# CONTENTS

## CHAPTER 1

**Cisco Embedded Service 3300 Series Switches Software Configuration Overview**  
- Finding Feature Information  
- General Description  
- SKU Information  
- Network Ports  
- Main Module  
- Expansion Module  
- Secure Boot  
- Secure Boot Architecture  
- Auto Boot Stages  
- Software Overview  
- Cisco IOS-XE  
- Software Features Available in IOS-XE  
- Layer 2 Software Features  
- Layer 2 Security Features  
- Manageability Features  
- Unsupported Features for the Initial Software Release  
- Quick Setup Tasks  
- Initial Setup Tasks  
- Perform Day 0 Configuration  
- Creating User Accounts  
- Configure Switch-Wide Settings  
- Configure VLAN Settings  
- Configure STP Settings  
- Next Steps
Using the Web User Interface 8
Web User Interface 8
Related Documentation 10

CHAPTER 2

New Features for Release 16.12.1 11

VRF-Lite 11
  VRF-Lite Characteristics 11
  Routing Table Setup in Ternary Content-Addressable Memory (TCAM) 12
  Run Time Packet Processing 12
  VRF Table ID Management 12
  Command Line Interface 13

OSPF 13
  OSPF Area Parameters 14
  Other OSPF Parameters 14
  LSA Group Pacing 15
  Configuring OSPF 15

Layer 2 Network Address Translation 15

MACsec and the MACsec Key Agreement (MKA) Protocol 16
  Information About MACsec Encryption 16
    MKA Policies 16
    Single-Host Mode 16
    MKA Statistics 17
  How to Configure MACsec Encryption 22
    Configuring MKA and MACsec 22
    Configuring MACsec MKA using PSK 26
    Configuring MKA/MACsec for Port Channel 28
    Configuring MACsec Cipher Announcement 30

Configuration Examples for MACsec Encryption 32
  Configuring MACsec on an Interface 32
  Example: Configuring MACsec MKA for Port Channel using PSK 35
  Examples: Configuring MACsec Cipher Announcement 39

Support for Routed Ports 42
  Command Line Interface 43
  Feature Restrictions 43
CHAPTER 3

Information About L2 Network Address Translation (NAT) 57

Prerequisites 61
Guidelines and Limitations 61
Default Settings 61
Configuring Layer 2 NAT 62
Verifying Configuration 63
Basic Inside-to-Outside Communications Example 64
Duplicate IP Addresses Example 65
Related Documents 68
Feature History 68

CHAPTER 4

Configuring Precision Time Protocol 69

Information About Precision Time Protocol 69
Why PTP? 69
Ethernet Switches and Delays 70
Message-Based Synchronization 70
PTP Event Message Sequences 71
  Synchronizing with Boundary Clocks 71
  Synchronizing with Peer-to-Peer Transparent Clocks 72
  Synchronizing the Local Clock 73
CHAPTER 6  Configuring Resilient Ethernet Protocol  109
Finding Feature Information  109
Resilient Ethernet Protocol Overview  109
   Link Integrity  111
   Fast Convergence  112
   VLAN Load Balancing  112
   Spanning Tree Interaction  113
   REP Ports  114
How to Configure Resilient Ethernet Protocol  114
   Default REP Configuration  114
   REP Configuration Guidelines  114
   Configuring the REP Administrative VLAN  116
   Configuring a REP Interface  117
   Setting Manual Preemption for VLAN Load Balancing  120
   Configuring SNMP Traps for REP  121
   Monitoring Resilient Ethernet Protocol Configurations  122

CHAPTER 7  Common Industrial Protocol (CIP)  125
   CIP Restrictions  125
   Enabling CIP  125
   Additional References  126

CHAPTER 8  Modicon Communication Bus (MODBUS)  129
   MODBUS Overview  129
   Configuring MODBUS  129
   Displaying MODBUS Information  130

CHAPTER 9  Serviceability and Zeroization Features for IoT  133
   Serviceability and Zeroization Features for IoT  133
   Serviceability Features  133
      Examples  133
   Device Zeroization or Depollution  135
      Command Line Interface  135
Class-Based Weighted Fair Queuing 158
Priority Queuing 159
Congestion Avoidance and Queuing 160
Configuring QoS 163
  Default QoS Configuration 164
  QoS Configuration Guidelines 164
  Using ACLs to Classify Traffic 164
  Creating IP Standard ACLs 165
  Creating IP Extended ACLs 166
  Creating Layer 2 MAC ACLs 168
  Using Class Maps to Define a Traffic Class 169
  Attaching a Traffic Policy to an Interface 171
Configuring Input Policy Maps 172
  Configuring Input Policy Maps with Individual Policing 172
  Configuring Input Policy Maps with Individual 2-rate, 3-color Policing 176
  Configuring Input Policy Maps with Marking 179
Configuring Output Policy Maps 181
  Configuring Output Policy Maps with Class-Based-Weighted-Queuing 182
  Configuring Output Policy Maps with Class-Based Shaping 184
  Configuring Output Policy Maps with Port Shaping 185
  Configuring Output Policy Maps with Class-Based Priority Queuing 186
  Configuring Priority Without Police 186
  Configuring Output Policy Maps with Weighted Tail Drop 188
Displaying QoS Information 191
  QoS Statistics 191
  Restrictions and Limitations 193

CHAPTER 13

Locate Switch 195
  Configuring Locate Switch 195

Full Cisco Trademarks with Software License
CHAPTER 1

Cisco Embedded Service 3300 Series Switches Software Configuration Overview

- Finding Feature Information, on page 2
- General Description, on page 2
- SKU Information, on page 2
- Network Ports, on page 3
- Main Module, on page 3
- Expansion Module, on page 3
- Secure Boot, on page 4
- Secure Boot Architecture, on page 4
- Auto Boot Stages, on page 4
- Software Overview, on page 5
- Cisco IOS-XE, on page 5
- Software Features Available in IOS-XE, on page 6
- Layer 2 Software Features, on page 6
- Layer 2 Security Features, on page 6
- Manageability Features, on page 6
- Unsupported Features for the Initial Software Release, on page 7
- Quick Setup Tasks, on page 7
- Initial Setup Tasks, on page 7
- Perform Day 0 Configuration, on page 7
- Creating User Accounts, on page 7
- Configure Switch-Wide Settings, on page 8
- Configure VLAN Settings, on page 8
- Configure STP Settings, on page 8
- Next Steps, on page 8
- Using the Web User Interface, on page 8
- Web User Interface, on page 8
- Related Documentation, on page 10
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

General Description

The Cisco ESS 3300 is an embedded Ethernet switch card that conforms to the PC104 form factor board size. The compact design simplifies integration and offers system integrators the ability to use the Cisco ESS 3300 in a wide variety of applications. The Cisco ESS 3300 consists of a Main Board and an optional Expansion Board. Both the Main Board and the Expansion Board are available with Cisco-designed cooling plates, and are also available without the cooling plates for system integrators who want to design their own custom thermal solutions.

