLAN identified as the destination of an RSPAN source session on the device.
- If you enable VTP and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network for VLAN IDs that are lower than 1005.
- It is recommended not to configure RSPAN VLAN as Native VLAN.
- RSPAN sessions do not capture DHCP-inject packets. DHCP-inject packets refer to DHCP packets (DISCOVER, OFFER, REQUEST, and ACK packets) which are modified by the CPU and inserted back into the network.

# Information About SPAN and RSPAN

The following sections provide information about SPAN and RSPAN.

## SPAN and RSPAN

You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the device or on another device that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source VLANs can be monitored by using SPAN; traffic routed to a source VLAN cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another VLAN to the source VLAN cannot be monitored; however, traffic that is received on the source VLAN and routed to another VLAN can be monitored.

You can use the SPAN or RSPAN destination port to inject traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) sensor appliance to a destination port, the IDS device can send TCP reset packets to close down the TCP session of a suspected attacker.

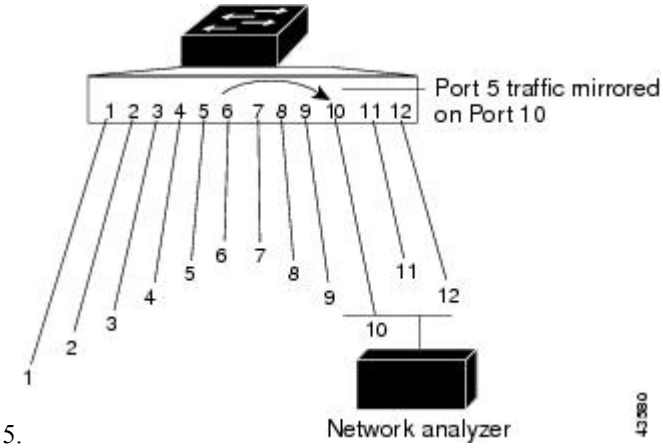
### Local SPAN

Local SPAN supports a SPAN session entirely within one device; all source ports or source VLANs and destination ports are in the same device or device stack. Local SPAN copies traffic from one or more source ports in any VLAN or from one or more VLANs to a destination port for analysis.

Local SPAN supports a SPAN session entirely within one switch; all source ports and destination ports are in the same switch. Local SPAN copies traffic from one or more source ports to a destination port for analysis.

***Figure 6: Example of Local SPAN Configuration on a Single Device***

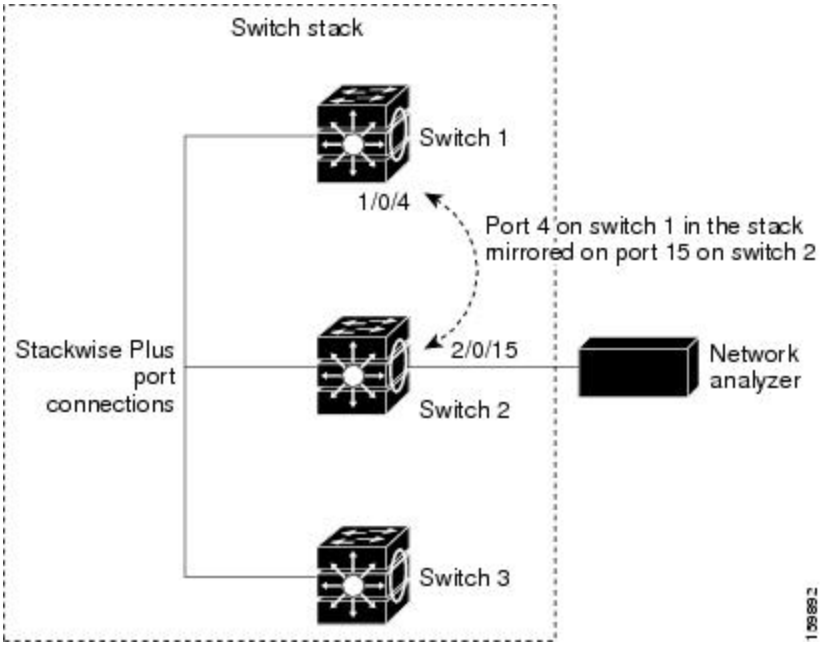
All traffic on port 5 (the source port) is mirrored to port 10 (the destination port). A network analyzer on port 10 receives all network traffic from port 5 without being physically attached to port




5.

***Figure 7: Example of Local SPAN Configuration on a Device Stack***

This is an example of a local SPAN in a device stack, where the source and destination ports reside on different stack members.

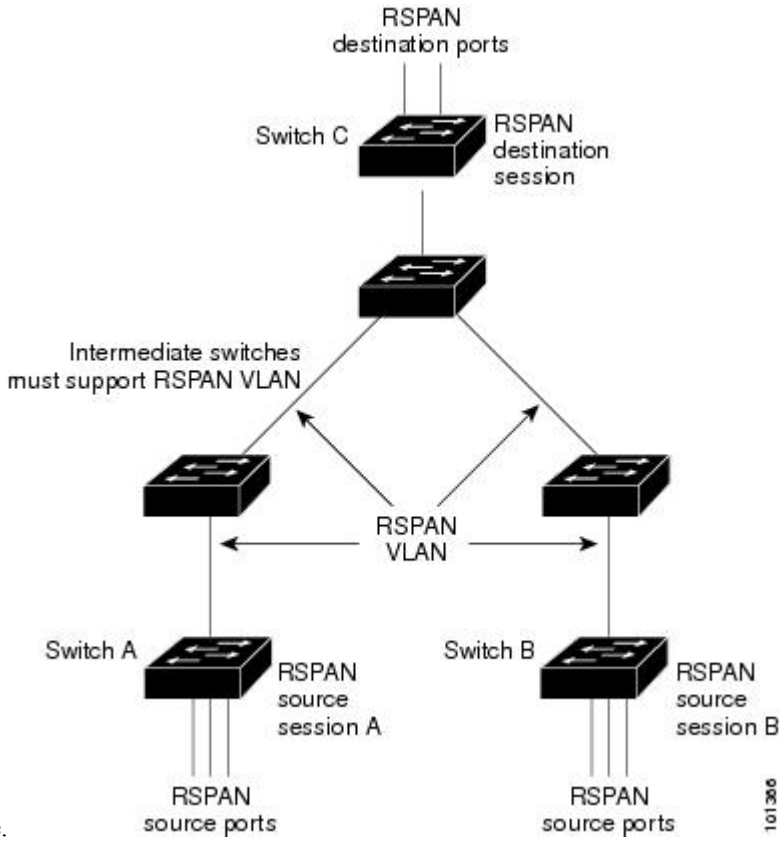



## Remote SPAN

RSPAN supports source ports, source VLANs, and destination ports on different devices (or different device stacks), enabling remote monitoring of multiple devices across your network.

*Figure 8: Example of RSPAN Configuration*

The figure below shows source ports on Device A and Device B. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating devices. The RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and forwarded over trunk ports carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN. Each RSPAN source device must have either ports or VLANs as RSPAN sources. The destination is always a physical port, as shown on Device C in the figure.




## SPAN and RSPAN Concepts and Terminology

### SPAN Sessions

SPAN sessions (local or remote) allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports.

A local SPAN session is an association of a destination port with source ports or source VLANs, all on a single network device. Local SPAN does not have separate source and destination sessions. Local SPAN sessions gather a set of ingress and egress packets specified by the user and form them into a stream of SPAN data, which is directed to the destination port.

RSPAN consists of at least one RSPAN source session, an RSPAN VLAN, and at least one RSPAN destination session. You separately configure RSPAN source sessions and RSPAN destination sessions on different network devices. To configure an RSPAN source session on a device, you associate a set of source ports or source VLANs with an RSPAN VLAN. The output of this session is the stream of SPAN packets that are sent to the RSPAN VLAN. To configure an RSPAN destination session on another device, you associate the

destination port with the RSPAN VLAN. The destination session collects all RSPAN VLAN traffic and sends it out the RSPAN destination port.

An RSPAN source session is very similar to a local SPAN session, except for where the packet stream is directed. In an RSPAN source session, SPAN packets are relabeled with the RSPAN VLAN ID and directed over normal trunk ports to the destination device.

An RSPAN destination session takes all packets received on the RSPAN VLAN, strips off the VLAN tagging, and presents them on the destination port. The session presents a copy of all RSPAN VLAN packets (except Layer 2 control packets) to the user for analysis.

Traffic monitoring in a SPAN session has these restrictions:

- Sources can be ports or VLANs, but you cannot mix source ports and source VLANs in the same session.
- You can run both a local SPAN and an RSPAN source session in the same device or device stack. The device or device stack supports a total of 66 source and RSPAN destination sessions.
- You can configure two separate SPAN or RSPAN source sessions with separate or overlapping sets of SPAN source ports and VLANs. Both switched and routed ports can be configured as SPAN sources and destinations.
- You can have multiple destination ports in a SPAN session, but no more than 64 destination ports per device stack.
- SPAN sessions do not interfere with the normal operation of the device. However, an oversubscribed SPAN destination, for example, a 10-Mb/s port monitoring a 100-Mb/s port, can result in dropped or lost packets.
- When SPAN or RSPAN is enabled, each packet being monitored is sent twice, once as normal traffic and once as a monitored packet. Therefore monitoring a large number of ports or VLANs could potentially generate large amounts of network traffic.
- You can configure SPAN sessions on disabled ports; however, a SPAN session does not become active unless you enable the destination port and at least one source port or VLAN for that session.
- The device does not support a combination of local SPAN and RSPAN in a single session.
  - An RSPAN source session cannot have a local destination port.
  - An RSPAN destination session cannot have a local source port.
  - An RSPAN destination session and an RSPAN source session that are using the same RSPAN VLAN cannot run on the same device or device stack.

## Monitored Traffic

SPAN sessions can monitor these traffic types:

- Receive (Rx) SPAN—Receive (or ingress) SPAN monitors as much as possible all of the packets received by the source interface or VLAN before any modification or processing is performed by the device. A copy of each packet received by the source is sent to the destination port for that SPAN session.

  Packets that are modified because of routing or Quality of Service (QoS)—for example, modified Differentiated Services Code Point (DSCP)—are copied before modification.

  Features that can cause a packet to be dropped during receive processing have no effect on ingress SPAN; the destination port receives a copy of the packet even if the actual incoming packet is dropped. These

features include IP standard and extended input Access Control Lists (ACLs), ingress QoS policing, VLAN ACLs, and egress QoS policing.

- Transmit (Tx) SPAN—Transmit (or egress) SPAN monitors as much as possible all of the packets sent by the source interface after all modification and processing is performed by the device. A copy of each packet sent by the source is sent to the destination port for that SPAN session. The copy is provided after the packet is modified.

  Packets that are modified because of routing (for example, with modified time-to-live (TTL), MAC address, or QoS values) are duplicated (with the modifications) at the destination port.

  Features that can cause a packet to be dropped during transmit processing also affect the duplicated copy for SPAN. These features include IP standard and extended output ACLs and egress QoS policing.

- Both—In a SPAN session, you can also monitor a port or VLAN for both received and sent packets. This is the default.

Therefore, a local SPAN session with encapsulation replicate enabled can have a mixture of untagged and IEEE 802.1Q tagged packets appear on the destination port.

Device congestion can cause packets to be dropped at ingress source ports, egress source ports, or SPAN destination ports. In general, these characteristics are independent of one another. For example:

- A packet might be forwarded normally but dropped from monitoring due to an oversubscribed SPAN destination port.
- An ingress packet might be dropped from normal forwarding, but still appear on the SPAN destination port.
- An egress packet dropped because of device congestion is also dropped from egress SPAN.

In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination port. For example, a bidirectional (both Rx and Tx) SPAN session is configured for the Rx monitor on port A and Tx monitor on port B. If a packet enters the device through port A and is switched to port B, both incoming and outgoing packets are sent to the destination port. Both packets are the same unless a Layer 3 rewrite occurs, in which case the packets are different because of the packet modification.

## Source Ports

A source port (also called a monitored port) is a switched or routed port that you monitor for network traffic analysis.

In a local SPAN session or RSPAN source session, you can monitor source ports or VLANs for traffic in one or both directions.

The device supports any number of source ports (up to the maximum number of available ports on the device) and any number of source VLANs (up to the maximum number of VLANs supported).

You cannot mix ports and VLANs in a single session.

A source port has these characteristics:

- It can be monitored in multiple SPAN sessions.
- Each source port can be configured with a direction (ingress, egress, or both) to monitor.
- It can be any port type (for example, EtherChannel, Gigabit Ethernet, and so forth).

- For EtherChannel sources, you can monitor traffic for the entire EtherChannel or individually on a physical port as it participates in the port channel.
- It can be an access port, trunk port, routed port, or voice VLAN port.
- It cannot be a destination port.
- Source ports can be in the same or different VLANs.
- You can monitor multiple source ports in a single session.

### Source VLANs

VLAN-based SPAN (VSPAN) is the monitoring of the network traffic in one or more VLANs. The SPAN or RSPAN source interface in VSPAN is a VLAN ID, and traffic is monitored on all the ports for that VLAN.

VSPAN has these characteristics:

- All active ports in the source VLAN are included as source ports and can be monitored in either or both directions.
- On a given port, only traffic on the monitored VLAN is sent to the destination port.
- If a destination port belongs to a source VLAN, it is excluded from the source list and is not monitored.
- If ports are added to or removed from the source VLANs, the traffic on the source VLAN received by those ports is added to or removed from the sources being monitored.
- You cannot use filter VLANs in the same session with VLAN sources.
- You can monitor only Ethernet VLANs.

### VLAN Filtering

When you monitor a trunk port as a source port, by default, all VLANs active on the trunk are monitored. You can limit SPAN traffic monitoring on trunk source ports to specific VLANs by using VLAN filtering.

- VLAN filtering applies only to trunk ports or to voice VLAN ports.
- VLAN filtering applies only to port-based sessions and is not allowed in sessions with VLAN sources.
- When a VLAN filter list is specified, only those VLANs in the list are monitored on trunk ports or on voice VLAN access ports.
- SPAN traffic coming from other port types is not affected by VLAN filtering; that is, all VLANs are allowed on other ports.
- VLAN filtering affects only traffic forwarded to the destination SPAN port and does not affect the switching of normal traffic.

### Destination Port

Each local SPAN session or RSPAN destination session must have a destination port (also called a monitoring port) that receives a copy of traffic from the source ports or VLANs and sends the SPAN packets to the user, usually a network analyzer.

A destination port has these characteristics:

- For a local SPAN session, the destination port must reside on the same device or device stack as the source port. For an RSPAN session, it is located on the device containing the RSPAN destination session. There is no destination port on a device or device stack running only an RSPAN source session.
- When a port is configured as a SPAN destination port, the configuration overwrites the original port configuration. When the SPAN destination configuration is removed, the port reverts to its previous configuration. If a configuration change is made to the port while it is acting as a SPAN destination port, the change does not take effect until the SPAN destination configuration had been removed.
- If the port was in an EtherChannel group, it is removed from the group while it is a destination port. If it was a routed port, it is no longer a routed port.
- It can be any Ethernet physical port.
- It cannot be a secure port.
- It cannot be a source port.
- It can be an EtherChannel group (**ON** mode only).
- It can participate in only one SPAN session at a time (a destination port in one SPAN session cannot be a destination port for a second SPAN session).
- When it is active, incoming traffic is disabled. The port does not transmit any traffic except that required for the SPAN session. Incoming traffic is never learned or forwarded on a destination port.
- If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.
- It does not participate in any of the Layer 2 protocols (STP, VTP, CDP, DTP, PagP).
- A destination port that belongs to a source VLAN of any SPAN session is excluded from the source list and is not monitored.
- The maximum number of destination ports in a device or device stack is 64.

Local SPAN and RSPAN destination ports function differently with VLAN tagging and encapsulation:

- For local SPAN, if the **encapsulation replicate** keywords are specified for the destination port, these packets appear with the original encapsulation (untagged, ISL, or IEEE 802.1Q). If these keywords are not specified, packets appear in the untagged format. Therefore, the output of a local SPAN session with **encapsulation replicate** enabled can contain a mixture of untagged, ISL, or IEEE 802.1Q-tagged packets.
- For RSPAN, the original VLAN ID is lost because it is overwritten by the RSPAN VLAN identification. Therefore, all packets appear on the destination port as untagged.

## RSPAN VLAN

The RSPAN VLAN carries SPAN traffic between RSPAN source and destination sessions. RSPAN VLAN has these special characteristics:

- All traffic in the RSPAN VLAN is always flooded.
- No MAC address learning occurs on the RSPAN VLAN.
- RSPAN VLAN traffic only flows on trunk ports.

- RSPAN VLANs must be configured in VLAN configuration mode by using the **remote-span** VLAN configuration mode command.
- STP can run on RSPAN VLAN trunks but not on SPAN destination ports.
- An RSPAN VLAN cannot be a private-VLAN primary or secondary VLAN.

For VLANs 1 to 1005 that are visible to VLAN Trunking Protocol (VTP), the VLAN ID and its associated RSPAN characteristic are propagated by VTP. If you assign an RSPAN VLAN ID in the extended VLAN range (1006 to 4094), you must manually configure all intermediate devices.

It is normal to have multiple RSPAN VLANs in a network at the same time with each RSPAN VLAN defining a network-wide RSPAN session. That is, multiple RSPAN source sessions anywhere in the network can contribute packets to the RSPAN session. It is also possible to have multiple RSPAN destination sessions throughout the network, monitoring the same RSPAN VLAN and presenting traffic to the user. The RSPAN VLAN ID separates the sessions.

## SPAN and RSPAN Interaction with Other Features

SPAN interacts with these features:

- Routing—SPAN does not monitor routed traffic. VSPAN only monitors traffic that enters or exits the device, not traffic that is routed between VLANs. For example, if a VLAN is being Rx-monitored and the device routes traffic from another VLAN to the monitored VLAN, that traffic is not monitored and not received on the SPAN destination port.
- STP—A destination port does not participate in STP while its SPAN or RSPAN session is active. The destination port can participate in STP after the SPAN or RSPAN session is disabled. On a source port, SPAN does not affect the STP status. STP can be active on trunk ports carrying an RSPAN VLAN.
- CDP—A SPAN destination port does not participate in CDP while the SPAN session is active. After the SPAN session is disabled, the port again participates in CDP.
- VTP—You can use VTP to prune an RSPAN VLAN between devices.
- VLAN and trunking—You can modify VLAN membership or trunk settings for source or destination ports at any time. However, changes in VLAN membership or trunk settings for a destination port do not take effect until you remove the SPAN destination configuration. Changes in VLAN membership or trunk settings for a source port immediately take effect, and the respective SPAN sessions automatically adjust accordingly.
- EtherChannel—You can configure an EtherChannel group as a source port. When a group is configured as a SPAN source, the entire group is monitored.

  If a physical port is added to a monitored EtherChannel group, the new port is added to the SPAN source port list. If a port is removed from a monitored EtherChannel group, it is automatically removed from the source port list.

  A physical port that belongs to an EtherChannel group can be configured as a SPAN source port and still be a part of the EtherChannel. In this case, data from the physical port is monitored as it participates in the EtherChannel. However, if a physical port that belongs to an EtherChannel group is configured as a SPAN destination, it is removed from the group. After the port is removed from the SPAN session, it rejoins the EtherChannel group. Ports removed from an EtherChannel group remain members of the group, but they are in the inactive or suspended state.

  If a physical port that belongs to an EtherChannel group is a destination port and the EtherChannel group is a source, the port is removed from the EtherChannel group and from the list of monitored ports.

- Multicast traffic can be monitored. For egress and ingress port monitoring, only a single unedited packet is sent to the SPAN destination port. It does not reflect the number of times the multicast packet is sent.
- A private-VLAN port cannot be a SPAN destination port.
- A secure port cannot be a SPAN destination port.

  For SPAN sessions, do not enable port security on ports with monitored egress when ingress forwarding is enabled on the destination port. For RSPAN source sessions, do not enable port security on any ports with monitored egress.
- An IEEE 802.1x port can be a SPAN source port. You can enable IEEE 802.1x on a port that is a SPAN destination port; however, IEEE 802.1x is disabled until the port is removed as a SPAN destination.

  For SPAN sessions, do not enable IEEE 802.1x on ports with monitored egress when ingress forwarding is enabled on the destination port. For RSPAN source sessions, do not enable IEEE 802.1x on any ports that are egress monitored.

## SPAN and RSPAN and Device Stacks

Because the stack of switches represents one logical switch, local SPAN source ports and destination ports can be in different switches in the stack. Therefore, the addition or deletion of switches in the stack can affect a local SPAN session, as well as an RSPAN source or destination session. An active session can become inactive when a switch is removed from the stack or an inactive session can become active when a switch is added to the stack.

## Flow-Based SPAN

You can control the type of network traffic to be monitored in SPAN or RSPAN sessions by using flow-based SPAN (FSPAN) or flow-based RSPAN (FRSPAN), which apply access control lists (ACLs) to the monitored traffic on the source ports. The FSPAN ACLs can be configured to filter IPv4, IPv6, and non-IP monitored traffic.

You apply an ACL to a SPAN session through the interface. It is applied to all the traffic that is monitored on all interfaces in the SPAN session.The packets that are permitted by this ACL are copied to the SPAN destination port. No other packets are copied to the SPAN destination port.

The original traffic continues to be forwarded, and any port, VLAN, and router ACLs attached are applied. The FSPAN ACL does not have any effect on the forwarding decisions. Similarly, the port, VLAN, and router ACLs do not have any effect on the traffic monitoring. If a security input ACL denies a packet and it is not forwarded, the packet is still copied to the SPAN destination ports if the FSPAN ACL permits it. But if the security output ACL denies a packet and it is not sent, it is not copied to the SPAN destination ports. However, if the security output ACL permits the packet to go out, it is only copied to the SPAN destination ports if the FSPAN ACL permits it. This is also true for an RSPAN session.

You can attach three types of FSPAN ACLs to the SPAN session:

- IPv4 FSPAN ACL— Filters only IPv4 packets.
- IPv6 FSPAN ACL— Filters only IPv6 packets.
- MAC FSPAN ACL— Filters only non-IP packets.

If a VLAN-based FSPAN session configured on a stack cannot fit in the hardware memory on one or more devices, it is treated as unloaded on those devices, and traffic meant for the FSPAN ACL and sourcing on that device is not copied to the SPAN destination ports. The FSPAN ACL continues to be correctly applied,

and traffic is copied to the SPAN destination ports on the devices where the FSPAN ACL fits in the hardware memory.

When an empty FSPAN ACL is attached, some hardware functions copy all traffic to the SPAN destination ports for that ACL. If sufficient hardware resources are not available, even an empty FSPAN ACL can be unloaded.

## Default SPAN and RSPAN Configuration

***Table 9: Default SPAN and RSPAN Configuration***

| Feature | Default Setting |
|---|---|
| SPAN state (SPAN and RSPAN) | Disabled. |
| Source port traffic to monitor | Both received and sent traffic (**both**). |
| Encapsulation type (destination port) | Native form (untagged packets). |
| Ingress forwarding (destination port) | Disabled. |
| VLAN filtering | On a trunk interface used as a source port, all VLANs are monitored. |
| RSPAN VLANs | None configured. |

# Configuring SPAN and RSPAN

## SPAN Configuration Guidelines

- To remove a source or destination port or VLAN from the SPAN session, use the **no monitor session** *session_number* **source interface** *interface-id* {**interface** *interface-id* | **vlan** *vlan-id*} global configuration command or the **no monitor session** *session_number* **destination interface** *interface-id* global configuration command. For destination interfaces, the **encapsulation** options are ignored with the **no** form of the command.
- To monitor all VLANs on the trunk port, use the **no monitor session** *session_number* **filter** global configuration command.

## RSPAN Configuration Guidelines

- All the SPAN configuration guidelines apply to RSPAN.
- As RSPAN VLANs have special properties, you should reserve a few VLANs across your network for use as RSPAN VLANs; do not assign access ports to these VLANs.
- You can apply an output ACL to RSPAN traffic to selectively filter or monitor specific packets. Specify these ACLs on the RSPAN VLAN in the RSPAN source .

- For RSPAN configuration, you can distribute the source ports and the destination ports across multiple in your network.
- Access ports (including voice VLAN ports) on the RSPAN VLAN are put in the inactive state.
- You can configure any VLAN as an RSPAN VLAN as long as these conditions are met:
  - The same RSPAN VLAN is used for an RSPAN session in all the .
  - All participating  support RSPAN.

## FSPAN and FRSPAN Configuration Guidelines

- When at least one FSPAN ACL is attached, FSPAN is enabled.
- When you attach at least one FSPAN ACL that is not empty to a SPAN session, and you have not attached one or more of the other FSPAN ACLs (for instance, you have attached an IPv4 ACL that is not empty, and have not attached IPv6 and MAC ACLs), FSPAN blocks the traffic that would have been filtered by the unattached ACLs. Therefore, this traffic is not monitored.

# How to Configure SPAN and RSPAN

The following sections provide information on how to configure SPAN and RSPAN.

## Creating a Local SPAN Session

Follow these steps to create a SPAN session and specify the source (monitored) ports or VLANs and the destination (monitoring) ports.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **no monitor session** {*session_number* \| **all** \| **local** \| **remote**}<br>**Example:**<br>`Device(config)# no monitor session all` | Removes any existing SPAN configuration for the session.<br>• For *session_number*, the range is 1 to 66.<br>• **all**—Removes all SPAN sessions. |

| | Command or Action | Purpose |
|---|---|---|
| | | • **local**—Removes all local sessions.<br>• **remote**—Removes all remote SPAN sessions. |
| **Step 4** | **monitor session** *session_number* **source** {**interface** *interface-id* \| **vlan** *vlan-id*} [**,** \| **-**] [**both** \| **rx** \| **tx**]<br>**Example:**<br>`Device(config)# monitor session 1 source interface gigabitethernet1/0/1` | Specifies the SPAN session and the source port (monitored port).<br>• For *session_number*, the range is 1 to 66.<br>• For *interface-id*, specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). Valid port-channel numbers are 1 to 48.<br>• For *vlan-id*, specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN).<br>**Note** A single session can include multiple sources (ports or VLANs) defined in a series of commands, but you cannot combine source ports and source VLANs in one session.<br>• (Optional) [**,** \| **-**] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.<br>• (Optional) **both** \| **rx** \| **tx**—Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic.<br>  • **both**—Monitors both received and sent traffic.<br>  • **rx**—Monitors received traffic.<br>  • **tx**—Monitors sent traffic.<br>  **Note** You can use the **monitor session** *session_number* **source** command multiple times to configure multiple source ports. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** \| -] [**encapsulation {replicate \| dot1q}**]}<br>**Example:**<br>`Device(config)# monitor session 1 destination interface gigabitethernet1/0/2 encapsulation replicate` | Specifies the SPAN session and the destination port (monitoring port). The port LED changes to amber when the configuration changes take effect. The LED returns to its original state (green) only after removing the SPAN destination configuration.<br>**Note** For local SPAN, you must use the same session number for the source and destination interfaces.<br>• For *session_number*, specify the session number entered in step 4.<br>• For *interface-id*, specify the destination port.<br>The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN.<br>• (Optional) [**,** \| -] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.<br>(Optional) **encapsulation replicate** specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).<br>(Optional) **encapsulation dot1q**specifies that the destination interface accepts the source interface incoming packets with IEEE 802.1Q encapsulation.<br>**Note** You can use **monitor session** *session_number* **destination** command multiple times to configure multiple destination ports. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show running-config**<br>**Example:** | Verifies your entries. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device# show running-config` | |
| **Step 8** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Creating a Local SPAN Session and Configuring Incoming Traffic

Follow these steps to create a SPAN session, to specify the source ports or VLANs and the destination ports, and to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **no monitor session** {*session_number* \| **all** \| **local** \| **remote**}<br>**Example:**<br>`Device(config)# no monitor session all` | Removes any existing SPAN configuration for the session.<br>• For *session_number*, the range is 1 to 66.<br>• **all**—Removes all SPAN sessions.<br>• **local**—Removes all local sessions.<br>• **remote**—Removes all remote SPAN sessions. |
| **Step 4** | **monitor session** *session_number* **source** {**interface** *interface-id* \| **vlan** *vlan-id*} [**,** \| **-**] [**both** \| **rx** \| **tx**]<br>**Example:**<br>`Device(config)# monitor session 2 source gigabitethernet1/0/1 rx` | Specifies the SPAN session and the source port (monitored port). |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** \| -] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* \| **untagged vlan** *vlan-id* \| **vlan** *vlan-id*}]}<br>**Example:**<br>`Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate ingress dot1q vlan 6` | Specifies the SPAN session, the destination port, the packet encapsulation, and the ingress VLAN and encapsulation.<br>• For *session_number*, specify the session number entered in Step 4.<br>• For *interface-id*, specify the destination port.<br>The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN.<br>• (Optional) [**,** \| -]—Specifies a series or range of interfaces. Enter a space before and after the comma or hyphen.<br>• (Optional) **encapsulation replicate** specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).<br>• (Optional) **encapsulation dot1q**specifies that the destination interface accepts the source interface incoming packets with IEEE 802.1Q encapsulation.<br>• **ingress** enables forwarding of incoming traffic on the destination port and to specify the encapsulation type:<br>  • **dot1q vlan** *vlan-id*—Accepts incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.<br>  • **untagged vlan** *vlan-id* or **vlan** *vlan-id*—Accepts incoming packets with untagged encapsulation type with the specified VLAN as the default VLAN. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 8** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Specifying VLANs to Filter

Follow these steps to limit SPAN source traffic to specific VLANs.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **no monitor session** {*session_number* \| **all** \| **local** \| **remote**}<br>**Example:**<br>`Device(config)# no monitor session all` | Removes any existing SPAN configuration for the session.<br>• For *session_number*, the range is 1 to 66.<br>• **all**—Removes all SPAN sessions.<br>• **local**—Removes all local sessions.<br>• **remote**—Removes all remote SPAN sessions. |
| **Step 4** | **monitor session** *session_number* **source interface** *interface-id*<br>**Example:**<br>`Device(config)# monitor session 2 source interface gigabitethernet1/0/2 rx` | Specifies the characteristics of the source port (monitored port) and SPAN session.<br>• For *session_number*, the range is 1 to 66. |

| | Command or Action | Purpose |
|---|---|---|
| | | • For *interface-id*, specify the source port to monitor. The interface specified must already be configured as a trunk port. |
| **Step 5** | **monitor session** *session_number* **filter vlan** *vlan-id* [**,** \| **-**]<br>**Example:**<br>`Device(config)# monitor session 2 filter vlan 1 - 5 , 9` | Limits the SPAN source traffic to specific VLANs.<br>• For *session_number*, enter the session number specified in Step 4.<br>• For *vlan-id*, the range is 1 to 4094.<br>• (Optional) Use a comma (**,**) to specify a series of VLANs, or use a hyphen (-) to specify a range of VLANs. Enter a space before and after the comma; enter a space before and after the hyphen. |
| **Step 6** | **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** \| **-**] [**encapsulation replicate**]}<br>**Example:**<br>`Device(config)# monitor session 2 destination interface gigabitethernet1/0/1` | Specifies the SPAN session and the destination port (monitoring port).<br>• For *session_number*, specify the session number entered in Step 4.<br>• For *interface-id*, specify the destination port.<br>The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN.<br>• (Optional) [**,** \| **-**] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.<br>• (Optional) **encapsulation replicate** specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). |
| **Step 7** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 8** | **show running-config**<br>**Example:** | Verifies your entries. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device# show running-config` | |
| **Step 9** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring a VLAN as an RSPAN VLAN

Follow these steps to create a new VLAN, then configure it to be the RSPAN VLAN for the RSPAN session.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **vlan** *vlan-id*<br>**Example:**<br>`Device(config)# vlan 100` | Enters a VLAN ID to create a VLAN, or enters the VLAN ID of an existing VLAN, and enters VLAN configuration mode. The range is 2 to 1001 and 1006 to 4094.<br>The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 through 1005 (reserved for Token Ring and FDDI VLANs). |
| **Step 4** | **remote-span**<br>**Example:**<br>`Device(config-vlan)# remote-span` | Configures the VLAN as an RSPAN VLAN. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-vlan)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 7** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### What to do next

You must create the RSPAN VLAN in all devices that will participate in RSPAN. If the RSPAN VLAN-ID is in the normal range (lower than 1005) and VTP is enabled in the network, you can create the RSPAN VLAN in one device, and VTP propagates it to the other devices in the VTP domain. For extended-range VLANs (greater than 1005), you must configure RSPAN VLAN on both source and destination devices and any intermediate devices.

Use VTP pruning to get an efficient flow of RSPAN traffic, or manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.

To remove the remote SPAN characteristic from a VLAN and convert it back to a normal VLAN, use the **no remote-span** VLAN configuration command.

To remove a source port or VLAN from the SPAN session, use the **no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} global configuration command. To remove the RSPAN VLAN from the session, use the **no monitor session** *session_number* **destination remote vlan** *vlan-id*.

# Creating an RSPAN Source Session

Follow these steps to create and start an RSPAN source session and to specify the monitored source and the destination RSPAN VLAN.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **no monitor session** {*session_number* \| **all** \| **local** \| **remote**}<br>**Example:**<br>`Device(config)# no monitor session 1` | Removes any existing SPAN configuration for the session.<br>• For *session_number*, the range is 1 to 66.<br>• **all**—Removes all SPAN sessions.<br>• **local**—Removes all local sessions.<br>• **remote**—Removes all remote SPAN sessions. |
| **Step 4** | **monitor session** *session_number* **source** {**interface** *interface-id* \| **vlan** *vlan-id*} [**,** \| **-**] [**both** \| **rx** \| **tx**]<br>**Example:**<br>`Device(config)# monitor session 1 source interface gigabitethernet1/0/1 tx` | Specifies the RSPAN session and the source port (monitored port).<br>• For *session_number*, the range is 1 to 66.<br>• Enter a source port or source VLAN for the RSPAN session:<br>  • For *interface-id*, specifies the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). Valid port-channel numbers are 1 to 48.<br>  • For *vlan-id*, specifies the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN).<br>  A single session can include multiple sources (ports or VLANs), defined in a series of commands, but you cannot combine source ports and source VLANs in one session.<br>• (Optional) [**,** \| **-**]—Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.<br>• (Optional) **both** \| **rx** \| **tx**—Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic.<br>  • **both**—Monitors both received and sent traffic.<br>  • **rx**—Monitors received traffic. |

| | Command or Action | Purpose |
|---|---|---|
| | | • **tx**—Monitors sent traffic. |
| **Step 5** | **monitor session** *session_number* **destination remote vlan** *vlan-id*<br>**Example:**<br>`Device(config)# monitor session 1 destination remote vlan 100` | Specifies the RSPAN session, the destination RSPAN VLAN, and the destination-port group.<br>• For *session_number*, enter the number defined in Step 4.<br>• For *vlan-id*, specify the source RSPAN VLAN to monitor. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 8** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Specifying VLANs to Filter

Follow these steps to configure the RSPAN source session to limit RSPAN source traffic to specific VLANs.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **no monitor session** {*session_number* \| **all** \| **local** \| **remote**}<br>**Example:**<br>`Device(config)# no monitor session 2` | Removes any existing SPAN configuration for the session.<br>• For *session_number*, the range is 1 to 66.<br>• **all**—Removes all SPAN sessions.<br>• **local**—Removes all local sessions.<br>• **remote**—Removes all remote SPAN sessions. |
| **Step 4** | **monitor session** *session_number* **source interface** *interface-id*<br>**Example:**<br>`Device(config)# monitor session 2 source interface gigabitethernet1/0/2 rx` | Specifies the characteristics of the source port (monitored port) and SPAN session.<br>• For *session_number*, the range is 1 to 66.<br>• For *interface-id*, specify the source port to monitor. The interface specified must already be configured as a trunk port. |
| **Step 5** | **monitor session** *session_number* **filter vlan** *vlan-id* [**,** \| **-**]<br>**Example:**<br>`Device(config)# monitor session 2 filter vlan 1 - 5 , 9` | Limits the SPAN source traffic to specific VLANs.<br>• For *session_number*, enter the session number specified in step 4.<br>• For *vlan-id*, the range is 1 to 4094.<br>• (Optional) **,** \| - Use a comma (**,**) to specify a series of VLANs or use a hyphen (**-**) to specify a range of VLANs. Enter a space before and after the comma; enter a space before and after the hyphen. |
| **Step 6** | **monitor session** *session_number* **destination remote vlan** *vlan-id*<br>**Example:**<br>`Device(config)# monitor session 2 destination remote vlan 902` | Specifies the RSPAN session and the destination remote VLAN (RSPAN VLAN).<br>• For *session_number*, enter the session number specified in Step 4.<br>• For *vlan-id*, specify the RSPAN VLAN to carry the monitored traffic to the destination port. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 9** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Creating an RSPAN Destination Session

You configure an RSPAN destination session on a different device or device stack; that is, not the device or device stack on which the source session was configured.