The ESS-3300 is a ruggedized GigE Embedded platform for tactical, outdoor and mobile installations. Some of the key features are:

- PC104 form-factor (mechanical size)
- Main Board – 2 Optical 10G + 8 GE ports (4 combo)
- Expansion Board – 16 GE ports (4 combo)
- Next Generation IE switch feature set
- Software: IOS-XE, Network Essentials (available August 2018) and Network Advantage (Available early 2019)
- Native PoE software visibility
- External Express Setup Push Button, that supports the Zero-ize feature
- Two alarm inputs and One alarm output
- One SD interface
- One USB 2.0 Host interface for USB Flash Memory Device.
- One USB 2.0 Console Interface.
- One RS-232 Console Interface.

SKU Information

The following table lists the different SKUs available for the ESS3300.

<table>
<thead>
<tr>
<th>SKU</th>
<th>Description</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESS-3300-NCP-E</td>
<td>Main Board without a cooling plate.</td>
<td>2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper ports can also be combo ports.</td>
</tr>
</tbody>
</table>
Network Ports

Main Module

- 2 - Optical 10G Ports on the main module
- 4 - 1G Combo Ports on the main module
  - Support 10/100/1000 Copper
  - Support 100/1000 SFP interfaces
- 4 - Dedicated 10/100/1000 Copper ports on the main module for total of 8 – 1G network ports

Expansion Module

- 4 - 1G Combo Ports on the main module
  - Support 10/100/1000 Copper
  - Support 100/1000 SFP interfaces
- 12 - Dedicated 10/100/1000 Copper ports on the main module for total of 16 network ports

Note: 802.3af and 802.3at support is available if the integrator provides the PoE controllers on their finished product.

The ESS-3300 supports IOS-XE software control of PoE if the integrator adds the appropriate circuitry to their host chassis.

---

<table>
<thead>
<tr>
<th>SKU</th>
<th>Description</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESS-3300-CON-E</td>
<td>Main Board conduction cooled</td>
<td>2 ports of 10 GE fiber, 8 ports of GE copper. 4 of the 8 GE copper</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ports can also be combo ports</td>
</tr>
<tr>
<td>ESS-3300-24T-NCP-E</td>
<td>Main Board with a 16p Expansion Board without a</td>
<td>2 ports of 10 GE fiber, 24 ports of GE copper</td>
</tr>
<tr>
<td></td>
<td>cooling plate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 of 8 GE ports can be combo ports on mainboard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 of 16 GE ports can be combo ports on expansion board</td>
</tr>
<tr>
<td>ESS-3300-24T-CON-E</td>
<td>Main Board with a 16p Expansion Board conduction</td>
<td>2 ports of 10 GE fiber, 24 ports of GE copper</td>
</tr>
<tr>
<td></td>
<td>cooled</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 of 8 GE ports can be combo ports on mainboard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 of 16 GE ports can be combo ports on expansion board</td>
</tr>
</tbody>
</table>
Secure Boot

Secure Boot Architecture

The processor uses a multi-stage boot process that supports both a non-secure and a secure boot. For a secure boot, the system decrypts and authenticates the images while the 4096-bit RSA block authenticates the image. Upon reset, the CPU reads the device mode pins to determine the primary boot device to be used. Booting from these flash boot devices is supported.

- SD Flash
- On-board Flash

Note: The prior generation, ESS-2020, runs IOS Classic while the ESS-3300 uses IOS-XE. If you were connected to the console of an ESS-2020, you would not see the Linux boot messages that you will on the ESS-3300.

Auto Boot Stages

See the following graphic for an illustration of the auto boot sequence.
Software Overview

Cisco IOS-XE

The ESS3300 offers a rich IOS-XE feature set. This marketing data sheet provides a complete list of all of the features.


The Cisco IOS-XE information can be found at:

Software Features Available in IOS-XE

The following list of features are available.

Layer 2 Software Features

- STP
- VLAN
- Jumbo Frame
- Ether-Channel
- PVLAN
- Multicast
- VTP
- UDLD - Unidirectional Link Detection
- Address Learning
- SFP (minus combo ports)
- Basic PoE functionality

Layer 2 Security Features

- Port Security
- Storm Control
- SPAN
- DAI (Dynamic ARP Inspection)

Manageability Features

- DHCP Port based allocation
- DHCP Option 12
- Configuration Replace & Rollback
- CDP
- IPSLA
- LLDP-MED
- NTP
- SCP
- SNMPv3
- Vlan 1 Minimization
- RMON
- L2 Traceroute
- SNMPv3 Crypto
Unsupported Features for the Initial Software Release

- REP
- Netflow
- PAgP

Quick Setup Tasks

Initial Setup Tasks

On your first day with your new device, you can perform a number of tasks to ensure that your device is online, reachable and easily configured. Basic configuration will include:

- Perform Day Zero Configuration
- Create User Accounts
- Configure Switch-Wide Settings

Perform Day 0 Configuration

Complete the following steps to set up a device, which is configured with factory defaults, on Day 0:

1. Power on the device and connect a PC directly to a port.
2. Do not type in the initial dialog box that appears. At this point, IP address 192.168.1.1 is assigned to the device, and 192.168.1.2 is assigned to the PC. The PC launches Device manager using IP address 192.168.1.1.
3. Use the wizard to configure basic features.