Follow these steps to define the RSPAN VLAN on that device, to create an RSPAN destination session, and to specify the source RSPAN VLAN and the destination port.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **vlan** *vlan-id*<br>**Example:**<br>`Device(config)# vlan 901` | Specifies the VLAN ID of the RSPAN VLAN created from the source device, and enters VLAN configuration mode.<br>If both devices are participating in VTP and the RSPAN VLAN ID is from 2 to 1005, Steps 3 through 5 are not required because the RSPAN VLAN ID is propagated through the VTP network. |
| **Step 4** | **remote-span**<br>**Example:** | Identifies the VLAN as the RSPAN VLAN. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-vlan)# remote-span` | |
| **Step 5** | **exit**<br>**Example:**<br>`Device(config-vlan)# exit` | Returns to global configuration mode. |
| **Step 6** | **no monitor session** {*session_number* \| **all** \| **local** \| **remote**}<br>**Example:**<br>`Device(config)# no monitor session 1` | Removes any existing SPAN configuration for the session.<br>• For *session_number*, the range is 1 to 66.<br>• **all**—Removes all SPAN sessions.<br>• **local**—Removes all local sessions.<br>• **remote**—Removes all remote SPAN sessions. |
| **Step 7** | **monitor session** *session_number* **source remote vlan** *vlan-id*<br>**Example:**<br>`Device(config)# monitor session 1 source remote vlan 901` | Specifies the RSPAN session and the source RSPAN VLAN.<br>• For *session_number*, the range is 1 to 66.<br>• For *vlan-id*, specify the source RSPAN VLAN to monitor. |
| **Step 8** | **monitor session** *session_number* **destination interface** *interface-id*<br>**Example:**<br>`Device(config)# monitor session 1 destination interface gigabitethernet2/0/1` | Specifies the RSPAN session and the destination interface.<br>• For *session_number*, enter the number defined in Step 7.<br>In an RSPAN destination session, you must use the same session number for the source RSPAN VLAN and the destination port.<br>• For *interface-id*, specify the destination interface. The destination interface must be a physical interface.<br>• Though visible in the command-line help string, **encapsulation replicate** is not supported for RSPAN. The original VLAN ID is overwritten by the RSPAN VLAN ID, and all packets appear on the destination port as untagged. |
| **Step 9** | **end**<br>**Example:** | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# end` | |
| **Step 10** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 11** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Creating an RSPAN Destination Session and Configuring Incoming Traffic

Follow these steps to create an RSPAN destination session, to specify the source RSPAN VLAN and the destination port, and to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **no monitor session** {*session_number* \| **all** \| **local** \| **remote**}<br>**Example:**<br>`Device(config)# no monitor session 2` | Removes any existing SPAN configuration for the session.<br>• For *session_number*, the range is 1 to 66.<br>• **all**—Removes all SPAN sessions.<br>• **local**—Removes all local sessions.<br>• **remote**—Removes all remote SPAN sessions. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **monitor session** *session_number* **source remote vlan** *vlan-id*<br>**Example:**<br>`Device(config)# monitor session 2 source remote vlan 901` | Specifies the RSPAN session and the source RSPAN VLAN.<br>• For *session_number*, the range is 1 to 66.<br>• For *vlan-id*, specify the source RSPAN VLAN to monitor. |
| **Step 5** | **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** \| **-**] [**ingress** {**dot1q vlan** *vlan-id* \| **untagged vlan** *vlan-id* \| **vlan** *vlan-id*}]}<br>**Example:**<br>`Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6` | Specifies the SPAN session, the destination port, the packet encapsulation, and the incoming VLAN and encapsulation.<br>• For *session_number*, enter the number defined in Step 5.<br>In an RSPAN destination session, you must use the same session number for the source RSPAN VLAN and the destination port.<br>• For *interface-id*, specify the destination interface. The destination interface must be a physical interface.<br>• Though visible in the command-line help string, **encapsulation replicate** is not supported for RSPAN. The original VLAN ID is overwritten by the RSPAN VLAN ID, and all packets appear on the destination port as untagged.<br>• (Optional) [**,** \| **-**] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.<br>• Enter **ingress** with additional keywords to enable forwarding of incoming traffic on the destination port and to specify the encapsulation type:<br>  • **dot1q vlan** *vlan-id*—Forwards incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.<br>  • **untagged vlan** *vlan-id* or **vlan** *vlan-id*—Forwards incoming packets with untagged encapsulation type with the specified VLAN as the default VLAN. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 7** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 8** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring an FSPAN Session

Follow these steps to create a SPAN session, specify the source (monitored) ports or VLANs and the destination (monitoring) ports, and configure FSPAN for the session.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **no monitor session** {*session_number* \| **all** \| **local** \| **remote**}<br>**Example:**<br>`Device(config)# no monitor session 2` | Removes any existing SPAN configuration for the session.<br>• For *session_number*, the range is 1 to 66.<br>• **all**—Removes all SPAN sessions.<br>• **local**—Removes all local sessions.<br>• **remote**—Removes all remote SPAN sessions. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **monitor session** *session_number* **source** {**interface** *interface-id* \| **vlan** *vlan-id*} [**,** \| **-**] [**both** \| **rx** \| **tx**]<br>**Example:**<br>`Device(config)# monitor session 2 source interface gigabitethernet1/0/1` | Specifies the SPAN session and the source port (monitored port).<br>• For *session_number*, the range is 1 to 66.<br>• For *interface-id*, specifies the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). Valid port-channel numbers are 1 to 48.<br>• For *vlan-id*, specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN).<br>**Note** A single session can include multiple sources (ports or VLANs) defined in a series of commands, but you cannot combine source ports and source VLANs in one session.<br>• (Optional) [**,** \| **-**]—Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.<br>• (Optional) [**both** \| **rx** \| **tx**]—Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the SPAN monitors both sent and received traffic.<br>• **both**—Monitors both sent and received traffic. This is the default.<br>• **rx**—Monitors received traffic.<br>• **tx**—Monitors sent traffic.<br>**Note** You can use the **monitor session** *session_number* **source** command multiple times to configure multiple source ports. |
| **Step 5** | **monitor session** *session_number* **destination** {**interface** *interface-id* [**,** \| **-**] [**encapsulation replicate**]}<br>**Example:** | Specifies the SPAN session and the destination port (monitoring port).<br>• For *session_number*, specify the session number entered in Step 4. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate` | • For **destination**, specify the following parameters:<br>• For *interface-id*, specify the destination port.<br>The destination interface must be a physical port; it cannot be an EtherChannel, and it cannot be a VLAN.<br>• (Optional) [**,** \| -] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.<br>• (Optional) **encapsulation replicate** specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).<br>**Note**<br>For local SPAN, you must use the same session number for the source and destination interfaces.<br>You can use **monitor session** *session_number* **destination** command multiple times to configure multiple destination ports. |
| **Step 6** | **monitor session** *session_number* **filter** {**ip** \| **ipv6** \| **mac**} **access-group** {*access-list-number* \| *name*}<br>**Example:**<br>`Device(config)# monitor session 2 filter ipv6 access-group 4` | Specifies the SPAN session, the types of packets to filter, and the ACLs to use in an FSPAN session.<br>• For *session_number*, specify the session number entered in Step 4.<br>• For *access-list-number*, specify the ACL number that you want to use to filter traffic.<br>• For *name*, specify the ACL name that you want to use to filter traffic. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 9** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring an FRSPAN Session

Follow these steps to start an RSPAN source session, specify the monitored source and the destination RSPAN VLAN, and configure FRSPAN for the session.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **no monitor session** {*session_number* \| **all** \| **local** \| **remote**}<br>**Example:**<br>`Device(config)# no monitor session 2` | Removes any existing SPAN configuration for the session.<br>• For *session_number*, the range is 1 to 66.<br>• **all**—Removes all SPAN sessions.<br>• **local**—Removes all local sessions.<br>• **remote**—Removes all remote SPAN sessions. |
| **Step 4** | **monitor session** *session_number* **source** {**interface** *interface-id* \| **vlan** *vlan-id*} [**,** \| **-**] [**both** \| **rx** \| **tx**]<br>**Example:** | Specifies the SPAN session and the source port (monitored port).<br>• For *session_number*, the range is 1 to 66. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# monitor session 2 source interface gigabitethernet1/0/1` | • For *interface-id*, specifies the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (**port-channel** *port-channel-number*). Valid port-channel numbers are 1 to 48.<br>• For *vlan-id*, specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN).<br>**Note** A single session can include multiple sources (ports or VLANs) defined in a series of commands, but you cannot combine source ports and source VLANs in one session.<br>• (Optional) [**,** \| -]—Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.<br>• (Optional) [**both** \| **rx** \| **tx**]—Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the SPAN monitors both sent and received traffic.<br>• **both**—Monitors both sent and received traffic. This is the default.<br>• **rx**—Monitors received traffic.<br>• **tx**—Monitors sent traffic.<br>**Note** You can use the **monitor session** *session_number* **source** command multiple times to configure multiple source ports. |
| **Step 5** | **monitor session** *session_number* **destination remote vlan** *vlan-id*<br>**Example:**<br>`Device(config)# monitor session 2 destination remote vlan 5` | Specifies the RSPAN session and the destination RSPAN VLAN.<br>• For *session_number*, enter the number defined in Step 4.<br>• For *vlan-id*, specify the destination RSPAN VLAN to monitor. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **vlan** *vlan-id*<br>**Example:**<br>`Device(config)# vlan 10` | Enters the VLAN configuration mode. For *vlan-id*, specify the source RSPAN VLAN to monitor. |
| **Step 7** | **remote-span**<br>**Example:**<br>`Device(config-vlan)# remote-span` | Specifies that the VLAN you specified in Step 5 is part of the RSPAN VLAN. |
| **Step 8** | **exit**<br>**Example:**<br>`Device(config-vlan)# exit` | Returns to global configuration mode. |
| **Step 9** | **monitor session** *session_number* **filter** {**ip** \| **ipv6** \| **mac**} **access-group** {*access-list-number* \| *name*}<br>**Example:**<br>`Device(config)# monitor session 2 filter ip access-group 7` | Specifies the RSPAN session, the types of packets to filter, and the ACLs to use in an FRSPAN session.<br>• For *session_number*, specify the session number entered in Step 4.<br>• For *access-list-number*, specify the ACL number that you want to use to filter traffic.<br>• For *name*, specify the ACL name that you want to use to filter traffic. |
| **Step 10** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 11** | **show running-config**<br>**Example:**<br>`Device# show running-config` | Verifies your entries. |
| **Step 12** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Monitoring SPAN and RSPAN Operations

The following table describes the command used to display SPAN and RSPAN operations configuration and results to monitor operations:

*Table 10: Monitoring SPAN and RSPAN Operations*

| Command | Purpose |
|---|---|
| **show monitor** | Displays the current SPAN configuration. |

# Configuration Examples for SPAN and RSPAN

The following sections provide configuration examples for SPAN and RSPAN

## Example: Configuring Local SPAN

This example shows how to set up SPAN session 1 for monitoring source port traffic to a destination port. First, any existing SPAN configuration for session 1 is deleted, and then bidirectional traffic is mirrored from source Gigabit Ethernet port 1 to destination Gigabit Ethernet port 2, retaining the encapsulation method.

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
encapsulation replicate
Device(config)# end
```

This example shows how to remove port 1 as a SPAN source for SPAN session 1:

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1 source interface gigabitethernet1/0/1
Device(config)# end
```

This example shows how to disable received traffic monitoring on port 1, which was configured for bidirectional monitoring:

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1 source interface gigabitethernet1/0/1 rx
```

The monitoring of traffic received on port 1 is disabled, but traffic sent from this port continues to be monitored.

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on all ports belonging to VLANs 1 through 3, and send it to destination Gigabit Ethernet port 2. The configuration is then modified to also monitor all traffic on all ports belonging to VLAN 10.

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source vlan 1 - 3 rx

Device(config)# monitor session 2 destination interface gigabitethernet1/0/2
Device(config)# monitor session 2 source vlan 10
Device(config)# end
```

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor received traffic on Gigabit Ethernet source port 1, and send it to destination Gigabit Ethernet port 2 with the same egress encapsulation type as the source port, and to enable ingress forwarding with VLAN 6 as the default ingress VLAN:

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source gigabitethernet0/1 rx
Device(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
replicate ingress vlan 6
Device(config)# end
```

This example shows how to remove any existing configuration on SPAN session 2, configure SPAN session 2 to monitor traffic received on Gigabit Ethernet trunk port 2, and send traffic for only VLANs 1 through 5 and VLAN 9 to destination Gigabit Ethernet port 1:

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Device(config)# monitor session 2 filter vlan 1 - 5 , 9
Device(config)# monitor session 2 destination interface gigabitethernet1/0/1
Device(config)# end
```

# Examples: Creating an RSPAN VLAN

This example shows how to create the RSPAN VLAN 901:

```
Device> enable
Device# configure terminal
Device(config)# vlan 901
Device(config-vlan)# remote span
Device(config-vlan)# end
```

This example shows how to remove any existing RSPAN configuration for session 1, configure RSPAN session 1 to monitor multiple source interfaces, and configure the destination as RSPAN VLAN 901:

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
Device(config)# monitor session 1 source interface gigabitethernet1/0/2 rx
Device(config)# monitor session 1 source interface port-channel 2
Device(config)# monitor session 1 destination remote vlan 901
Device(config)# end
```

This example shows how to remove any existing configuration on RSPAN session 2, configure RSPAN session 2 to monitor traffic received on trunk port 2, and send traffic for only VLANs 1 through 5 and 9 to destination RSPAN VLAN 902:

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Device(config)# monitor session 2 filter vlan 1 - 5 , 9
Device(config)# monitor session 2 destination remote vlan 902
Device(config)# end
```

This example shows how to configure VLAN 901 as the source remote VLAN and port 1 as the destination interface:

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 source remote vlan 901
Device(config)# monitor session 1 destination interface gigabitethernet2/0/1
Device(config)# end
```

This example shows how to configure VLAN 901 as the source remote VLAN in RSPAN session 2, to configure Gigabit Ethernet source port 2 as the destination interface, and to enable forwarding of incoming traffic on the interface with VLAN 6 as the default receiving VLAN:

```
Device> enable
Device# configure terminal
Device(config)# monitor session 2 source remote vlan 901
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6
Device(config)# end
```

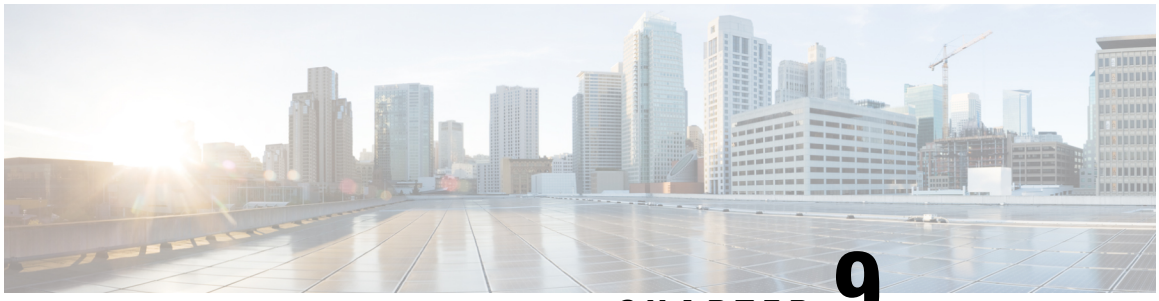
# Feature History for SPAN and RSPAN

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless notedotherwise.

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Fuji 16.9.2 | Switch Port Analyzer (SPAN) | Switch Port Analyzer allows monitoring of device traffic on a port or VLAN using a sniffer/analyzer or RMON probe. |
| | Flow-based Switch Port Analyzer (SPAN) | Flow-based SPAN provides a method to capture only required data between end hosts by using specified filters. The filters are defined in terms of access lists that limit IPv4, IPv6 or IPv4 + IPv6, or non-IP traffic (MAC) between specified source and destination addresses. |
| | Switch Port Analyzer (SPAN) - distributed egress SPAN | The feature provides distributed egress SPAN functionality onto line cards in conjunction with ingress SPAN already been distributed to line cards. By distributing egress SPAN functionalities onto line cards, the performance of the system is improved. |

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.



CHAPTER 9

# Configuring Packet Capture


- Prerequisites for Configuring Packet Capture, on page 131
- Restrictions for Configuring Embedded Packet Capture, on page 131
- Information About Packet Capture, on page 132
- How to Implement Embedded Packet Capture, on page 133
- Configuration Examples for Embedded Packet Capture, on page 136
- Feature History for Packet Capture, on page 138


# Prerequisites for Configuring Packet Capture

Packet capture is supported on Cisco Catalyst 9200 Series Switches

The following section provides information about the prerequisites for configuring packet capture.

## Prerequisites for Configuring Embedded Packet Capture

The Embedded Packet Capture (EPC) software subsystem consumes CPU and memory resources during its operation. You must have adequate system resources for different types of operations. The following table provides some guidelines for using the system resources.

***Table 11: System Requirements for the EPC Subsystem***

| System Resources | Requirements |
|---|---|
| Hardware | CPU utilization requirements are platform-dependent. |
| Memory | The DRAM stores the packet buffer. The size of the packet buffer is user specified. |
| Disk space | Packets can be exported to external devices. No intermediate storage on flash disk is required. |

# Restrictions for Configuring Embedded Packet Capture

- Layer 2 EtherChannels aren't supported.

- You can't use VRFs, management ports, and private VLANs as attachment points.
- Embedded Packet Capture (EPC) isn't supported on logical ports, which includes port channels, switch virtual interfaces (SVIs), and subinterfaces. It's supported only on physical ports.
- A VLAN interface that is in shutdown state doesn't support EPC.
- If you change interface from switch port to routed port (Layer 2 to Layer 3) or the opposite way, you must delete the capture point and create a new one, once the interface comes back up. Stop/start the capture point won't work.
- Packets captured in the output direction of an interface might not reflect the changes made by the device rewrite. This includes TTL, VLAN tag, CoS, checksum, MAC addresses, DSCP, precedent, UP, etc.
- Even though the minimum configurable duration for packet capture is 1 second, packet capture works for a minimum of 2 seconds.
- It's not possible to modify a capture point parameter when a capture is already active or has started.
- EPC captures multicast packets only on ingress and doesn't capture the replicated packets on egress.
- The Rewrite information of both ingress and egress packets aren't captured.
- CPU-injected packets are considered control plane packets. Therefore, these types of packets won't be captured on an interface egress capture.
- Control plane packets aren't rate limited and performance impacting. Use filters to limit control plane packet capture.
- DNA Advantage supports decoding of protocols such as Control and Provisioning of Wireless Access Points (CAPWAP).
- You can define up to eight capture points, but only one can be active at a time. Stop one before you can start the other.
- MAC filter won't capture IP packets even if it matches the MAC address. This applies to all interfaces (Layer 2 switch port, Layer 3 routed port).
- MAC ACL is only used for non-IP packets such as ARP. It won't be supported on a Layer 3 port or SVI.
- MAC filter can't capture Layer 2 packets (ARP) on Layer 3 interfaces.
- VACL doesn't support IPv6-based ACLs.
- EPC cannot capture based on the underlying routing protocols in MPLS packets.

# Information About Packet Capture

The Packet Capture feature is an onboard packet capture facility that allows network administrators to capture packets flowing to, through, and from the device. You can analyze them locally or save and export them for offline analysis by using Embedded Packet Capture (EPC). This feature simplifies network operations by allowing devices to become active participants in the management and operation of the network. This feature facilitates troubleshooting by gathering information about the packet format. This feature also facilitates application analysis and security.

# About Embedded Packet Capture

EPC provides an embedded systems management facility that helps in tracing and troubleshooting packets. This feature allows network administrators to capture data packets flowing through, to, and from a Cisco device. The network administrator may define the capture buffer size and type (circular, or linear) and the maximum number of bytes of each packet to capture. You can throttle the packet capture rate using further administrative controls. For example, You can filter the packets using an Access Control List. You can further define the controls by specifying a maximum packet capture rate or by specifying a sampling interval.

Prior to Cisco IOS XE Amsterdam 17.2.1 , EPC isn't supported on an interface in shutdown state. Starting from Cisco IOS XE Amsterdam 17.2.1 , EPC is supported on an interface in shutdown state. This is useful in capturing packets on an interface as it's being brought up.

## Benefits of Embedded Packet Capture

- Ability to capture IPv4 and IPv6 packets in the device, and also capture non-IP packets with MAC filter or match any MAC address.
- Extensible infrastructure for enabling packet capture points. A capture point is a traffic transit point where a packet is captured and associated with a buffer.
- Facility to export the packet capture in packet capture file (PCAP) format suitable for analysis using any external tool.
- Methods to decode data packets captured with varying degrees of detail.

## Packet Data Capture

Packet data capture is the capture of data packets that are then stored in a buffer. You can define packet data captures by providing unique names and parameters.

You can perform the following actions on the capture:

- Activate captures at any interface.
- Apply access control lists (ACLs) or class maps to capture points.

**Note** Network Based Application Recognition (NBAR) and MAC-style class map is not supported.

- Destroy captures.
- Specify buffer storage parameters such as size and type. The size ranges from 1 MB to 100 MB. The default option for the buffer is linear and the other option for the buffer is circular.
- Specify match criteria that includes information about the protocol, IP address or port address.

# How to Implement Embedded Packet Capture

The following sections provide information on how to implement EPC.

# Managing Packet Data Capture

To manage Packet Data Capture in the buffer mode, perform the following steps:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password if prompted. |
| **Step 2** | **monitor capture** *capture-name* **access-list** *access-list-name*<br>**Example:**<br>`Device# monitor capture mycap access-list v4acl` | Configures a monitor capture specifying an access list as the core filter for the packet capture. |
| **Step 3** | **monitor capture** *capture-name* **limit duration** *seconds*<br>**Example:**<br>`Device# monitor capture mycap limit duration 1000` | Configures monitor capture limits. |
| **Step 4** | **monitor capture** *capture-name* **interface** *interface-name* **both**<br>**Example:**<br>`Device# monitor capture mycap interface GigabitEthernet 0/0/1 both` | Configures monitor capture specifying an attachment point and the packet flow direction. |
| **Step 5** | **monitor capture** *capture-name* **buffer circular size** *bytes*<br>**Example:**<br>`Device# monitor capture mycap buffer circular size 10` | Configures a buffer to capture packet data. |
| **Step 6** | **monitor capture** *capture-name* **start**<br>**Example:**<br>`Device# monitor capture mycap start` | Starts the capture of packet data at a traffic trace point into a buffer. |
| **Step 7** | **monitor capture** *capture-name* **stop**<br>**Example:**<br>`Device# monitor capture mycap stop` | Stops the capture of packet data at a traffic trace point. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **monitor capture** *capture-name* **export** *file--location/file-name*<br>**Example:**<br>`Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap` | Exports captured data for analysis. |
| **Step 9** | **end**<br>**Example:**<br>`Device# end` | Returns to privileged EXEC mode. |

# Monitoring and Maintaining Captured Data

Perform this task to monitor and maintain the packet data captured. Capture buffer details and capture point details are displayed.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password if prompted. |
| **Step 2** | **show monitor capture** *capture-buffer-name* **buffer dump**<br>**Example:**<br>`Device# show monitor capture mycap buffer dump` | (Optional) Displays a hexadecimal dump of captured packet and its metadata. |
| **Step 3** | **show monitor capture** *capture-buffer-name* **parameter**<br>**Example:**<br>`Device# show monitor capture mycap parameter` | (Optional) Displays a list of commands that were used to specify the capture. |
| **Step 4** | **debug epc capture-point**<br>**Example:**<br>`Device# debug epc capture-point` | (Optional) Enables packet capture point debugging. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **debug epc provision**<br>**Example:**<br>`Device# debug epc provision` | (Optional) Enables packet capture provisioning debugging. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |

# Configuration Examples for Embedded Packet Capture

## Example: Managing Packet Data Capture

The following example shows how to manage packet data capture:

```
Device> enable
Device# monitor capture mycap access-list v4acl
Device# monitor capture mycap limit duration 1000
Device# monitor capture mycap interface GigabitEthernet 0/0/1 both
Device# monitor capture mycap buffer circular size 10
Device# monitor capture mycap start
Device# monitor capture mycap stop
Device# monitor capture mycap export tftp://10.1.88.9/mycap.pcap
Device# end
```

## Example: Monitoring and Maintaining Captured Data

The following example shows how to dump packets in ASCII format:

```
Device# show monitor capture mycap buffer dump
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

0
0000: 01005E00 00020000 0C07AC1D 080045C0 ..^...........E.
0010: 00300000 00000111 CFDC091D 0002E000 .0..............
0020: 000207C1 07C1001C 802A0000 10030AFA .........*......
0030: 1D006369 73636F00 0000091D 0001 ..example.......
1
0000: 01005E00 0002001B 2BF69280 080046C0 ..^.....+.....F.
0010: 00200000 00000102 44170000 0000E000 . ......D.......
0020: 00019404 00001700 E8FF0000 0000 ..............
2
0000: 01005E00 0002001B 2BF68680 080045C0 ..^.....+.....E.
0010: 00300000 00000111 CFDB091D 0003E000 .0..............
0020: 000207C1 07C1001C 88B50000 08030A6E ...............n
0030: 1D006369 73636F00 0000091D 0001 ..example.......
3
0000: 01005E00 000A001C 0F2EDC00 080045C0 ..^...........E.
0010: 003C0000 00000258 CE7F091D 0004E000 .<.....X........
0020: 000A0205 F3000000 00000000 00000000 ................
```

```
0030: 00000000 00D10001 000C0100 01000000 ................
0040: 000F0004 00080501 0300
```

The following example shows how to display the list of commands used to configure the capture named mycap:

```
Device# show monitor capture mycap parameter
monitor capture mycap interface GigabitEthernet 1/0/1 both
monitor capture mycap match any
monitor capture mycap buffer size 10
monitor capture mycap limit pps 1000
```

The following example shows how to debug the capture point:

```
Device# debug epc capture-point
EPC capture point operations debugging is on

Device# monitor capture mycap start
*Jun 4 14:17:15.463: EPC CP: Starting the capture cap1
*Jun 4 14:17:15.463: EPC CP: (brief=3, detailed=4, dump=5) = 0
*Jun 4 14:17:15.463: EPC CP: final check before activation
*Jun 4 14:17:15.463: EPC CP: setting up c3pl infra
*Jun 4 14:17:15.463: EPC CP: Setup c3pl acl-class-policy
*Jun 4 14:17:15.463: EPC CP: Creating a class
*Jun 4 14:17:15.464: EPC CP: Creating a class : Successful
*Jun 4 14:17:15.464: EPC CP: class-map Created
*Jun 4 14:17:15.464: EPC CP: creating policy-name epc_policy_cap1
*Jun 4 14:17:15.464: EPC CP: Creating Policy epc_policy_cap1 of type 49 and client type 21
*Jun 4 14:17:15.464: EPC CP: Storing a Policy
*Jun 4 14:17:15.464: EPC CP: calling ppm_store_policy with epc_policy
*Jun 4 14:17:15.464: EPC CP: Creating Policy : Successful
*Jun 4 14:17:15.464: EPC CP: policy-map created
*Jun 4 14:17:15.464: EPC CP: creating filter for ANY
*Jun 4 14:17:15.464: EPC CP: Adding acl to class : Successful
*Jun 4 14:17:15.464: EPC CP: Setup c3pl class to policy
*Jun 4 14:17:15.464: EPC CP: Attaching Class to Policy
*Jun 4 14:17:15.464: EPC CP: Attaching epc_class_cap1 to epc_policy_cap1
*Jun 4 14:17:15.464: EPC CP: Attaching Class to Policy : Successful
*Jun 4 14:17:15.464: EPC CP: setting up c3pl qos
*Jun 4 14:17:15.464: EPC CP: DBG> Set packet rate limit to 1000
*Jun 4 14:17:15.464: EPC CP: creating action for policy_map epc_policy_cap1 class_map
epc_class_cap1
*Jun 4 14:17:15.464: EPC CP: DBG> Set packet rate limit to 1000
*Jun 4 14:17:15.464: EPC CP: Activating Interface GigabitEthernet1/0/1 direction both
*Jun 4 14:17:15.464: EPC CP: Id attached 0
*Jun 4 14:17:15.464: EPC CP: inserting into active lists
*Jun 4 14:17:15.464: EPC CP: Id attached 0
*Jun 4 14:17:15.465: EPC CP: inserting into active lists
*Jun 4 14:17:15.465: EPC CP: Activating Vlan
*Jun 4 14:17:15.465: EPC CP: Deleting all temp interfaces
*Jun 4 14:17:15.465: %BUFCAP-6-ENABLE: Capture Point cap1 enabled.
*Jun 4 14:17:15.465: EPC CP: Active Capture 1

Device# monitor capture mycap1 stop
*Jun 4 14:17:31.963: EPC CP: Stopping the capture cap1
*Jun 4 14:17:31.963: EPC CP: Warning: unable to unbind capture cap1
*Jun 4 14:17:31.963: EPC CP: Deactivating policy-map
*Jun 4 14:17:31.963: EPC CP: Policy epc_policy_cap1
*Jun 4 14:17:31.964: EPC CP: Deactivating policy-map Successful
*Jun 4 14:17:31.964: EPC CP: removing povision feature
*Jun 4 14:17:31.964: EPC CP: Found action for policy-map epc_policy_cap1 class-map
epc_class_cap1
*Jun 4 14:17:31.964: EPC CP: cleanning up c3pl infra
*Jun 4 14:17:31.964: EPC CP: Removing Class epc_class_cap1 from Policy
*Jun 4 14:17:31.964: EPC CP: Removing Class from epc_policy_cap1
```

```
*Jun 4 14:17:31.964: EPC CP: Successfully removed
*Jun 4 14:17:31.964: EPC CP: Removing acl mac from class
*Jun 4 14:17:31.964: EPC CP: Removing acl from class : Successful
*Jun 4 14:17:31.964: EPC CP: Removing all policies
*Jun 4 14:17:31.964: EPC CP: Removing Policy epc_policy_cap1
*Jun 4 14:17:31.964: EPC CP: Removing Policy : Successful
*Jun 4 14:17:31.964: EPC CP: Removing class epc_class_cap1
*Jun 4 14:17:31.965: EPC CP: Removing class : Successful
*Jun 4 14:17:31.965: %BUFCAP-6-DISABLE: Capture Point cap1 disabled.
*Jun 4 14:17:31.965: EPC CP: Active Capture 0
```

The following example shows how to debug the Embedded Packet Capture (EPC) provisioning:

```
Device# debug epc provision
EPC provisionioning debugging is on

Device# monitor capture mycap start
*Jun 4 14:17:54.991: EPC PROV: No action found for policy-map epc_policy_cap1 class-map
epc_class_cap1
*Jun 4 14:17:54.991: EPC PROV:
*Jun 4 14:17:54.991: Attempting to install service policy epc_policy_cap1
*Jun 4 14:17:54.992: EPC PROV: Attached service policy to epc idb subblock
*Jun 4 14:17:54.992: EPC PROV: Successful. Create feature object
*Jun 4 14:17:54.992: EPC PROV:
*Jun 4 14:17:54.992: Attempting to install service policy epc_policy_cap1
*Jun 4 14:17:54.992: EPC PROV: Successful. Create feature object
*Jun 4 14:17:54.992: %BUFCAP-6-ENABLE: Capture Point cap1 enabled.

Device# monitor capture mycap stop
*Jun 4 14:18:02.503: EPC PROV: Successful. Remove feature object
*Jun 4 14:18:02.504: EPC PROV: Successful. Remove feature object
*Jun 4 14:18:02.504: EPC PROV: Destroyed epc idb subblock
*Jun 4 14:18:02.504: EPC PROV: Found action for policy-map epc_policy_cap1 class-map
epc_class_cap1
*Jun 4 14:18:02.504: EPC PROV: Deleting EPC action
*Jun 4 14:18:02.504: EPC PROV: Successful. CLASS_REMOVE, policy-map epc_policy_cap1, class
 epc_class_cap1
*Jun 4 14:18:02.504: %BUFCAP-6-DISABLE: Capture Point cap1 disabled.
```

# Feature History for Packet Capture

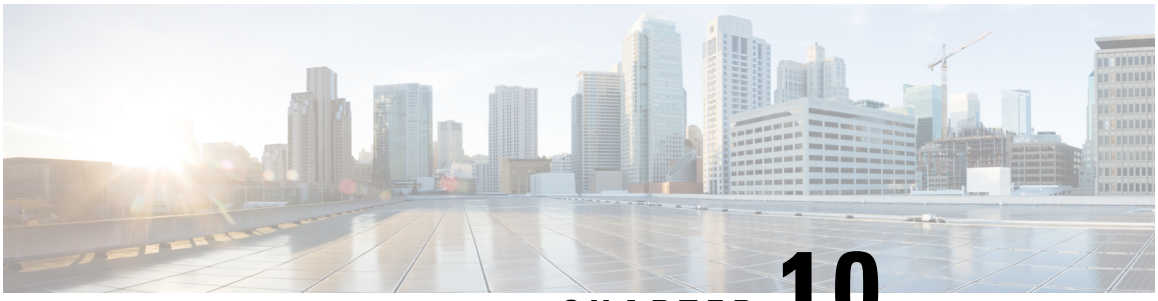
This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless notedotherwise.

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Fuji 16.9.2 | Packet Capture | The Packet Capture feature is an onboard packet capture facility that allows network administrators to capture packets flowing to, through, and from the device. |

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Amsterdam 17.2.1 | Embedded Packet Capture (EPC) on an interface either in down state or admin state. | This feature allows you to configure Embedded Packet Capture (EPC) on an interface that is either in down state or admin down state. This does not affect packet capture once the interface changes to up state. |

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.



CHAPTER 10

# Configuring Flexible NetFlow


- Prerequisites for Flexible NetFlow, on page 141
- Restrictions for Flexible NetFlow, on page 142
- Information About Flexible Netflow, on page 144
- How to Configure Flexible Netflow, on page 158
- Monitoring Flexible NetFlow, on page 169
- Configuration Examples for Flexible NetFlow, on page 169
- Feature History for Flexible NetFlow, on page 173


## Prerequisites for Flexible NetFlow

- You are familiar with the Flexible NetFlow key fields as they are defined in the following commands:
  - **match flow**
  - **match interface**
  - **match** {**ipv4** | **ipv6**}
  - **match routing**
  - **match transport**
- You are familiar with the Flexible NetFlow nonkey fields as they are defined in the following commands:
  - **collect counter**
  - **collect flow**
  - **collect interface**
  - **collect**{**ipv4** | **ipv6**}
  - **collect routing**
  - **collect timestamp sys-uptime**
  - **collect transport**
- The networking device must be running a Cisco release that supports Flexible NetFlow.

### IPv4 Traffic

- The networking device must be configured for IPv4 routing.
- One of the following must be enabled on your device and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding or distributed Cisco Express Forwarding.

### IPv6 Traffic

- The networking device must be configured for IPv6 routing.
- One of the following must be enabled on your device and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding IPv6 or distributed Cisco Express Forwarding.

# Restrictions for Flexible NetFlow

The following are restrictions for Flexible NetFlow:

- Flexible NetFlow is not supported on the Layer 2 port-channel interface, but is supported on the Layer 2 port-channel member ports.
- Flexible NetFlow is supported on the Layer 3 port-channel interfaces and member ports but not on both at the same time for the same traffic type and direction.
- Multiple Flexible Netflow configurations are supported either on port-channel interface or port-channel member ports but not on both.
- Traditional NetFlow accounting is not supported.
- Flexible NetFlow Version 9 and Version 10 export formats are supported. However, if you have not configured the export protocol, Version 9 export format is applied by default.
- Flexible NetFlow and NBAR cannot be configured together at the same time on the same interface.
- Layer 2, IPv4, and IPv6 traffic types are supported. Multiple flow monitors of different traffic types can be applied for a given interface and direction. Multiple flow monitors of same traffic type cannot be applied for a given interface and direction.
- Layer 2, VLAN, Layer 3 and SVI interfaces are supported, but the device does not support tunnels.
- Depending on the switch type, a switch will have one or two forwarding ASICs. The capacities listed in the above table are on a per-Core/per-ASIC basis.
- The switch has a single core ASIC and the total flows supported is 16K flows (8K per ingress and egress directions). The TCAM limit is 128 entries per direction.
- The NetFlow tables are on separate compartments and cannot be combined. Depending on which core processed the packet, the flows will be created in the table in the corresponding core.
- NetFlow hardware implementation supports four hardware samplers. You can select a sampler rate from 1 out of 2 to 1 out of 1024. Both — random and deterministic — sampling modes are supported.
- NetFlow hardware uses hash tables internally. Hash collisions can occur in the hardware. Therefore, in spite of the internal overflow Content Addressable Memory (CAM), the actual NetFlow table utilization could be about 80 percent.

- Depending on the fields that are used for the flow, a single flow could take two consecutive entries. IPv6 and datalink flows also take two entries. In these situations, the effective usage of NetFlow entries is half the table size, which is separate from the above hash collision limitation.
- The device supports up to 15 flow monitors.
- The NetFlow software implementation supports distributed NetFlow export, so the flows are exported from the same device in which the flow was created.
- Ingress flows are present in the ASIC that first received the packets for the flow. Egress flows are present in the ASIC from which the packets actually left the device set up.
- The reported value for the bytes count field (called “bytes long”) is Layer-2-packet-size—18 bytes. For classic Ethernet traffic (802.3), this will be accurate. For all other Ethernet types, this field will not be accurate. Use the "bytes layer2” field, which always reports the accurate Layer 2 packet size. For information about supported Flexible NetFlow fields, see 'Supported Flexible NetFlow Fields' topic.
- Configuration of IPFIX exporter on an AVC flow monitor is not supported.
- Flexible NetFlow export is not supported on the Ethernet management port, GigabitEthernet 0/0.
- When a flow record has only Source Group Tag (SGT) and Destination Group Tag (DGT) fields (or only either of the two) and if both the values are not applicable, then a flow will still be created with zero values for SGT and DGT. The flow records are expected to include source and destination IP addresses, along with SGT and DGT fields.
- On non-Cisco TrustSec interfaces, an SGT value of zero implies that there is no command header. On Cisco TrustSec interfaces, an SGT value of zero implies an unknown tag.
- When a quality of service (QoS) marked packet is received on an interface which has NetFlow configured in the ingress direction, the QoS value of the packet is captured by the NetFlow collector. However, when the packet is received on an interface which has NetFlow configured in the egress direction and the QoS value has been rewritten on ingress by the switch, the new QoS value of the packet is not captured by the collector.
- For an IPv6 flow monitor, Source Group Tag (SGT) and Destination Group Tag (DGT) fields cannot co-exist with MAC address fields.
- NetFlow records do not support MultiProtocol Label Switching-enabled (MPLS-enabled) interfaces.
- A flow monitor cannot be shared across Layer 3 physical interfaces and logical interfaces (such as, Layer 3 port-channel interface, Layer 3 port-channel member, and switch virtual interface [SVI]), but a flow monitor can be shared across logical interfaces or Layer 3 physical interfaces.
- When Flexible NetFlow and Network Address Translation (NAT) are configured on an interface,
    - Flexible NetFlow will display and export the actual flow details; but not the translated flow details. Application-level gateway (ALG) flow details are not part of the actual flow details that are exported.
    - If the ALG traffic gets translated through the CPU, Flexible NetFlow will display and export the translated flow details for the ALG traffic.
- When configuring a flow record if you include the **match application name** field, the corresponding flow monitor will not support a flow sampler.

# Information About Flexible Netflow

The following sections provide information about Flexible Netflow.

## Flexible Netflow Overview

Flexible NetFlow uses flows to provide statistics for accounting, network monitoring, and network planning.

A flow is a unidirectional stream of packets that arrives on a source interface and has the same values for the keys. A key is an identified value for a field within the packet. You create a flow using a flow record to define the unique keys for your flow.

The device supports the Flexible NetFlow feature that enables enhanced network anomalies and security detection. Flexible NetFlow allows you to define an optimal flow record for a particular application by selecting the keys from a large collection of predefined fields.

All key values must match for the packet to count in a given flow. A flow might gather other fields of interest, depending on the export record version that you configure. Flows are stored in the Flexible NetFlow cache.

You can export the data that Flexible NetFlow gathers for your flow by using an exporter and export this data to a remote system such as a Flexible NetFlow collector. The Flexible NetFlow collector can use an IPv4 address.

You define the size of the data that you want to collect for a flow using a monitor. The monitor combines the flow record and exporter with the Flexible NetFlow cache information.

Starting with the Cisco IOS XE 16.12.1 release, Source Group Tag (SGT) and Destination Group Tag (DGT) fields over Flexible NetFlow are supported for IPv6 traffic.

## Original NetFlow and Benefits of Flexible NetFlow

Flexible NetFlow allows the flow to be user defined. The benefits of Flexible NetFlow include:

- High-capacity flow recognition, including scalability and aggregation of flow information.
- Enhanced flow infrastructure for security monitoring and dDoS detection and identification.
- New information from packets to adapt flow information to a particular service or operation in the network. The flow information available will be customizable by Flexible NetFlow users.
- Extensive use of Cisco’s flexible and extensible NetFlow Version 9.
- A comprehensive IP accounting feature that can be used to replace many accounting features, such as IP accounting, Border Gateway Protocol (BGP) Policy Accounting, and persistent caches.

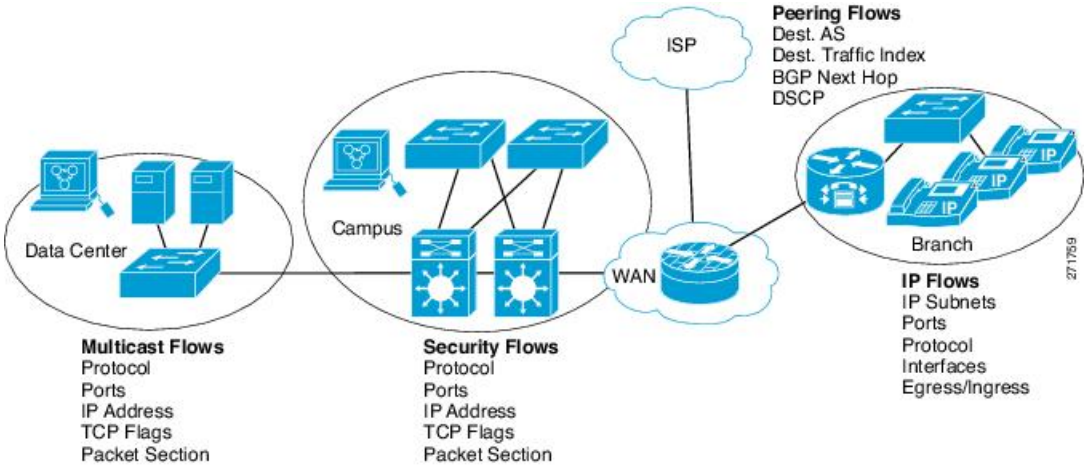
Flexible NetFlow allows you to understand network behavior with more efficiency, with specific flow information tailored for various services used in the network. The following are some example applications for a Flexible NetFlow feature:

- Flexible NetFlow enhances Cisco NetFlow as a security monitoring tool. For instance, new flow keys can be defined for packet length or MAC address, allowing users to search for a specific type of attack in the network.

- Flexible NetFlow allows you to quickly identify how much application traffic is being sent between hosts by specifically tracking TCP or UDP applications by the class of service (CoS) in the packets.
- The accounting of traffic entering a Multiprotocol Label Switching (MPLS) or IP core network and its destination for each next hop per class of service. This capability allows the building of an edge-to-edge traffic matrix.

The figure below is an example of how Flexible NetFlow might be deployed in a network.

***Figure 9: Typical Deployment for Flexible NetFlow***




# Flexible NetFlow Components

Flexible NetFlow consists of components that can be used together in several variations to perform traffic analysis and data export. The user-defined flow records and the component structure of Flexible NetFlow facilitates the creation of various configurations for traffic analysis and data export on a networking device with a minimum number of configuration commands. Each flow monitor can have a unique combination of flow record, flow exporter, and cache type. If you change a parameter such as the destination IP address for a flow exporter, it is automatically changed for all the flow monitors that use the flow exporter. The same flow monitor can be used in conjunction with different flow samplers to sample the same type of network traffic at different rates on different interfaces. The following sections provide more information on Flexible NetFlow components:

## Flow Records

In Flexible NetFlow a combination of key and nonkey fields is called a record. Flexible NetFlow records are assigned to Flexible NetFlow flow monitors to define the cache that is used for storing flow data. Flexible NetFlow includes several predefined records that can help you get started using Flexible NetFlow.

A flow record defines the keys that Flexible NetFlow uses to identify packets in the flow, as well as other fields of interest that Flexible NetFlow gathers for the flow. You can define a flow record with any combination of keys and fields of interest. The device supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 64-bit packet or byte counters. The device enables the following match fields as the defaults when you create a flow record:

- **match datalink**—Layer 2 attributes

- **match flow direction**—Specifies a match to the fields identifying the direction of flow.
- **match interface**—Interface attributes
- **match ipv4**—IPv4 attributes
- **match ipv6**—IPv6 attributes
- **match transport**—Transport layer fields
- **match flow cts**—Cisco TrustSec fields

### NetFlow Predefined Records

Flexible NetFlow includes several predefined records that you can use to start monitoring traffic in your network. The predefined records are available to help you quickly deploy Flexible NetFlow and are easier to use than user-defined flow records. You can choose from a list of already defined records that may meet the needs for network monitoring. As Flexible NetFlow evolves, popular user-defined flow records will be made available as predefined records to make them easier to implement.

**Note** Predefined records are not supported for regular Flexible NetFlow on Cisco Catalyst 9000 Series Switches.

### User-Defined Records

Flexible NetFlow enables you to define your own records for a Flexible NetFlow flow monitor cache by specifying the key and nonkey fields to customize the data collection to your specific requirements. When you define your own records for a Flexible NetFlow flow monitor cache, they are referred to as *user-defined records*. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow. Flexible NetFlow enables you to capture counter values such as the number of bytes and packets in a flow as nonkey fields.

You can create user-defined records for applications such as QoS and bandwidth monitoring, application and end user traffic profiling, and security monitoring for dDoS attacks. Flexible NetFlow user-defined records provide the capability to monitor a contiguous section of a packet of a user-configurable size, and use it in a flow record as a key or a nonkey field along with other fields and attributes of the packet. The section may include any Layer 3 data from the packet. The ability to analyze packet fields, enables more detailed traffic monitoring, facilitates the investigation of dDoS attacks, and enables implementation of other security applications such as URL monitoring.

The *bytes* values are the sizes in bytes of these fields in the flow record. If the corresponding fragment of the packet is smaller than the requested section size, Flexible NetFlow will fill the rest of the section field in the flow record with zeros. If the packet type does not match the requested section type, Flexible NetFlow will fill the entire section field in the flow record with zeros.

Flexible NetFlow adds a new Version 9 export format field type for the header and packet section types. Flexible NetFlow will communicate to the NetFlow collector the configured section sizes in the corresponding Version 9 export template fields. The payload sections will have a corresponding length field that can be used to collect the actual size of the collected section.

## Flexible NetFlow Match Parameters

The following table describes Flexible NetFlow match parameters. You must configure at least one of the following match parameters for the flow records.

*Table 12: Match Parameters*

| Command | Purpose |
|---|---|
| **match datalink** {**dot1q** \| **ethertype** \| **mac** \| **vlan** } | Specifies a match to datalink or Layer 2 fields. The following command options are available:<br>• **dot1q**—Matches to the dot1q field.<br>• **ethertype**—Matches to the ethertype of the packet.<br>• **mac**—Matches the source or destination MAC fields.<br>• **vlan**—Matches to the VLAN that the packet is located on (input or output). |
| **match flow direction** | Specifies a match to the flow identifying fields. |
| **match interface** {**input** \| **output**} | Specifies a match to the interface fields. The following command options are available:<br>• **input**—Matches to the input interface.<br>• **output**—Matches to the output interface. |
| **match ipv4** {**destination** \| **protocol** \| **source** \| **tos** \| **ttl** \| **version**} | Specifies a match to the IPv4 fields. The following command options are available:<br>• **destination**—Matches to the IPv4 destination address-based fields.<br>• **protocol**—Matches to the IPv4 protocols.<br>• **source**—Matches to the IPv4 source address based fields.<br>• **tos**—Matches to the IPv4 Type of Service fields.<br>• **ttl**—Matches to the IPv4 Time To Live fields.<br>• **version**—Matches to the IP version from the IPv4 header. |

| Command | Purpose |
|---|---|
| **match ipv6** {**destination** \| **hop-limit** \| **protocol** \| **source** \| **traffic-class** \| **version** } | Specifies a match to the IPv6 fields. The following command options are available:<br>• **destination**—Matches to the IPv6 destination address-based fields.<br>• **hop-limit**—Matches to the IPv6 hop limit fields.<br>• **protocol**—Matches to the IPv6 payload protocol fields.<br>• **source**—Matches to the IPv6 source address based fields.<br>• **traffic-class**—Matches to the IPv6 traffic class.<br>• **version**—Matches to the IP version from the IPv6 header. |
| **match transport** {**destination-port** \| **igmp** \| **icmp** \| **source-port**} | Specifies a match to the Transport Layer fields. The following command options are available:<br>• **destination-port**—Matches to the transport destination port.<br>• **icmp**—Matches to ICMP fields, including ICMP IPv4 and IPv6 fields.<br>• **igmp**—Matches to IGMP fields.<br>• **source-port**—Matches to the transport source port. |

## Flexible NetFlow Collect Parameters

The following table describes the Flexible NetFlow collect parameters.

*Table 13: Collect Parameters*

| Command | Purpose |
|---|---|
| **collect counter** { **bytes** { **layer2** { **long** } \| **long** } \| **packets** { **long** } } | Collects the counter fields total bytes and total packets. |
| **collect interface** {**input** \| **output**} | Collects the fields from the input or output interface. |
| **collect timestamp absolute** {**first** \| **last**} | Collects the fields for the absolute time the first packet was seen or the absolute time the most recent packet was last seen (in milliseconds). |

| Command | Purpose |
|---|---|
| **collect transport** | • **packets**—packet fields<br>• **rcp**—RCP fields<br>• **tcp**—TCP fields |
| **collect transport tcp flags** | Collects the following transport TCP flags:<br>• **ack**—TCP acknowledgement flag<br>• **cwr**—TCP congestion window reduced flag<br>• **ece**—TCP ECN echo flag<br>• **fin**—TCP finish flag<br>• **psh**—TCP push flag<br>• **rst**—TCP reset flag<br>• **syn**—TCP synchronize flag<br>• **urg**—TCP urgent flag<br>**Note**<br>On the device, you cannot specify which TCP flag to collect. You can only specify to collect transport TCP flags. All TCP flags will be collected with this command. |
| **collect flow** {**sampler** \|**username**} | Collects the following flow values:<br>• **sampler**— Configures a flow sampler ID as a non-key field for the record. This field contains the ID of the flow sampler used to monitor the flow.<br>• **username**— Configures the username associated with the flow. |
| **collect ipv4** {**source**\|**destination**} | Collects the following IPv4 fields:<br>• **source**— Configures the IPv4 source as a non-key field for a flow record.<br>• **destination**— Configures the IPv4 destination as a non-key field for a flow record. |
| **collect ipv6** {**source**\|**destination**} | Collects the following IPv6 information:<br>• **source**— Configures the IPv6 source as a non-key field for a flow record.<br>• **destination**— Configures the IPv6 destination as a non-key field for a flow record. |

| Command | Purpose |
|---|---|
| **collect routing**{ **next-hop address** \|**destination**\|**source**\|**forwarding-status**\|**multicast** | Collects the following routing values:<br>• **next-hop address**— Information regarding the next hop from the flows.<br>• **destination**— Destination routing attributes.<br>• **source**— Source routing attributes.<br>• **forwarding status**— Forwarding status of the packet.<br>• **multicast**— Multicast routing attributes. |
| **collect policy firewall event** | Configures the collect policy firewall event as a non-key field and enables collecting information on SGACL denied or permitted traffic based on the traffic pattern. |

## Flow Exporters

Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.

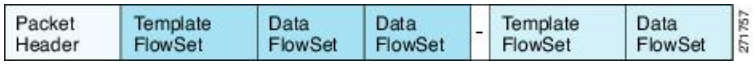
### NetFlow Data Export Format Version 9

The basic output of NetFlow is a flow record. Several different formats for flow records have evolved as NetFlow has matured. The most recent evolution of the NetFlow export format is known as Version 9. The distinguishing feature of the NetFlow Version 9 export format is that it is template-based. Templates provide an extensible design to the record format, a feature that should allow future enhancements to NetFlow services without requiring concurrent changes to the basic flow-record format. Using templates provides several key benefits:

- Third-party business partners who produce applications that provide collector or display services for NetFlow do not have to recompile their applications each time a new NetFlow feature is added. Instead, they should be able to use an external data file that documents the known template formats.
- New features can be added to NetFlow quickly without breaking current implementations.
- NetFlow is “future-proofed” against new or developing protocols because the Version 9 format can be adapted to provide support for them.

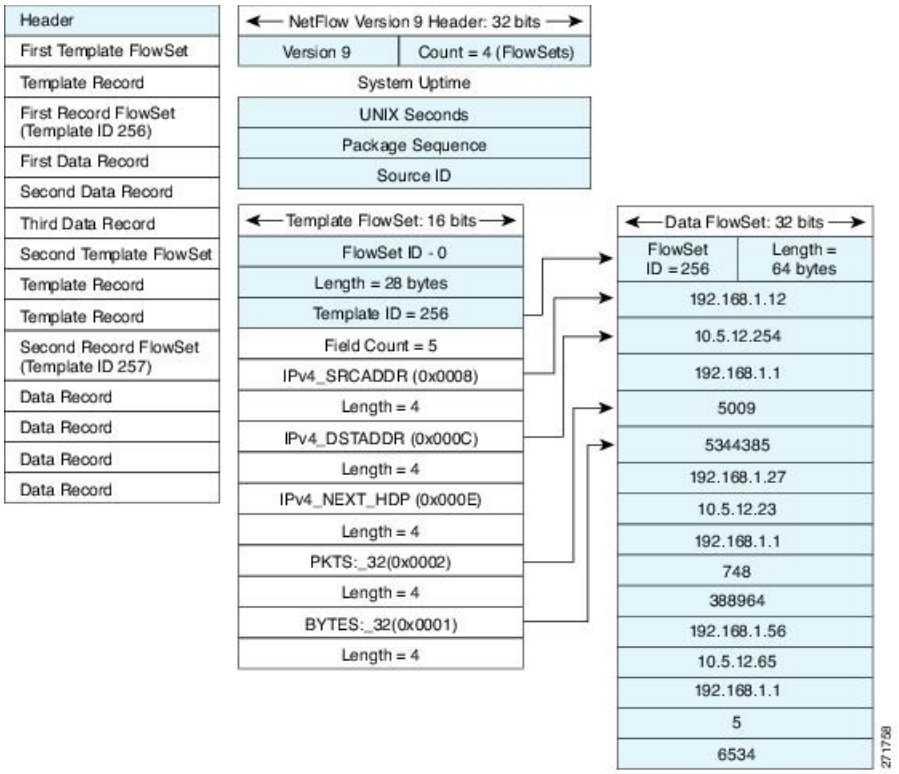
The Version 9 export format consists of a packet header followed by one or more template flow or data flow sets. A template flow set provides a description of the fields that will be present in future data flow sets. These data flow sets may occur later within the same export packet or in subsequent export packets. Template flow and data flow sets can be intermingled within a single export packet, as illustrated in the figure below.

*Figure 10: Version 9 Export Packet*




NetFlow Version 9 will periodically export the template data so the NetFlow collector will understand what data is to be sent and also export the data flow set for the template. The key advantage to Flexible NetFlow is that the user configures a flow record, which is effectively converted to a Version 9 template and then forwarded to the collector. The figure below is a detailed example of the NetFlow Version 9 export format, including the header, template flow, and data flow sets.

*Figure 11: Detailed Example of the NetFlow Version 9 Export Format*




For more information on the Version 9 export format, refer to the white paper titled Cisco IOS NetFlow Version 9 Flow-Record Format, available at this URL: http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper09186a00800a3db9.shtml.