Creating User Accounts

Setting a username and password is the first task you will perform on your device. Typically, as a network administrator, you will want to control access to your device and prevent unauthorized users from seeing your network configuration or manipulating your settings.

Log on using the default username and password provided with the device. The default username is cisco; the default password is the serial number of the switch chassis.

Set a password of up to 25 alphanumeric characters. The username password combination you set gives you privilege 15 access. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces.
Configure Switch-Wide Settings

Configure VLAN Settings

1. In the VLAN Configuration section, you can configure both data and voice VLANs. Type a name for your data VLAN.
2. To configure a data VLAN, ensure that the Data VLAN check box is checked, type a name for your VLAN, and assign a VLAN ID to it. If you are creating several VLANs, indicate only a VLAN range.
3. To change a bridge priority number from the default value 32748, change Bridge Priority to Yes and choose a priority number from the drop-down list.

Configure STP Settings

1. PVRST+ is the default STP mode configured on your device. You can change it to PVST from the STP Mode drop-down list.
2. To change a bridge priority number from the default value 32748, change Bridge Priority to Yes and choose a priority number from the drop-down list.

Next Steps

1. Click Day 0 Config Summary to verify your setup.
2. Click Finish.
3. Using the Web user interface is the quickest and easiest method of configuring your device for use. There are also a wide variety of command line options and commands available for configuration. See the section for further information.

Related Topics

Related Documentation, on page 10

Using the Web User Interface

Web User Interface

The Cisco IOS-XE operating system provides a graphical user interface for monitoring and configuration of your device. You can access the application from a client web browser. Ensure that the following web client requirements are met:

- Hardware - A Mac (OS version 10.9.5) or Windows (OS version 10) laptop or desktop compatible with one of the following tested and supported browsers:
  - Google Chrome 38 or later
  - Mozilla Firefox 35 or later
  - Microsoft Edge browser
• Display resolution - We recommend that you set the screen resolution to 1280 x 800 or higher.

The Web User Interface helps you to quickly perform the basic router configuration. To configure the device using quick setup wizard:

1. Connect the PC to the router using Ethernet cable.
2. Set up your PC as a DHCP client to obtain the IP address of the router automatically.
3. Launch the browser. In the address bar, type the IP address of the device.
4. Log on using the default username (cisco) and password provided with the router.

When launched, the initial display is a dashboard that looks similar to the following example:

**Figure 2: Home Page**

The application pages contain the following static global toolbar at the top right:

- **Home** - Takes you to the Home page.
- **Alerts** - Displays high severity, critical alerts that require your attention. Click the alerts icon, and click View All to see all the alerts that are currently reported by your device. You can search for alerts on your device and export them to an .xls file.
- **Save Configuration** - Saves your configuration.
- **Preferences** - Allows you to configure a home page and save it as a default view.
- **Language** - Displays the language options available for the Web user interface. The current options are English, Japanese and Chinese.
- **Help** - Launches the online help for the Web user interface.
- **Logout** - Exits the user interface.

The Web user interface allows you to perform the following tasks from the navigation pane:

<table>
<thead>
<tr>
<th>Navigation Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>View dashboards to give you a snapshot of connected client devices, performance information, incidents, and search options.</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Monitor your network on a daily basis and perform other ad-hoc operations related to network device inventory management.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Configure your device.</td>
</tr>
<tr>
<td>Administration</td>
<td>Perform administrative tasks regarding your device.</td>
</tr>
</tbody>
</table>
Troubleshoot connectivity problems and packet loss using Ping and Traceroute, and monitor device health and performance using web server logs, syslogs and packet captures.

### Related Documentation

The following documentation is available:

**Cisco Embedded Service 3300 Series Switches**

- Cisco Embedded Service 3300 Series Switches Hardware Technical Guide:

- Release Notes for Embedded Service 3300 Series Switches
CHAPTER 2

New Features for Release 16.12.1

- VRF-Lite, on page 11
- OSPF, on page 13
- Layer 2 Network Address Translation, on page 15
- MACsec and the MACsec Key Agreement (MKA) Protocol, on page 16
- Support for Routed Ports, on page 42
- USB Support, on page 43
- Layer 3 ACL Support, on page 43
- Resilient Ethernet Protocol (REP) Preferred, on page 44
- Parallel Redundancy Protocol (PRP) Support, on page 48
- Precision Time Protocol (PTP) Enhancements, on page 48
- PTP Use Case, on page 49
- Information About MRP, on page 49

VRF-Lite

VRF-Lite is a feature that enables a service provider to support two or more VPNs, where IP addresses can be overlapped among the VPNs. VRF-Lite uses input interfaces to distinguish routes for different VPNs, and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Interfaces in a VRF can be either physical, such as Ethernet ports, or logical, such as VLAN SVIs. However, a Layer 3 interface cannot belong to more than one VRF at any time. Every layer 3 interface (either an SVI or a routed port) needs to be grouped into its own VPN so that the proper routing table will be used for switching. CEF processes routes and adjacencies and passes the information down to the switch code to program the hardware. The VRF table id is freed when the IOS-XE OS deletes a table ID. The interface between CEF and the platform does not change for VRF-Lite. All the notifications for route addition, deletion, etc, are the same as Global Routing. The switch differentiates between different VRF routes as well as Global Routing via the table id. Separate Routing Tables define the domain for VRFs and Global Routing, and these tables are used to limit the forwarding within the domain. The Multi-VRF Support feature allows an operator to support two or more routing domains on a customer edge (CE) device, with each routing domain having its own set of interfaces and its own set of routing and forwarding tables.

VRF-Lite Characteristics

- Layer 3 interfaces: Since VRF-Lite is a layer 3 feature, nodes are connected through a layer 3 interface, for example Switch Virtual Interface (SVI) or Routed Port.
• Shall support overlapping ip unicast address across different VRFs.
• Multiple VLANs can be used as long as they are not overlapped with other customers. VLANs belonging to a customer will be mapped to a VRF table id for that customer. The VRF table id will be used to identify the appropriate routing table entry in the TCAM.
• 16 VRFs will be supported including Global Routing Table.
• VRF-Lite is supported with static/dynamic routing.