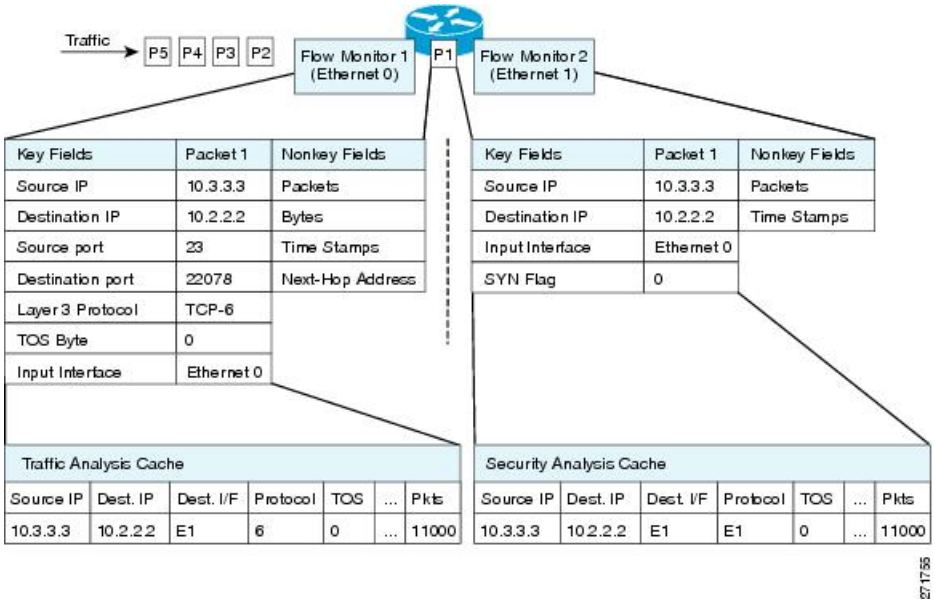
## Flow Monitors

Flow monitors are the Flexible NetFlow component that is applied to interfaces to perform network traffic monitoring.

Flow data is collected from the network traffic and added to the flow monitor cache during the monitoring process based on the key and nonkey fields in the flow record.

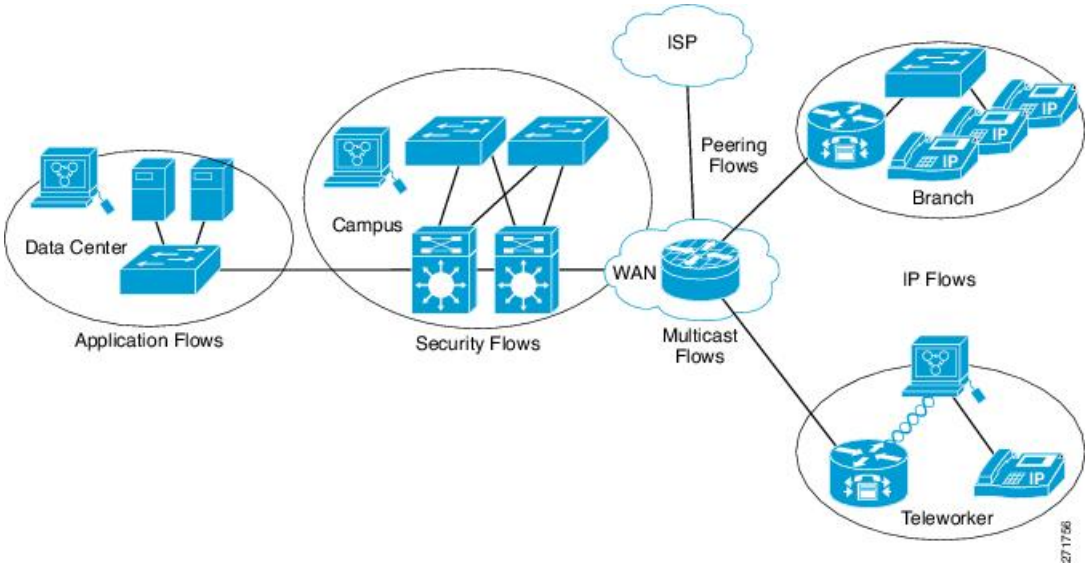
Flexible NetFlow can be used to perform different types of analysis on the same traffic. In the figure below, packet 1 is analyzed using a record designed for standard traffic analysis on the input interface and a record designed for security analysis on the output interface.

*Figure 12: Example of Using Two Flow Monitors to Analyze the Same Traffic*




The figure below shows a more complex example of how you can apply different types of flow monitors with custom records.

*Figure 13: Complex Example of Using Multiple Types of Flow Monitors with Custom Records*




## Normal

The default cache type is “normal”. In this mode, the entries in the cache are aged out according to the timeout active and timeout inactive settings. When a cache entry is aged out, it is removed from the cache and exported via any exporters configured.

## Flow Samplers

Flow samplers are created as separate components in a router's configuration. Flow samplers are used to reduce the load on the device that is running Flexible NetFlow by limiting the number of packets that are selected for analysis.

Flow sampling exchanges monitoring accuracy for router performance. When you apply a sampler to a flow monitor, the overhead load on the router of running the flow monitor is reduced because the number of packets that the flow monitor must analyze is reduced. The reduction in the number of packets that are analyzed by the flow monitor causes a corresponding reduction in the accuracy of the information stored in the flow monitor's cache.

Samplers are combined with flow monitors when they are applied to an interface with the **ip flow monitor** command.

# Supported Flexible NetFlow Fields

The following tables provide a consolidated list of supported fields in Flexible NetFlow (FNF) for various traffic types and traffic direction.

**Note** If the packet has a VLAN field, then that length is not accounted for.

| Field | Layer 2 In | Layer 2 Out | IPv4 In | IP v4 Out | IPv6 In | IPv6 Out | Notes |
|---|---|---|---|---|---|---|---|
| **Key or Collect Fields** | | | | | | | |
| Interface input | Yes | — | Yes | — | Yes | — | If you apply a flow monitor in the input direction:<br>• Use the **match** keyword and use the input interface as a key field.<br>• Use the **collect** keyword and use the output interface as a collect field. This field will be present in the exported records but with a value of 0. |

| Field | Layer 2 In | Layer 2 Out | IPv4 In | IP v4 Out | IPv6 In | IPv6 Out | Notes |
|---|---|---|---|---|---|---|---|
| Interface output | — | Yes | — | Yes | — | Yes | If you apply a flow monitor in the output direction:<br>• Use the **match** keyword and use the output interface as a key field.<br>• Use the **collect** keyword and use the input interface as a collect field. This field will be present in the exported records but with a value of 0. |

| Field | Layer 2 In | Layer 2 Out | IPv4 In | IP v4 Out | IPv6 In | IPv6 Out | Notes |
|---|---|---|---|---|---|---|---|
| **Key Fields** | | | | | | | |
| Flow direction | Yes | Yes | Yes | Yes | Yes | Yes | |
| Ethertype | Yes | Yes | — | — | — | — | |
| VLAN input | Yes | — | Yes | — | Yes | — | Supported only for a switch port. |
| VLAN output | — | Yes | — | Yes | — | Yes | Supported only for a switch port. |
| dot1q VLAN input | Yes | — | Yes | — | Yes | — | Supported only for a switch port. |
| dot1q VLAN output | — | Yes | — | Yes | — | Yes | Supported only for a switch port. |
| dot1q priority | Yes | Yes | Yes | Yes | Yes | Yes | Supported only for a switch port. |
| MAC source address input | Yes | Yes | Yes | Yes | Yes | Yes | |

| Field | Layer 2 In | Layer 2 Out | IPv4 In | IP v4 Out | IPv6 In | IPv6 Out | Notes |
|---|---|---|---|---|---|---|---|
| MAC source address output | — | — | — | — | — | — | |
| MAC destination address input | Yes | — | Yes | — | Yes | — | |
| MAC destination address output | — | Yes | — | Yes | — | Yes | |
| IPv4 version | — | — | Yes | Yes | Yes | Yes | |
| IPv4 TOS | — | — | Yes | Yes | Yes | Yes | |
| IPv4 protocol | — | — | Yes | Yes | Yes | Yes | Must use if any of src/dest port, ICMP code/type, IGMP type or TCP flags are used. |
| IPv4 TTL | — | — | Yes | Yes | Yes | Yes | |
| IPv4 TTL | — | — | Yes | Yes | Yes | Yes | Same as IPv4 TTL. |
| IPv4 protocol | — | — | Yes | Yes | Yes | Yes | Same as IPv4 protocol. Must use if any of src/dest port, ICMP code/type, IGMP type or TCP flags are used. |
| IPv4 source address | — | — | Yes | Yes | — | — | |

| Field | Layer 2 In | Layer 2 Out | IPv4 In | IP v4 Out | IPv6 In | IPv6 Out | Notes |
|---|---|---|---|---|---|---|---|
| IPv4 destination address | — | — | Yes | Yes | — | — | |
| ICMP IPv4 type | — | — | Yes | Yes | — | — | |
| ICMP IPv4 code | — | — | Yes | Yes | — | — | |
| IGMP type | — | — | Yes | Yes | — | — | |

| Field | Layer 2 In | Layer 2 Out | IPv4 In | IP v4 Out | IPv6 In | IPv6 Out | Notes |
|---|---|---|---|---|---|---|---|
| **Key Fields continued** | | | | | | | |
| IPv6 version | — | — | Yes | Yes | Yes | Yes | Same as IP version. |
| IPv6 protocol | — | — | Yes | Yes | Yes | Yes | Same as IP protocol. Must use if any of src/dest port, ICMP code/type, IGMP type or TCP flags are used. |
| IPv6 source address | — | — | — | — | Yes | Yes | |
| IPv6 destination address | — | — | — | — | Yes | Yes | |
| IPv6 traffic-class | — | — | Yes | Yes | Yes | Yes | Same as IP TOS. |
| IPv6 hop-limit | — | — | Yes | Yes | Yes | Yes | Same as IP TTL. |
| ICMP IPv6 type | — | — | — | — | Yes | Yes | |
| ICMP IPv6 code | — | — | — | — | Yes | Yes | |
| source-port | — | — | Yes | Yes | Yes | Yes | |

| Field | Layer 2 In | Layer 2 Out | IPv4 In | IP v4 Out | IPv6 In | IPv6 Out | Notes |
|---|---|---|---|---|---|---|---|
| dest-port | — | — | Yes | Yes | Yes | Yes | |

| Field | Layer 2 In | Layer 2 Out | IPv4 In | IP v4 Out | IPv6 In | IPv6 Out | Notes |
|---|---|---|---|---|---|---|---|
| **Collect Fields** | | | | | | | |
| Bytes long | Yes | Yes | Yes | Yes | Yes | Yes | Packet size = (Ethernet frame size including FCS - 18 bytes)<br>**Recommended:**<br>Avoid this field and use Bytes layer2 long. |
| Packets long | Yes | Yes | Yes | Yes | Yes | Yes | |
| Timestamp absolute first | Yes | Yes | Yes | Yes | Yes | Yes | |
| Timestamp absolute last | Yes | Yes | Yes | Yes | Yes | Yes | |
| TCP flags | Yes | Yes | Yes | Yes | Yes | Yes | Collects all flags. |
| Bytes layer2 long | Yes | Yes | Yes | Yes | Yes | Yes | |

# Default Settings

The following table lists the Flexible NetFlow default settings for the device.

***Table 14: Default Flexible NetFlow Settings***

| Setting | Default |
|---|---|
| Flow active timeout | 1800 seconds |
| Flow timeout inactive | 15 seconds |

## Flexible NetFlow—Ingress VRF Support Overview

The Flexible NetFlow—Ingress VRF Support feature enables collecting the virtual routing and forwarding (VRF) ID from incoming packets on a device by applying an input flow monitor having a flow record that collects the VRF ID as a key field.

## Flexible Netflow—Egress VRF Support Overview

The Flexible Netflow—Egress VRF Support feature enables collecting the VRF ID from outgoing packets on a device by applying an output flow monitor having a flow record that collects the VRF ID as a key field.

# How to Configure Flexible Netflow

To configure Flexible Netflow, follow these general steps:

1. Create a flow record by specifying keys and non-key fields to the flow.
2. Create an optional flow exporter by specifying the protocol and transport destination port, destination, and other parameters.
3. Create a flow monitor based on the flow record and flow exporter.
4. Create an optional sampler.
5. Apply the flow monitor to a Layer 2 port, Layer 3 port, or VLAN.

## Creating a Flow Record

Perform this task to configure a customized flow record.

Customized flow records are used to analyze traffic data for a specific purpose. A customized flow record must have at least one **match** criterion for use as the key field and typically has at least one **collect** criterion for use as a nonkey field.

There are hundreds of possible permutations of customized flow records. This task shows the steps that are used to create one of the possible permutations. Modify the steps in this task as appropriate to create a customized flow record for your requirements.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:** | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device# configure terminal` | |
| **Step 3** | **flow record** *record-name*<br>**Example:**<br>`Device(config)# flow record FLOW-RECORD-1` | Creates a flow record and enters Flexible NetFlow flow record configuration mode.<br>• This command also allows you to modify an existing flow record. |
| **Step 4** | **description** *description*<br>**Example:**<br>`Device(config-flow-record)# description Used for basic traffic analysis` | (Optional) Creates a description for the flow record. |
| **Step 5** | **match** {**ip** \| **ipv6**} {**destination** \| **source**} **address**<br>**Example:**<br>`Device(config-flow-record)# match ipv4 destination address` | **Note**<br>This example configures the IPv4 destination address as a key field for the record. |
| **Step 6** | Repeat Step 5 as required to configure additional key fields for the record. | — |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-flow-record)# end` | Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode. |
| **Step 8** | **show flow record** *record-name*<br>**Example:**<br>`Device# show flow record FLOW_RECORD-1` | (Optional) Displays the current status of the specified flow record. |
| **Step 9** | **show running-config flow record** *record-name*<br>**Example:**<br>`Device# show running-config flow record FLOW_RECORD-1` | (Optional) Displays the configuration of the specified flow record. |

# Creating a Flow Exporter

You can create a flow export to define the export parameters for a flow.

**Note** Each flow exporter supports only one destination. If you want to export the data to multiple destinations, you must configure multiple flow exporters and assign them to the flow monitor.

You can export to a destination using IPv4 address.

## Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device(config)# configure terminal` | Enters global configuration mode. |
| **Step 3** | **flow exporter** *name*<br>**Example:**<br>`Device(config)# flow exporter ExportTest` | Creates a flow exporter and enters flow exporter configuration mode. |
| **Step 4** | **description** *string*<br>**Example:**<br>`Device(config-flow-exporter)# description ExportV9` | (Optional) Describes this flow record as a maximum 63-character string. |
| **Step 5** | **destination** {*ipv4-address*}<br>**Example:**<br>`Device(config-flow-exporter)# destination 192.0.2.1 (IPv4 destination)` | Sets the IPv4 destination address or hostname for this exporter. |
| **Step 6** | **dscp** *value*<br>**Example:**<br>`Device(config-flow-exporter)# dscp 0` | (Optional) Specifies the differentiated services codepoint value. The range is from 0 to 63. The default is 0. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **source** *interface type interface number*<br>**Example:**<br>`Device(config-flow-exporter)# source gigabitEthernet1/0/1` | (Optional) Specifies the interface to use to reach the NetFlow collector at the configured destination.<br>**Note** Flow Exporter does not support unnumbered IP interface as source interface.<br>The following interfaces can be configured as source:<br>• **Auto Template**—Auto-Template interface<br>• **Capwap**—CAPWAP tunnel interface<br>• **GigabitEthernet**—Gigabit Ethernet IEEE 802<br>• **GroupVI**—Group virtual interface<br>• **Internal Interface**—Internal interface<br>• **Loopback**—Loopback interface<br>• **Null**—Null interface<br>• **Port-channel**—Ethernet Channel of interface<br>• **TenGigabitEthernet**—10-Gigabit Ethernet<br>• **Tunnel**—Tunnel interface<br>• **Vlan**—Catalyst VLANs |
| **Step 8** | **transport udp** *number*<br>**Example:**<br>`Device(config-flow-exporter)# transport udp 200` | (Optional) Specifies the UDP port to use to reach the NetFlow collector. |
| **Step 9** | **ttl** *seconds*<br>**Example:**<br>`Device(config-flow-exporter)# ttl 210` | (Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. The range is from 1 to 255 seconds. The default is 255. |
| **Step 10** | **export-protocol** {**netflow-v9**}<br>**Example:**<br>`Device(config-flow-exporter)# export-protocol netflow-v9` | Specifies the version of the NetFlow export protocol used by the exporter. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 11** | **end**<br>**Example:**<br>`Device(config-flow-record)# end` | Returns to privileged EXEC mode. |
| **Step 12** | **show flow exporter** [**name** *record-name*]<br>**Example:**<br>`Device# show flow exporter ExportTest` | (Optional) Displays information about NetFlow flow exporters. |
| **Step 13** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

### What to do next

Define a flow monitor based on the flow record and flow exporter.

# Creating a Customized Flow Monitor

Perform this required task to create a customized flow monitor.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. These record formats can be one of the predefined formats or a user-defined format. An advanced user can create a customized format using the **flow record** command.

### Before you begin

If you want to use a customized record instead of using one of the Flexible NetFlow predefined records, you must create the customized record before you can perform this task. If you want to add a flow exporter to the flow monitor for data export, you must create the exporter before you can complete this task.

**Note** You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command on the flow monitor.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:** | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device> enable` | |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **flow monitor** *monitor-name*<br>**Example:**<br>`Device(config)# flow monitor FLOW-MONITOR-1` | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode.<br>• This command also allows you to modify an existing flow monitor. |
| **Step 4** | **description** *description*<br>**Example:**<br>`Device(config-flow-monitor)# description Used for basic ipv4 traffic analysis` | (Optional) Creates a description for the flow monitor. |
| **Step 5** | **record** {*record-name* \| **netflow-original** \| **netflow** {**ipv4** \| **ipv6**} *record* [**peer**]}<br>**Example:**<br>`Device(config-flow-monitor)# record FLOW-RECORD-1` | Specifies the record for the flow monitor. |
| **Step 6** | **cache** {**timeout** {**active** \| **inactive** \| **update**} *seconds* \| **type normal** }<br>**Example:**<br>`Device(config-flow-monitor)# cache type normal`<br>`Device(config-flow-monitor)# cache timeout active` | (Optional) Modifies the flow monitor cache parameters such as timeout values, and the cache type. Associates a flow cache with the specified flow monitor. |
| **Step 7** | Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor. | — |
| **Step 8** | **statistics packet protocol**<br>**Example:**<br>`Device(config-flow-monitor)# statistics packet protocol` | (Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors. |
| **Step 9** | **statistics packet size**<br>**Example:**<br>`Device(config-flow-monitor)# statistics packet size` | (Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | **exporter** *exporter-name*<br>**Example:**<br>`Device(config-flow-monitor)# exporter EXPORTER-1` | (Optional) Specifies the name of an exporter that was created previously. |
| **Step 11** | **end**<br>**Example:**<br>`Device(config-flow-monitor)# end` | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |
| **Step 12** | **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** \| **record** \| **table**} ]] [**statistics**]]<br>**Example:**<br>`Device# show flow monitor FLOW-MONITOR-2 cache` | (Optional) Displays the status and statistics for a Flexible NetFlow flow monitor. |
| **Step 13** | **show running-config flow monitor** *monitor-name*<br>**Example:**<br>`Device# show running-config flow monitor FLOW_MONITOR-1` | (Optional) Displays the configuration of the specified flow monitor. |
| **Step 14** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Creating a Flow Sampler

Perform this required task to configure and enable a flow sampler.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **sampler** *sampler-name*<br>**Example:**<br>`Device(config)# sampler SAMPLER-1` | Creates a sampler and enters sampler configuration mode.<br>• This command also allows you to modify an existing sampler. |
| **Step 4** | **description** *description*<br>**Example:**<br>`Device(config-sampler)# description Sample at 50%` | (Optional) Creates a description for the flow sampler. |
| **Step 5** | **mode** {**random**} **1 out-of** *window-size*<br>**Example:**<br>`Device(config-sampler)# mode random 1 out-of 2` | Specifies the sampler mode and the flow sampler window size.<br>• The range for the *window-size* argument is from 0 to 1024. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-sampler)# exit` | Exits sampler configuration mode and returns to global configuration mode. |
| **Step 7** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface GigabitEthernet 0/0/0` | Specifies an interface and enters interface configuration mode. |
| **Step 8** | {**ip** \| **ipv6**} **flow monitor** *monitor-name* [[**sampler**] *sampler-name*] {**input** \| **output**}<br>**Example:**<br>`Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input` | Assigns the flow monitor and the flow sampler that you created to the interface to enable sampling. |
| **Step 9** | **end**<br>**Example:**<br>`Device(config-if)# end` | Exits interface configuration mode and returns to privileged EXEC mode. |
| **Step 10** | **show sampler sampler-name**<br>**Example:** | Displays the status and statistics of the flow sampler that you configured and enabled. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device# show sampler SAMPLER-1` | |

# Applying a Flow to an Interface

You can apply a flow monitor and an optional sampler to an interface.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device(config)# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type*<br>**Example:**<br>`Device(config)# interface GigabitEthernet1/0/1` | Enters interface configuration mode and configures an interface.<br>Flexible NetFlow is not supported on the L2 port-channel interface, but is supported on the L2 port-channel member ports.<br>Flexible NetFlow is supported on the L3 port-channel interfaces and member ports but not on both at the same time. |
| **Step 4** | {**ip flow monitor** \| **ipv6 flow monitor** \| **datalink flow monitor**} *name* [**sampler** *name*] {**input** \| **output**}<br>**Example:**<br>`Device(config-if)# ip flow monitor MonitorTest input` | Associates an IPv4, IPv6 and datalink flow monitor, and an optional sampler to the interface for input or output packets.<br>**ip flow monitor** – Enables Flexible NetFlow to monitor IPv4 traffic.<br>**ipv6 flow monitor** – Enables Flexible NetFlow to monitor IPv6 traffic.<br>**datalink flow monitor** – Enables Flexible NetFlow to monitor non-IP traffic. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-flow-monitor)# end` | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **show flow interface** [*interface-type number*]<br>**Example:**<br>`Device# show flow interface` | (Optional) Displays information about NetFlow on an interface. |
| **Step 7** | **copy running-config startup-config**<br>**Example:**<br>`Device# copy running-config startup-config` | (Optional) Saves your entries in the configuration file. |

# Configuring a Bridged NetFlow on a VLAN

You can apply a flow monitor and an optional sampler to a VLAN.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device(config)# configure terminal` | Enters global configuration mode. |
| **Step 3** | **vlan** [**configuration**] *vlan-id*<br>**Example:**<br>`Device(config)# vlan configuration 30`<br>`Device(config-vlan-config)#` | Enters VLAN or VLAN configuration mode. |
| **Step 4** | **ip flow monitor** *monitor name* [**sampler** *sampler name*] {**input** } <br>**Example:**<br>`Device(config-vlan-config)# ip flow monitor MonitorTest input` | Associates a flow monitor and an optional sampler to the VLAN for input packets. |
| **Step 5** | **copy running-config startup-config**<br>**Example:** | (Optional) Saves your entries in the configuration file. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device# copy running-config startup-config` | |

# Configuring Layer 2 NetFlow

You can define Layer 2 keys in Flexible NetFlow records that you can use to capture flows in Layer 2 interfaces.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device(config)# configure terminal` | Enters global configuration mode. |
| **Step 3** | **flow record** *name*<br>**Example:**<br>`Device(config)# flow record L2_record`<br>`Device(config-flow-record)#` | Enters flow record configuration mode. |
| **Step 4** | **match datalink** {**dot1q** \|**ethertype** \| **mac** \| **vlan**}<br>**Example:**<br>`Device(config-flow-record)# match datalink ethertype` | Specifies the Layer 2 attribute as a key. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-flow-record)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **show flow record** [*name* ]<br>**Example:**<br>`Device# show flow record` | (Optional) Displays information about NetFlow on an interface. |
| **Step 7** | **copy running-config startup-config**<br>**Example:** | (Optional) Saves your entries in the configuration file. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device# copy running-config startup-config` | |

# Monitoring Flexible NetFlow

The commands in the following table can be used to monitor Flexible NetFlow.

*Table 15: Flexible NetFlow Monitoring Commands*

| Command | Purpose |
|---|---|
| **show flow exporter** [**broker** \| **export-ids** \| **name** \| *name* \| **statistics** \| **templates**] | Displays information about NetFlow flow exporters and statistics. |
| **show flow exporter** [ **name** *exporter-name*] | Displays information about NetFlow flow exporters and statistics. |
| **show flow interface** | Displays information about NetFlow interfaces. |
| **show flow monitor** [ **name** *exporter-name*] | Displays information about NetFlow flow monitors and statistics. |
| **show flow monitor statistics** | Displays the statistics for the flow monitor |
| **show flow monitor cache format** {**table** \| **record** \| **csv**} | Displays the contents of the cache for the flow monitor, in the format specified. |
| **show flow record** [ **name** *record-name*] | Displays information about NetFlow flow records. |
| **show sampler** [**broker** \| **name** \| *name*] | Displays information about NetFlow samplers. |

# Configuration Examples for Flexible NetFlow

## Example: Configuring a Flow

This example shows how to create a flow and apply it to an interface:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Device(config)# flow export export1
Device(config-flow-exporter)# destination 10.0.101.254
Device(config-flow-exporter)# transport udp 2055
Device(config-flow-exporter)# exit
Device(config)# flow record record1
Device(config-flow-record)# match ipv4 source address
```

```
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port

Device(config-flow-record)# collect counter byte long
Device(config-flow-record)# collect counter packet long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# exit
Device(config)# flow monitor monitor1
Device(config-flow-monitor)# record record1
Device(config-flow-monitor)# exporter export1
Device(config-flow-monitor)# exit
Device(config)# interface tenGigabitEthernet 1/0/1
Device(config-if)# ip flow monitor monitor1 input
Device(config-if)# end
```