Routing Table Setup in Ternary Content-Addressable Memory (TCAM)

To support the VRF-Lite feature, multiple routing tables are entered in the switch layer 3 TCAM LPM tables. The switch identifies the table that a route belongs to. The table entries in TCAM can interleave with each other among different routing tables if their destination IP address mask is the same. The only way to tell the difference is through the VRF table id field. Each VLAN number is mapped to a VRF table id.

Run Time Packet Processing

When a packet is received, the switch determines which VPN it belongs to, and uses the proper VRF table to switch it. The VLAN number associated to a layer 3 interface receiving this packet is used. If the packet is received from a routed port, its internal VLAN number is used. If the packet is received from an SVI, the VLAN number is the same as the VLAN number when the SVI is configured. The VRF tables are identified by the VRF table id field in the switch TCAM LPM table, the overlapping IP addresses in different VPNs can be supported.

VRF Table ID Management

When a routing lookup occurs in the Local Forwarding Table, TCAM is searched sequentially and a match causes the packet to be Locally Forwarded. Table 2: Supported Features, on page 12 lists the supported features.

Table 2: Supported Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Supported Number or Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max IPv4 Route VRF</td>
<td>2048</td>
<td>Max number of supported IPv4 route is 2048 regardless the number of VRF created.</td>
</tr>
<tr>
<td>Max IPv6 Route VRF</td>
<td>512</td>
<td></td>
</tr>
<tr>
<td>VRF IPv6</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Static Routing</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Dynamic Routing</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Total VRFs supported</td>
<td>16</td>
<td>1 Global Routing Table + 15 VRFs</td>
</tr>
<tr>
<td>L3 Physical Port/SVI Interfaces Support</td>
<td>Yes</td>
<td>Only L3 Physical port / SVI are supported</td>
</tr>
<tr>
<td>VRF Leak</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Command Line Interface

The following are some examples of the CLIs.

Associates the VRF with the Layer 3 interface:

```
Switch(config-if)# vrf forwarding vrf name
```

Specifies the name of the VRF instance to associate with subsequent address family configuration mode commands:

```
config terminal
Switch# vrf definition vrf-name
Switch# address-family ipv4 unicast
```

Displays a summary of all VRFs present on the current router and their associated route-distinguishers and interface(s):

```
Switch# show ip vrf vrf-name
```

Displays the IP routing table associated with a specific VRF:

```
Switch# show ip route vrf vrf-name
```

OSPFA

OSPF is an Interior Gateway Protocol (IGP) designed expressly for IP networks, supporting IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets. The Cisco implementation supports RFC 1253, OSPF management information base (MIB).

The Cisco implementation conforms to the OSPF Version 2 specifications with these key features:

- Definition of stub areas is supported.
- Routes learned through any IP routing protocol can be redistributed into another IP routing protocol. At the intradomain level, this means that OSPF can import routes learned through EIGRP and RIP. OSPF routes can also be exported into RIP.
- Plain text and MD5 authentication among neighboring routers within an area is supported.
- Configurable routing interface parameters include interface output cost, retransmission interval, interface transmit delay, router priority, router dead and hello intervals, and authentication key.
- Virtual links are supported.
- Not-so-stubby-areas (NSSAs) per RFC 1587 are supported.

OSPF typically requires coordination among many internal routers, area border routers (ABRs) connected to multiple areas, and autonomous system boundary routers (ASBRs). The minimum configuration would use all default parameter values, no authentication, and interfaces assigned to areas. If you customize your environment, you must ensure coordinated configuration of all routers.
OSPF Area Parameters

You can optionally configure several OSPF area parameters. These parameters include authentication for password-based protection against unauthorized access to an area, stub areas, and not-so-stubby-areas (NSSAs). Stub areas are areas into which information on external routes is not sent. Instead, the area border router (ABR) generates a default external route into the stub area for destinations outside the autonomous system (AS). An NSSA does not flood all LSAs from the core into the area, but can import AS external routes within the area by redistribution.

Route summarization is the consolidation of advertised addresses into a single summary route to be advertised by other areas. If network numbers are contiguous, you can use the `area range` router configuration command to configure the ABR to advertise a summary route that covers all networks in the range.

Other OSPF Parameters

You can optionally configure other OSPF parameters in router configuration mode.

- **Route summarization:** When redistributing routes from other protocols. Each route is advertised individually in an external LSA. To help decrease the size of the OSPF link state database, you can use the `summary-address` router configuration command to advertise a single router for all the redistributed routes included in a specified network address and mask.

- **Virtual links:** In OSPF, all areas must be connected to a backbone area. You can establish a virtual link in case of a backbone-continuity break by configuring two Area Border Routers as endpoints of a virtual link. Configuration information includes the identity of the other virtual endpoint (the other ABR) and the nonbackbone link that the two routers have in common (the transit area). Virtual links cannot be configured through a stub area.

- **Default route:** When you specifically configure redistribution of routes into an OSPF routing domain, the route automatically becomes an autonomous system boundary router (ASBR). You can force the ASBR to generate a default route into the OSPF routing domain.

- **Domain Name Server (DNS) names for use in all OSPF show privileged EXEC command displays makes it easier to identify a router than displaying it by router ID or neighbor ID.**

- **Default Metrics:** OSPF calculates the OSPF metric for an interface according to the bandwidth of the interface. The metric is calculated as \( \text{ref-bw} \) divided by bandwidth, where \( \text{ref} \) is 10 by default, and \( \text{bandwidth} (bw) \) is specified by the `bandwidth` interface configuration command. For multiple links with high bandwidth, you can specify a larger number to differentiate the cost on those links.

- **Administrative distance:** is a rating of the trustworthiness of a routing information source, an integer between 0 and 255, with a higher value meaning a lower trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. OSPF uses three different administrative distances: routes within an area (interarea), routes to another area (interarea), and routes from another routing domain learned through redistribution (external). You can change any of the distance values.

- **Passive interfaces:** Because interfaces between two devices on an Ethernet represent only one network segment, to prevent OSPF from sending hello packets for the sending interface, you must configure the sending device to be a passive interface. Both devices can identify each other through the hello packet for the receiving interface.
• Route calculation timers: You can configure the delay time between when OSPF receives a topology change and when it starts the shortest path first (SPF) calculation and the hold time between two SPF calculations.

• Log neighbor changes: You can configure the router to send a syslog message when an OSPF neighbor state changes, providing a high-level view of changes in the router.

LSA Group Pacing

The OSPF LSA group pacing feature allows the router to group OSPF LSAs and pace the refreshing, check-summing, and aging functions for more efficient router use. This feature is enabled by default with a 4-minute default pacing interval, and you will not usually need to modify this parameter. The optimum group pacing interval is inversely proportional to the number of LSAs the router is refreshing, check-summing, and aging. For example, if you have approximately 10,000 LSAs in the database, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

Configuring OSPF

For detailed information about configuring OSPF, refer to the OSPF Configuration Guide.

Layer 2 Network Address Translation

Layer 2 NAT is a service that allows the assignment of a unique public IP address to an existing private IP address (end device), so that the end device can communicate on both the private and public subnets. This service is configured in a NAT-enabled device and is the public “alias” of the IP address physically programmed on the end device. This is typically represented by a table in the NAT device.

Layer 2 NAT has two translation tables where private-to-public and public-to-private subnet translations can be defined. Layer 2 NAT is a hardware based implementation that provides the same high level of (bump-on-the-wire) wire-speed performance. This implementation also supports multiple VLANs through the NAT boundary for enhanced network segmentation.

The Layer 2 static network address translation (L2NAT) feature is supported for the two uplink ports GigabitEthernet1/1 and GigabitEthernet1/2 respectively. L2NAT feature is supported on all expandable and advanced SKU combinations (IE3300 and IE3400) and available in both (essential and advantage) licenses. The Layer 2 NAT instances can be configured from management interfaces (CLI/SNMP/CIP/WebUI).

L2NAT feature scalability numbers for the IE3300 & IE3400 SKUs:

<table>
<thead>
<tr>
<th>SND</th>
<th>Name</th>
<th>Values</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Total number of NAT supported ports</td>
<td>2</td>
<td>Gi1/1 and Gi1/2</td>
</tr>
<tr>
<td>2</td>
<td>Total number of NAT instances</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Total number of NAT translations</td>
<td>256</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Total number VLAN mapped to NAT instances</td>
<td>128</td>
<td></td>
</tr>
</tbody>
</table>
MACsec and the MACsec Key Agreement (MKA) Protocol

Information About MACsec Encryption

MACsec and the MKA Protocol can be used with 802.1X single-host mode and Multi Domain Authentication (MDA) mode. Multiple-host mode and Multiple authentication mode are not supported in this release.

There are two Macsec Encryptions: 128-bit encryption and 256-bit encryption. The 128-bit encryption will be supported on both Network-Essentials and Advantage license. But the 256-bit encryption will only be supported on Network-Advantage license.

MACsec will be supported on all the ports of IE3200, IE3300, and IE3400. But on ESS3300, it will only be supported on 1-Gig ports but not on the 10-Gig ports.

MKA Policies

To enable MKA on an interface, a defined MKA policy should be applied to the interface. You can configure these options:

- Policy name, not to exceed 16 ASCII characters.
- Confidentiality (encryption) offset of 0, 30, or 50 bytes for each physical interface

Single-Host Mode

The figure shows how a single EAP authenticated session is secured by MACsec by using MKA.

Figure 3: MACsec in Single-Host Mode with a Secured Data Session
Some MKA counters are aggregated globally, while others are updated both globally and per session. You can also obtain information about the status of MKA sessions.

This is an example of the show mka statistics command output:

Switch# show mka sessions

Total MKA Sessions....... 1
  Secured Sessions... 1
  Pending Sessions... 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Local-TxSCI</th>
<th>Policy-Name</th>
<th>Inherited</th>
<th>Key-Server</th>
<th>Port-ID</th>
<th>Peer-RxSCI</th>
<th>MACsec-Peers</th>
<th>Status</th>
<th>CKN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>204c.9e85.ede4/002b</td>
<td>p2</td>
<td>NO</td>
<td>YES</td>
<td>43</td>
<td>c800.8459.e764/002a</td>
<td>1</td>
<td>Secured</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0100000000000000000000000000000000000000000000000000000000000000</td>
</tr>
</tbody>
</table>

Switch# show mka sessions interface Gi1/0/1

Summary of All Currently Active MKA Sessions on Interface GigabitEthernet1/0/1...

<table>
<thead>
<tr>
<th>Interface</th>
<th>Local-TxSCI</th>
<th>Policy-Name</th>
<th>Inherited</th>
<th>Key-Server</th>
<th>Port-ID</th>
<th>Peer-RxSCI</th>
<th>MACsec-Peers</th>
<th>Status</th>
<th>CKN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>204c.9e85.ede4/002b</td>
<td>p2</td>
<td>NO</td>
<td>YES</td>
<td>43</td>
<td>c800.8459.e764/002a</td>
<td>1</td>
<td>Secured</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0100000000000000000000000000000000000000000000000000000000000000</td>
</tr>
</tbody>
</table>

Switch# show mka sessions interface Gi1/0/1 de

MKA Detailed Status for MKA Session

Status: SECURED - Secured MKA Session with MACsec
Local Tx-SCI............ 204c.9e85.ede4/002b
Interface MAC Address.... 204c.9e85.ede4
MKA Port Identifier...... 43
Interface Name........... GigabitEthernet1/0/1
Audit Session ID..........
CAK Name (CKN)............ 0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI).... D46CEBC65D56759454CEAE
Message Number (MN)..... 89567
EAP Role................. NA
Key Server.............. YES
MKA Cipher Suite........ AES-128-CMAC
Latest SAK Status....... Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (RN)....... D46CEBC65D56759454CEAB000000001 (1)
Old SAK Status.......... FIRST-SAK
Old SAK AN.............. 0
Old SAK KI (KN).......... FIRST-SAK (0)
SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
MKA Policy Name......... p2
Key Server Priority...... 2
Delay Protection........ NO
Replay Protection........ YES
Replay Window Size....... 0
Confidentiality Offset.... 0
Algorithm Agility......... 80C201
Send Secure Announcement.. DISABLED
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers ............. 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
MI     MN     Rx-SCI (Peer)   KS Priority
-----  -----  -----------------  -------
38046BA37D7DA77E06D006A9  89555  c800.8459.e764/002a  10