# Example: Monitoring IPv4 ingress traffic

This example shows how to monitor IPv4 ingress traffic (int g1/0/11 sends traffic to int g1/0/36 and int g3/0/11).

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# flow record  fr-1
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match interface input
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# collect counter bytes layer2 long
Device(config-flow-record)# exit

Device(config)# flow exporter fe-ipfix6
Device(config-flow-exporter)# destination 2001:0:0:24::10
Device(config-flow-exporter)# source Vlan106
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-ipfix
Device(config-flow-exporter)# description IPFIX format collector 100.0.0.80
Device(config-flow-exporter)# destination 100.0.0.80
Device(config-flow-exporter)# dscp 30
Device(config-flow-exporter)# ttl 210
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-1
Device(config-flow-exporter)# destination 10.5.120.16
Device(config-flow-exporter)# source Vlan105
Device(config-flow-exporter)# dscp 32
```

```
Device(config-flow-exporter)# ttl 200
Device(config-flow-exporter)# transport udp 2055

Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow monitor fm-1
Device(config-flow-monitor)# exporter fe-ipfix6
Device(config-flow-monitor)# exporter fe-ipfix
Device(config-flow-monitor)# exporter fe-1
Device(config-flow-monitor)# cache timeout inactive 60
Device(config-flow-monitor)#  cache timeout active 180
Device(config-flow-monitor)# record fr-1
Device(config-flow-monitor)# end

Device# show running-config interface g1/0/11
Device# show running-config interface g1/0/36
Device# show running-config interface g3/0/11
Device# show flow monitor fm-1 cache format table
```

# Example: Monitoring IPv4 egress traffic

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# flow record  fr-1 out
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match interface output
Device(config-flow-record)# collect counter bytes long
Device(config-flow-record)# collect counter packets long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# exit

Device(config)# flow exporter fe-1
Device(config-flow-exporter)# destination 10.5.120.16
Device(config-flow-exporter)# source Vlan105
Device(config-flow-exporter)# dscp 32
Device(config-flow-exporter)# ttl 200
Device(config-flow-exporter)# transport udp 2055
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-ipfix6
Device(config-flow-exporter)# destination 2001:0:0:24::10
Device(config-flow-exporter)# source Vlan106
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow exporter fe-ipfix
Device(config-flow-exporter)# description IPFIX format collector 100.0.0.80
Device(config-flow-exporter)# destination 100.0.0.80
Device(config-flow-exporter)# dscp 30
Device(config-flow-exporter)# ttl 210
Device(config-flow-exporter)# transport udp 4739
Device(config-flow-exporter)# export-protocol ipfix
```

```
Device(config-flow-exporter)# template data timeout 240
Device(config-flow-exporter)# exit

Device(config)# flow monitor fm-1-output
Device(config-flow-monitor)# exporter fe-1
Device(config-flow-monitor)# exporter fe-ipfix6
Device(config-flow-monitor)# exporter fe-ipfix
Device(config-flow-monitor)# cache timeout inactive 50
Device(config-flow-monitor)#  cache timeout active 120
Device(config-flow-monitor)# record fr-1-out
Device(config-flow-monitor)# end

Device# show flow monitor fm-1-output cache format table
```

# Example: Configuring Flexible NetFlow for Ingress VRF Support

The following example configures the collection of theVRF ID from incoming packets on a device by applying an input flow monitor having a flow record that collects the VRF ID as a key field.

```
Device> enable
Device# configure terminal
Device(config)# flow record rm_1
Device(config-flow-record)# match routing vrf input
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# collect interface input
Device(config-flow-record)# collect interface output
Device(config-flow-record)# collect counter packets
Device(config-flow-record)# exit

Device(config)# flow monitor mm_1
Device(config-flow-record)# record rm_1
Device(config-flow-record)# exit

Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip vrf forwarding green
Device(config-if)# ip address 172.16.2.2 255.255.255.252
Device(config-if)# ip flow monitor mm_1 input
Device(config-if)# end
```

# Example: Configuring Flexible NetFlow for Egress VRF Support

The following example configures the collection of the VRF ID from outgoing packets on a device by applying an output flow monitor having a flow record that collects the VRF ID as a key field.

```
Device> enable
Device# configure terminal
Device(config)# flow record rm_1
Device(config-flow-record)# match routing vrf intput
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# collect interface input
Device(config-flow-record)# collect interface output
Device(config-flow-record)# collect counter packets
Device(config-flow-record)# exit

Device(config)# flow monitor mm_1
```

```
Device(config-flow-record)# record rm_1
Device(config-flow-record)# exit

Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip vrf forwarding green
Device(config-if)# ip address 172.16.2.2 255.255.255.252
Device(config-if)# ip flow monitor mm_1 output
Device(config-if)# end
```

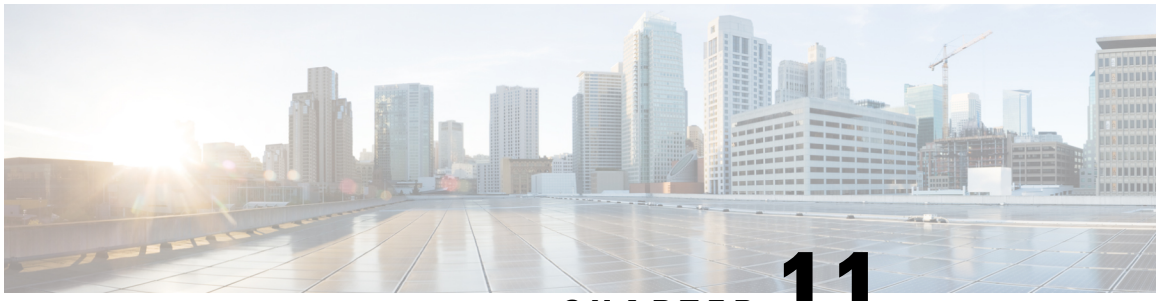
# Feature History for Flexible NetFlow

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless notedotherwise.

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Fuji 16.9.2 | Flexible NetFlow | Flexible NetFlow uses flows to provide statistics for accounting, network monitoring, and network planning. |
| Cisco IOS XE Gibraltar 16.12.1 | Source Group Tag (SGT), Destination Group Tag (DGT) over Flexible NetFlow for IPv6 traffic | Support was introduced for Source Group Tag (SGT), Destination Group Tag (DGT) fields over Flexible NetFlow, for IPv6 traffic. |
| Cisco IOS XE Bengaluru 17.5.1 | Flexible NetFlow for Egress VRF support | Support was introduced for configuring Flexible NetFlow for Egress VRF support.\ |

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.



CHAPTER 11

# Configuring Network Detection and Response


- Prerequisites for Network Detection and Response, on page 175
- Restrictions for Network Detection and Response, on page 175
- Information About Network Detection and Response, on page 175
- How to Configure Network Detection and Response, on page 176
- Verifying Network Detection and Response Configuration, on page 184
- Configuration Examples for Network Detection and Response, on page 185
- Feature History for Network Detection and Response, on page 188


## Prerequisites for Network Detection and Response

- All the devices in a network must have reachability to the Stealthwatch Cloud portal. Also, all the encrypted traffic must use HTTPS (TCP port 443) to reach the Stealthwatch Cloud portal.
- Ensure that there is sufficient bandwidth to avoid loss of data.

## Restrictions for Network Detection and Response

- Cisco Encrypted Traffic Analytics is not supported on the Stealthwatch Cloud portal.
- HTTPs proxy is not supported.
- Stealthwatch Cloud portal uses only the primary DNS server. An error is displayed if the primary DNS server fails.
- If DNS servers configured on the device are unable to resolve the Stealthwatch cloud monitor URLs, file uploads fail even if the Stealthwatch cloud sensor is registered to the Stealthwatch cloud portal.

## Information About Network Detection and Response

Cisco Secure Cloud Analytics (also known as the Stealthwatch Cloud) is a Network Detection and Response solution that uses enterprise telemetry to detect threats and provide accelerated threat response along with network segmentation. Cisco Secure Cloud Analytics also allows a network administrator to track all users logged into the network, and monitor their activities.

As part of the Network Detection and Response solution for Cisco Catalyst Switches, the enterprise telemetry used for analysis is Flexible NetFlow flows.

You must configure Stealthwatch Cloud properties on a device. You must then create a flow record and a flow exporter for the Stealthwatch Cloud portal.

**Note** A flow record must have the mandatory 5-tuple fields—protocol, source address, source port, destination address, and destination port configured along with the flow start, flow end, number of packets, and number of bytes for the records to be uploaded into the Stealthwatch Cloud portal.

Configure the flow record and flow exporter to a flow monitor. All the flows that are then generated from the flow monitor are converted into custom format and uploaded into the Stealthwatch Cloud portal.

# How to Configure Network Detection and Response

The following sections provide configuration information on network detection and response.