Potential Peers List:
MI     MN     Rx-SCI (Peer)   KS Priority
-----  -----  -----------------  -------

Dormant Peers List:
MI     MN     Rx-SCI (Peer)   KS Priority
-----  -----  -----------------  -------

Switch#show mka sessions de
Switch#show mka sessions detail

MKA Detailed Status for MKA Session
-------------------------------------
Status: SECURED - Secured MKA Session with MACsec
Local Tx-SCI............. 204c.9e85.ede4/002b
Interface MAC Address.... 204c.9e85.ede4
MKA Port Identifier...... 43
Interface Name............ GigabitEthernet1/0/1
Audit Session ID........
CAB Name (CKN)........... 0000000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5E759543CEAE
Message Number (MN)...... 89572
EAP Role.................. NA
Key Server............... YES
MKA Cipher Suite......... AES-128-CMAC
Latest SAK Status........ Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status......... FIRST-SAK
Old SAK AN.............. 0
Old SAK KI (KN).......... FIRST-SAK (0)
SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time......... 0s (No Old SAK to retire)

MKA Policy Name........ p2
Key Server Priority...... 2
Delay Protection........ NO
Replay Protection........ YES
Replay Window Size....... 0
Confidentiality Offset.... 0
Algorithm Agility......... 80C201
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired............ YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:

<table>
<thead>
<tr>
<th>MI</th>
<th>MN</th>
<th>Rx-SCI (Peer)</th>
<th>KS Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>38046Ba37D7DA77E06D006A9</td>
<td>89560</td>
<td>c800.8459.e764/002a</td>
<td>10</td>
</tr>
</tbody>
</table>

Potential Peers List:

<table>
<thead>
<tr>
<th>MI</th>
<th>MN</th>
<th>Rx-SCI (Peer)</th>
<th>KS Priority</th>
</tr>
</thead>
</table>

Dormant Peers List:

<table>
<thead>
<tr>
<th>MI</th>
<th>MN</th>
<th>Rx-SCI (Peer)</th>
<th>KS Priority</th>
</tr>
</thead>
</table>

Switch#sh mka pol

MKA Policy Summary...

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>KS Priority</th>
<th>Delay Protect</th>
<th>Replay Protect</th>
<th>Window Size</th>
<th>Offset</th>
<th>Cipher Suite(s)</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>DEFAULT POLICY</em></td>
<td>0</td>
<td>FALSE</td>
<td>TRUE</td>
<td>0</td>
<td>0</td>
<td>GCM-AES-128</td>
<td></td>
</tr>
<tr>
<td>p1</td>
<td>1</td>
<td>FALSE</td>
<td>TRUE</td>
<td>0</td>
<td>0</td>
<td>GCM-AES-128</td>
<td></td>
</tr>
<tr>
<td>p2</td>
<td>2</td>
<td>FALSE</td>
<td>TRUE</td>
<td>0</td>
<td>0</td>
<td>GCM-AES-128</td>
<td>Gi1/0/1</td>
</tr>
</tbody>
</table>

Switch#sh mka poli
Switch#sh mka policy p2
Switch#sh mka policy p2 ?

detail Detailed configuration/information for MKA Policy
sessions Summary of all active MKA Sessions with policy applied
| Output modifiers
<cr>

Switch#sh mka policy p2 de

MKA Policy Configuration ("p2")

MKA Policy Name........ p2
Key Server Priority.... 2
Confidentiality Offset. 0
Send Secure Announcement..DISABLED
Cipher Suite(s)........ GCM-AES-128

Applied Interfaces...
    GigabitEthernet1/0/1

Switch#sh mka policy p2

MKA Policy Summary...

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>KS Priority</th>
<th>Delay Protect</th>
<th>Replay Protect</th>
<th>Window Size</th>
<th>Offset</th>
<th>Cipher Suite(s)</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>p2</td>
<td>2</td>
<td>FALSE</td>
<td>TRUE</td>
<td>0</td>
<td>0</td>
<td>GCM-AES-128</td>
<td>Gi1/0/1</td>
</tr>
</tbody>
</table>

Switch#sh mka se?
sessions

Switch#sh mka ?
  default-policy  MKA Default Policy details
  keychains     MKA Pre-Shared-Key Key-Chains
  policy        MKA Policy configuration information
  presharedkeys MKA Preshared Keys
  sessions      MKA Sessions summary
  statistics    MKA Global statistics
  summary       MKA Sessions summary & global statistics

Switch#sh mka-statistics
Switch#sh mka statistics ?
  interface   Statistics for a MKA Session on an interface
  local-sci   Statistics for a MKA Session identified by its Local Tx-SCI
   |         Output modifiers
   <cr>

Switch#sh mka-statistics interface G1/0/1
Switch#show mka statistics interface G1/0/1

MKA Statistics for Session
====================================
Reauthentication Attempts.. 0

CA Statistics
  Pairwise CAKs Derived... 0
  Pairwise CAK Rekeys..... 0
  Group CAKs Generated.... 0
  Group CAKs Received..... 0

SA Statistics
  SAKs Generated.......... 1
  SAKs Rekeyed............ 0
  SAKs Received........... 0
  SAK Responses Received.. 1

MKPDU Statistics
  MKPDUs Validated & Rx... 89585
    "Distributed SAK".. 0
    "Distributed CAK".. 0
  MKPDUs Transmitted..... 89596
    "Distributed SAK".. 1
    "Distributed CAK".. 0

Switch#show mka ?
  default-policy  MKA Default Policy details
  keychains     MKA Pre-Shared-Key Key-Chains
  policy        MKA Policy configuration information
  presharedkeys MKA Preshared Keys
  sessions      MKA Sessions summary
  statistics    MKA Global statistics
  summary       MKA Sessions summary & global statistics