## Configuring a Certificate for Registration

To configure a certificate for registration, perform this procedure.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **crypto pki trustpoint** *name*<br>**Example:**<br>`Device(config)# crypto pki trustpoint stealthwatch1` | Declares the trustpoint and a given name and enters ca-trustpoint configuration mode. |
| **Step 4** | **revocation-check** *method1* [*method2 method3*]<br>**Example:**<br>`Device(ca-trustpoint)# revocation-check none` | Checks the revocation status of a certificate.<br>**none**: Certificate checking is ignored. |
| **Step 5** | **enrollment** *mode*<br>**Example:** | Specifies terminal as the enrollment mode of the certificate. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(ca-trustpoint)# enrollment terminal` | |
| **Step 6** | **exit**<br>**Example:**<br>`Device(ca-trustpoint)# exit` | Exits ca-trustpoint configuration mode and returns to global configuration mode. |
| **Step 7** | **crypto pki authenticate** *name*<br>**Example:**<br>`Device(config)# crypto pki authenticate stealthwatch1`<br>`Enter the base 64 encoded CA certificate.`<br>`End with a blank line or the word "quit" on a line by itself` | Authenticates the trustpoint name and enters ca-trustpoint configuration mode.<br>When prompted, copy and paste the Starfield Services Root Certificate from https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.pem.<br>The system prompts you with the following statement:<br>`% Do you accept this certificate? [yes/no]:`<br>Enter **yes** to confirm. |
| **Step 8** | **exit**<br>**Example:**<br>`Device(config)# exit` | Returns to privileged EXEC mode. |
| **Step 9** | **show pki trustpoints** *name*<br>**Example:**<br>`Device# show crypto pki trustpoints stealthwatch1` | (Optional) Displays information about the configured trustpoint. |

# Configuring a Certificate for File Upload

To configure a certificate for file upload, perform this procedure.

### Before you begin

Download the Baltimore CyberTrust Root certificate:

1. Open https://www.digicert.com/kb/digicert-root-certificates.htm in a web browser.
2. Under **Baltimore CyberTrust Root**, click **Download PEM**.
3. Choose a location and save the BaltimoreCyberTrustRoot.crt.pem file.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device> enable` | Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **crypto pki trustpoint** *name*<br>**Example:**<br>`Device(config)# crypto pki trustpoint stealthwatch2` | Declares the trustpoint and a given name and enters ca-trustpoint configuration mode. |
| **Step 4** | **revocation-check** *method1* [*method2 method3*]<br>**Example:**<br>`Device(ca-trustpoint)# revocation-check none` | Checks the revocation status of a certificate.<br>**none**: Certificate checking is ignored. |
| **Step 5** | **enrollment terminal**<br>**Example:**<br>`Device(ca-trustpoint)# enrollment terminal` | Specifies **terminal** as the enrollment mode of the certificate. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(ca-trustpoint)# exit` | Exits ca-trustpoint configuration mode and returns to global configuration mode. |
| **Step 7** | **crypto pki authenticate** *name*<br>**Example:**<br>`Device(config)# crypto pki authenticate stealthwatch2`<br>`Enter the base 64 encoded CA certificate.`<br>`End with a blank line or the word "quit" on a line by itself` | Authenticates the trustpoint name and enters ca-trustpoint configuration mode.<br>When prompted, copy and paste the text from the BaltimoreCyberTrustRoot.crt.pem file.<br>The system prompts you with the following statement:<br>`% Do you accept this certificate? [yes/no]:`<br>Enter **yes** to confirm. |
| **Step 8** | **exit**<br>**Example:**<br>`Device(config)# exit` | Returns to privileged EXEC mode. |
| **Step 9** | **show pki trustpoints** *name*<br>**Example:**<br>`Device# show crypto pki trustpoints stealthwatch2` | (Optional) Displays information about the configured trustpoint. |

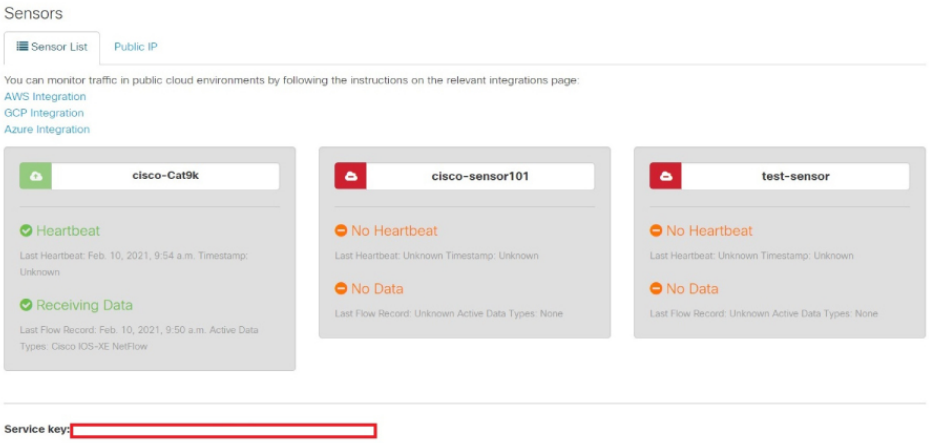
# Configuring Stealthwatch Cloud on a Device

To configure Stealthwatch Cloud on a device, perform this procedure.

### Before you begin

To view the service key from the Stealthwatch Cloud portal, peform the following steps:

1. Open the Stealthwatch Cloud portal from a browser.
2. In the **Dashboard** view, click the cloud icon located on the right corner of the window, and select **Sensors**.
3. Navigate to the bottom of the window to locate the service key.




### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **stealthwatch-cloud-monitor**<br>**Example:**<br>`Device(config)# stealthwatch-cloud-monitor` | Configures the Stealthwatch Cloud monitor and enters stealthwatch-cloud-monitor configuration mode. |
| **Step 4** | **service-key** *SwC-service-key*<br>**Example:** | Configures the Stealthwatch Cloud service key. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-stealthwatch-cloud-monitor)# service-key xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx` | |
| **Step 5** | **sensor-name** *SwC-sensor-name*<br>**Example:**<br>`Device(config-stealthwatch-cloud-monitor)# sensor-name mysensor` | (Optional) Sets a sensor name for the Stealthwatch Cloud registration. By default, the device serial number is used as the sensor name. |
| **Step 6** | **url** *SwC-server-url*<br>**Example:**<br>`Device(config-stealthwatch-cloud-monitor)# url https://sensors.eu-2.obsrvbl.com` | (Optional) Configures the URL of the Stealthwatch Cloud server.<br>To avoid redirects, configure the appropriate Stealthwatch Cloud server URL. If no URL is configured, by default, the URL of the Stealthwatch Cloud server, located in the U.S, is used. Based on your location, the default URL redirects you to the nearest Stealthwatch Cloud server URL. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-stealthwatch-cloud-monitor)# end` | Returns to privileged EXEC mode. |

# How to Integrate Flexible NetFlow with the Stealthwatch Cloud Portal

The following sections provide configuration information on how to integrate Flexible Netflow with the Stealthwatch Cloud portal.

## Creating a Flow Record

To create a flow record, perform this procedure.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **flow record** *record-name*<br>**Example:** | Creates a flow record and enters flow-record configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config)# flow record SWCRec` | |
| **Step 4** | **description** *description*<br>**Example:**<br>`Device(config-flow-record)# description swc flow` | (Optional) Creates a description for the flow record. |
| **Step 5** | **match ipv4 source address**<br>**Example:**<br>`Device(config-flow-record)# match ipv4 source address` | Configures the IPv4 source address as a key field for the record. |
| **Step 6** | **match ipv4 destination address**<br>**Example:**<br>`Device(config-flow-record)# match ipv4 destination address` | Configures the IPv4 destination address as a key field for the record. |
| **Step 7** | **match transport source-port**<br>**Example:**<br>`Device(config-flow-record)# match transport source-port` | Configures the source port as a key field for the record. |
| **Step 8** | **match transport destination-port**<br>**Example:**<br>`Device(config-flow-record)# match transport destination-port` | Configures the destination port as a key field for the record. |
| **Step 9** | **match ipv4 protocol**<br>**Example:**<br>`Device(config-flow-record)# match ipv4 protocol` | Configures the IPv4 protocol as a key field for the record. |
| **Step 10** | **collect counter bytes long**<br>**Example:**<br>`Device(config-flow-record)# collect counter bytes long` | Configures the number of bytes seen in a flow as a nonkey field and enables collecting the total number of bytes from the flow. |
| **Step 11** | **collect counter packets long**<br>**Example:**<br>`Device(config-flow-record)# collect counter packets long` | Configures the number of packets seen in a flow as a nonkey field and enables collecting the total number of packets from the flow. |
| **Step 12** | **collect timestamp absolute first**<br>**Example:**<br>`Device(config-flow-record)# collect timestamp absolute first` | Configures the timestamp seen in a flow as a nonkey field and enables the collection of the absolute time the first packet was seen, from the flow. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 13** | **collect timestamp absolute last**<br>**Example:**<br>`Device(config-flow-record)# collect timestamp absolute last` | Configures the timestamp seen in a flow as a nonkey field and enables the collection of the absolute time the most recent packet was seen, from the flow. |
| **Step 14** | **end**<br>**Example:**<br>`Device(config-flow-record)# end` | Returns to privileged EXEC mode. |

## Creating a Flow Exporter

To create a flow exporter, peform this procedure.

**Note** Only one active flow exporter can be configured for Stealthwatch Cloud.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **flow exporter** *name*<br>**Example:**<br>`Device(config)# flow exporter SWCExp` | Creates a flow exporter and enters flow-exporter configuration mode. |
| **Step 4** | **destination** {*hostname*}<br>**Example:**<br>`Device(config-flow-exporter)# destination stealthwatch-cloud` | Sets the IPv4 destination address or hostname for this exporter. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-flow-record)# end` | Returns to privileged EXEC mode. |

## Configuring a Flow Monitor

To configure a flow monitor, perform this procedure.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **flow monitor** *flow-monitor-name*<br>**Example:**<br>`Device(config)# flow monitor SWCMon` | Defines the flow monitor. |
| **Step 4** | **cache timeout active** *seconds*<br>**Example:**<br>`Device(config-flow-monitor)# cache timeout active 60` | Specifies the active flow timeout in seconds. |
| **Step 5** | **exporter** *flow-exporter-name*<br>**Example:**<br>`Device(config-flow-monitor)# exporter SWCExp` | Exports the flow information to the exporter. |
| **Step 6** | **record** *flow-exporter-name*<br>**Example:**<br>`Device(config-flow-monitor)# record SWCRec` | Specifies the flow record with a basic IPv4 template. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config-flow-monitor)# end` | Returns to privileged EXEC mode. |

## Applying a Flow to an Interface

To apply a flow to an interface, perform this procedure.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device> enable` | Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device(config)# interface gigabitethernet 1/0/1` | Specifies an interface and enters interface configuration mode. |
| **Step 4** | **ip flow monitor** *monitor-name* **input**<br>**Example:**<br>`Device(config-if)# ip flow monitor SWCMon input` | Associates an IPv4 flow monitor to the interface for input packets. |
| **Step 5** | **ip flow monitor** *monitor-name* **output**<br>**Example:**<br>`Device(config-if)# ip flow monitor SWCMon output` | Associates an IPv4 flow monitor to the interface for output packets. |
| **Step 6** | **end**<br>**Example:**<br>`Device(config-if)# end` | Exits interface configuration mode and returns to privileged EXEC mode. |

# Verifying Network Detection and Response Configuration

Use the following commands in privileged EXEC mode to verify Network Detection and Response configuration.

*Table 16: Commands to Verify Network Detection and Response Configuration*

| Command | Purpose |
|---|---|
| **show stealth-watch-cloud detail** | Displays the Stealthwatch Cloud registration status and its configured values. |
| **show platform software fed switch** *switch-number* **swc statistics** | Displays the statistical information of the Stealthwatch Cloud integration. |
| **clear platform software fed switch** *switch-number* **swc statistics** | Clears the statistical information of the Stealthwatch Cloud integration. |
| **show platform software fed switch** *switch-number* **swc connection** | Displays the connection details and events of the Stealthwatch Cloud integration. |

| Command | Purpose |
|---|---|
| **clear platform software fed switch** *switch-number* **swc connection** | Clears the connection details and events of the Stealthwatch Cloud integration. |

# Configuration Examples for Network Detection and Response

The following sections provide configuration examples for Network Detection and Response.

## Example: Configuring and Integrating Stealthwatch Cloud on a Device

The following example shows how to configure and integrate Stealthwatch Cloud on a device:

```
Device> enable
Device# configure terminal
Device(config)# stealthwatch-cloud-monitor
Device(stealthwatch-cloud-monitor)# service-key XXXXXXXXXXXXXXXXXXXX
Device(stealthwatch-cloud-monitor)# sensor-name mysensor
Device(stealthwatch-cloud-monitor)# url https://sensors.eu-2.obsrvbl.com
Device(stealthwatch-cloud-monitor)# exit
Device(config)# flow record SWCRec
Device(config-flow-record)# description for stealthwatch cloud
Device(config-flow-record)# match ipv4 source address
Device(config-flow-record)# match ipv4 destination address
Device(config-flow-record)# match ipv4 protocol
Device(config-flow-record)# match transport source-port
Device(config-flow-record)# match transport destination-port
Device(config-flow-record)# match flow cts source group-tag
Device(config-flow-record)# match flow cts destination group-tag
Device(config-flow-record)# collect counter byte long
Device(config-flow-record)# collect counter packet long
Device(config-flow-record)# collect timestamp absolute first
Device(config-flow-record)# collect timestamp absolute last
Device(config-flow-record)# exit
Device(config)# flow exporter SWCExp
Device(config-flow-exporter)# destination stealthwatch-cloud
Device(config- flow-exporter)# exit
Device(config)# flow monitor SWCMon
Device(config-flow-monitor)# cache timeout active 60
Device(config-flow-monitor)# exporter SWCExp
Device(config-flow-monitor)# record SWCRec
Device(config-flow-monitor)# exit
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# ip flow monitor SWCMon input
Device(config-if)# ip flow monitor SWCMon output
Device(config-if)# end
```

## Example: Verifying Stealthwatch Cloud Configuration

The following example shows a sample output of the **show stealthwatch-cloud detail** command:

```
Device> enable
Device# show stealthwatch-cloud detail
=======================================
Stealthwatch Cloud Parameters
=======================================
   Service Key  : XXXXXXXXXXXXXXXXXXXXXXXX
   Sensor Name  : C9200
   URL          : https://sensor.eu-prod.obsrvbl.com
=======================================
Stealthwatch Cloud Sensor Info
=======================================
   Sensor Status    : Registered
   Last heartbeat   : 2020-08-21T10:35:16
```

The following is a sample output of the **show platform fed switch active swc statistics** command:

```
Device> enable
Device# show platform software fed switch active swc statistics
==========================
SWC Upload Statistics:
==========================
 1: Last file uploaded  :  202102100928_1
 2: Time of upload  :  02/10/21 09:29:41 UTC
 3: Current file uploading :
 4: Files queued for upload :
 5: Number of files queued :  0
 6: Last failed upload  :
 7: Files failed to upload :  0
 8: Files successfully uploaded :  1
==========================
SWC File Creation Statistics:
==========================
 9: Last file created  :  202102100929_1
10: Time of creation  :  02/10/21 09:29:08 UTC
==========================
SWC Flow Statistics:
==========================
11: Number of flows in prev file:  15
12: Number of flows in curr file:  11
13: Invalid dropped flows :  0
14: Error dropped flows  :  0
==========================
SWC Flags:
==========================
15: Is Registered  :  Registered
16: Delete debug   :  Disabled
17: Exporter delete debug  :  Disabled
18: Certificate Validation  :  Enabled
```

The following is a sample output of the **show platform software fed switch active swc connection** command:

```
Device> enable
Device# show platform software fed switch active swc connection
Stealthwatch-Cloud details
  Registration
    #ID         : 0xc000001
    URL         : https://sensor.ext.obsrvbl.com
    Service Key : XXXXXXXXXXXXXXXXXXXXXXXX
    Sensor Name : C9200
```

```
    Registered  : N/A
  Connection
    Status               : DOWN
<<— Status will be in UP state only when the flow uploads into the Stealthwatch Cloud.
    Last status update   : 02/09/2021 10:10:47
    # Flaps              : 0
    # Heartbeats         : 0
    # Lost heartbeats    : 0
    Total RX bytes       : 7360
    Total TX bytes       : 869
    Upload Speed (B/s)   : 127
    Download Speed (B/s) : 58
    # Open sessions      : 0
    # Redirections       : 0
    # Timeouts           : 0

  HTTP Events
    GET response                  : 4
    GET request                   : 4
    GET Status Code 2XX           : 4
    PUT response                  : 12
    PUT request                   : 12
    PUT Status Code 2XX           : 2
    POST response                 : 2
    POST request                  : 2
    POST Status Code 2XX          : 2

  API Events
    TX                            : 4
    OK                            : 2
    Error                         : 2

  Event History
Timestamp               #Times   Event               RC Context
----------------------- -------- ------------------- --
----------------------------------------
02/10/2021 09:29:41.126 2        SEND_OK              0 ID:0003

02/10/2021 09:29:39.795 2        SIGNAL_DATA          0 ID:0003

02/10/2021 09:29:38.279 12       PUT_DATA             0 ID:0003

02/10/2021 09:29:37.962 4        GET_URL              0 ID:0003

02/10/2021 09:29:37.961 4        SEND_START           0 ID:0003

02/10/2021 09:27:41.484 2        SEND_ERR             0 ID:0001

02/10/2021 09:27:41.484 2        MAX_ATTEMPTS         0 ID:0001

02/10/2021 09:22:53.670 4        REGISTER_OK          0 Not applicable

02/10/2021 09:22:53.670 4        SEND_ABORT_ALL       0 config change

02/10/2021 09:22:53.670 1        OPTIONS_CONFIG       0 File Extension: .csv.gz (reset)

02/10/2021 09:22:53.669 1        OPTIONS_CONFIG       0 Data Type: ios-xe-catalyst

02/10/2021 09:22:53.669 1        OPTIONS_CONFIG       0 URL: https://sensor.ext.obsrvbl.com
 (res
02/10/2021 09:22:53.668 1        OPTIONS_CONFIG       0 Sensor Name: niinamdaUS (reset)

02/10/2021 09:22:53.553 1        OPTIONS_CONFIG       0 Service Key:
b5tQtXJM8AGZSp6oB8PvK4H0FiW
```

# Feature History for Network Detection and Response

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|---|---|---|
| Cisco IOS XE Bengaluru 17.5.1 | Network Detection and Response | Cisco Secure Cloud Analytics (also known as Stealthwatch Cloud) is a Network Detection and Response solution that provides advanced threat detection, accelerated threat response, and simplified network segmentation |

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.