Switch#show mka summ
Switch#show mka summary

Total MKA Sessions....... 1
  Secured Sessions... 1
  Pending Sessions... 0

<table>
<thead>
<tr>
<th>Interface</th>
<th>Local-TxSCI</th>
<th>Policy-Name</th>
<th>Inherited</th>
<th>Key-Server</th>
</tr>
</thead>
</table>

Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches Configuration Guide, Cisco IOS XE16.12.x
### Port-ID Peer-RxSCI MACsec-Peers Status CKN

<table>
<thead>
<tr>
<th>Port-ID</th>
<th>Peer-RxSCI</th>
<th>MACsec-Peers</th>
<th>Status</th>
<th>CKN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>204c.9e85.ede4/002b</td>
<td>p2</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>43</td>
<td>c800.8459.e764/002a.1</td>
<td></td>
<td>Secured</td>
<td>01000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
</tbody>
</table>

### MKA Global Statistics

**MKA Session Totals**
- Secured.................... 1
- Reauthentication Attempts.. 0
- Deleted (Secured)........... 0
- Keepalive Timeouts......... 0

**CA Statistics**
- Pairwise CAKs Derived...... 0
- Pairwise CAK Rekeys........ 0
- Group CAKs Generated....... 0
- Group CAKs Received........ 0

**SA Statistics**
- SAKs Generated............. 1
- SAKs Rekeyed................ 0
- SAKs Received.............. 0
- SAK Responses Received..... 1

**MKPDU Statistics**
- MKPDUs Validated & Rx...... 89589
  - "Distributed SAK"........ 0
  - "Distributed CAK"........ 0
- MKPDUs Transmitted......... 89600
  - "Distributed SAK"........ 1
  - "Distributed CAK"........ 0

**MKA Error Counter Totals**

**Session Failures**
- Bring-up Failures........... 0
- Reauthentication Failures... 0
- Duplicate Auth-Mgr Handle... 0

**SAK Failures**
- SAK Generation.............. 0
- Hash Key Generation......... 0
- SAK Encryption/Wrap.......... 0
- SAK Decryption/Unwrap........ 0
- SAK Cipher Mismatch......... 0

**CA Failures**
- Group CAK Generation......... 0
- Group CAK Encryption/Wrap.... 0
- Group CAK Decryption/Unwrap... 0
- Pairwise CAK Derivation...... 0
- CKN Derivation............... 0
- ICK Derivation............... 0
- KEK Derivation............... 0
- Invalid Peer MACsec Capability... 0

**MACsec Failures**
- Rx SC Creation.............. 0
- Tx SC Creation................ 0
- Rx SA Installation.......... 0
How to Configure MACsec Encryption

Configuring MKA and MACsec

Default MACsec MKA Configuration

MACsec is disabled. No MKA policies are configured.

Configuring an MKA Policy

SUMMARY STEPS

1. `configure terminal`
2. `mka policy policy name`
3. `send-secure-announcements`
4. `key-server priority`
5. `include-icv-indicator`
6. `macsec-cipher-suite gcm-aes-128`
7. `confidentiality-offset Offset value`
8. `end`
9. `show mka policy`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 mka policy policy name</td>
<td>Identify an MKA policy, and enter MKA policy configuration mode. The maximum policy name length is 16 characters. The default MACsec cipher suite in the MKA policy will always be &quot;GCM-AES-128&quot;. If the device supports both &quot;GCM-AES-128&quot; and &quot;GCM-AES-256&quot; ciphers, it is highly recommended to define and use a user defined MKA policy to include both 128 and 256 bits ciphers or only 256 bits cipher, as may be required.</td>
</tr>
<tr>
<td>Step 3 send-secure-announcements</td>
<td>Enabled secure announcements.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 4</strong> key-server priority</td>
<td>Configure MKA key server options and set priority (between 0-255).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When value of key server priority is set to 255, the peer can not become the key server. The key server priority value is valid only for MKA PSK; and not for MKA EAPTLS.</td>
</tr>
<tr>
<td><strong>Step 5</strong> include-icv-indicator</td>
<td>Enables the ICV indicator in MKPDU. Use the no form of this command to disable the ICV indicator — <strong>no include-icv-indicator</strong>.</td>
</tr>
<tr>
<td><strong>Step 6</strong> macsec-cipher-suite gcm-aes-128</td>
<td>Configures cipher suite for deriving SAK with 128-bit encryption.</td>
</tr>
<tr>
<td><strong>Step 7</strong> confidentiality-offset Offset value</td>
<td>Set the Confidentiality (encryption) offset for each physical interface</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Offset Value can be 0, 30 or 50. If you are using Anyconnect on the client, it is recommended to use Offset 0.</td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 9</strong> show mka policy</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>

**Example**

This example configures the MKA policy:

```
Switch(config)# mka policy mka_policy
Switch(config-mka-policy)# key-server priority 200
Switch(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Switch(config-mka-policy)# confidentiality-offset 30
Switch(config-mka-policy)# end
```

**Configuring MACsec on an Interface**

Follow these steps to configure MACsec on an interface with one MACsec session for voice and one for data:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface interface-id
4. switchport access vlan vlan-id
5. switchport mode access
### Configuring MACsec on an Interface

6. `macsec`
7. `authentication event linksec fail action authorize vlan vlan-id`
8. `authentication host-mode multi-domain`
9. `authentication linksec policy must-secure`
10. `authentication port-control auto`
11. `authentication periodic`
12. `authentication timer reauthenticate`
13. `authentication violation protect`
14. `mka policy policy name`
15. `dot1x pae authenticator`
16. `spanning-tree portfast`
17. `end`
18. `show authentication session interface interface-id`
19. `show authentication session interface interface-id details`
20. `show macsec interface interface-id`
21. `show mka sessions`
22. `copy running-config startup-config`

### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
Example:  
`Switch>enable`                                            | Enables privileged EXEC mode. Enter the password if prompted. |
| **Step 2**  
Example:  
`Switch>configure terminal`                                 | Enter global configuration mode. |
| **Step 3**  
`interface interface-id`                                     | Identify the MACsec interface, and enter interface configuration mode. The interface must be a physical interface. |
| **Step 4**  
`switchport access vlan vlan-id`                             | Configure the access VLAN for the port. |
| **Step 5**  
`switchport mode access`                                     | Configure the interface as an access port. |
| **Step 6**  
`macsec`                                                     | Enable 802.1ae MACsec on the interface. The macsec command enables MKA MACsec on switch-to-host links (downlink ports) only. |
| **Step 7**  
`authentication event linksec fail action authorize vlan vlan-id` | (Optional) Specify that the switch processes authentication link-security failures resulting from unrecognized user credentials by authorizing a restricted VLAN on the port after a failed authentication attempt. |
| **Step 8**  
`authentication host-mode multi-domain`                     | Configure authentication manager mode on the port to allow both a host and a voice device to be authenticated |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>authentication linksec policy must-secure</strong></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>authentication port-control auto</strong></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>authentication periodic</strong></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>authentication timer reauthenticate</strong></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td><strong>authentication violation protect</strong></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td><strong>mka policy policy name</strong></td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td><strong>dot1x pae authenticator</strong></td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td><strong>spanning-tree portfast</strong></td>
</tr>
<tr>
<td><strong>Step 17</strong></td>
<td><strong>end</strong></td>
</tr>
</tbody>
</table>

**Example:**
```
Switch (config)#end
```

**Step 18** | **show authentication session interface interface-id** | Verify the authorized session security status. |

**Step 19** | **show authentication session interface interface-id details** | Verify the details of the security status of the authorized session. |

**Step 20** | **show macsec interface interface-id** | Verify MacSec status on the interface. |

**Step 21** | **show mka sessions** | Verify the established mka sessions. |
Configuring MACsec MKA using PSK

### SUMMARY STEPS

1. `configure terminal`
2. `key chain key-chain-name macsec`
3. `key hex-string`
4. `cryptographic-algorithm {gcm-aes-128 | gcm-aes-256}`
5. `key-string { [0|6|7] pwd-string | pwd-string }`
6. `lifetime local [start timestamp {hh:mm:ss | day | month | year}] [duration seconds | end timestamp {hh:mm:ss | day | month | year}]`
7. `end`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>key chain key-chain-name macsec</code></td>
<td>Configures a key chain and enters the key chain configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>key hex-string</code></td>
<td>Configures a unique identifier for each key in the keychain</td>
</tr>
<tr>
<td></td>
<td>and enters the keychain's key configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> For 128-bit encryption, use 32 hex digit key-string. For</td>
</tr>
<tr>
<td></td>
<td>256-bit encryption, use 64 hex digit key-string.</td>
</tr>
<tr>
<td><strong>Step 4</strong> `cryptographic-algorithm {gcm-aes-128</td>
<td>gcm-aes-256}`</td>
</tr>
<tr>
<td></td>
<td>256-bit encryption.</td>
</tr>
<tr>
<td><strong>Step 5</strong> `key-string { [0</td>
<td>6</td>
</tr>
<tr>
<td><strong>Step 6</strong> `lifetime local [start timestamp {hh:mm:ss</td>
<td>day</td>
</tr>
<tr>
<td><strong>Step 7</strong> <code>end</code></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Example

Following is an indicative example:
Configuring MACsec MKA on an Interface using PSK

To avoid traffic drop across sessions, the `mka policy` command must be configured before the `mka pre-shared-key key-chain` command.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface interface-id`
3. `macsec`
4. `mka policy policy-name`
5. `mka pre-shared-key key-chain key-chain name`
6. `macsec replay-protection window-size frame number`
7. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 3</td>
<td>macsec</td>
</tr>
<tr>
<td>Step 4</td>
<td>mka policy policy-name</td>
</tr>
<tr>
<td>Step 5</td>
<td>mka pre-shared-key key-chain key-chain name</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The MKA pre-shared key can be configured on either physical interface or sub-interfaces and not on both.</td>
</tr>
<tr>
<td>Step 6</td>
<td>macsec replay-protection window-size frame number</td>
</tr>
<tr>
<td>Step 7</td>
<td>end</td>
</tr>
</tbody>
</table>

**Example**

Following is an indicative example:
Switch(config)# interface GigabitEthernet 0/0/0
Switch(config-if)# mka policy mka_policy
Switch(config-if)# mka pre-shared-key key-chain key-chain-name
Switch(config-if)# macsec replay-protection window-size 10
Switch(config-if)# end

What to do next

It is not recommended to change the MKA policy on an interface with MKA PSK configured when the session is running. However, if a change is required, you must reconfigure the policy as follows:

1. Disable the existing session by removing macsec configuration on each of the participating node using the no macsec command.
2. Configure the MKA policy on the interface on each of the participating node using the mka policy policy-name command.
3. Enable the new session on each of the participating node by using the macsec command.

Configuring MKA/MACsec for Port Channel

Configuring MKA/MACsec for Port Channel Using PSK

SUMMARY STEPS

1. configure terminal
2. interface interface-id
3. macsec
4. mka policy policy-name
5. mka pre-shared-key key-chain key-chain-name
6. channel-group channel-group-number mode {active | passive } | {on }
7. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>macsec</td>
<td>Enables MACsec on the interface. Supports layer 2 and layer 3 port channels.</td>
</tr>
<tr>
<td>Step 4</td>
<td>mka policy policy-name</td>
<td>Configures an MKA policy.</td>
</tr>
<tr>
<td>Step 5</td>
<td>mka pre-shared-key key-chain key-chain-name</td>
<td>Configures an MKA pre-shared-key key-chain name.</td>
</tr>
<tr>
<td>Note</td>
<td>The MKA pre-shared key can be configured on either physical interface or sub-interfaces and not on both.</td>
<td></td>
</tr>
</tbody>
</table>
Purpose
Command or Action

Step 6
channel-group channel-group-number mode {active | passive } | {on }

Purpose
Configures the port in a channel group and sets the mode. The channel-number range is from 1 to 4096. The port channel associated with this channel group is automatically created if the port channel does not already exist. For mode, select one of the following keywords:

- **on** — Forces the port to channel without PAgP or LACP. In the on mode, an EtherChannel exists only when a port group in the on mode is connected to another port group in the on mode.
- **active** — Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.
- **passive** — Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation.

Step 7
end

Returns to privileged EXEC mode.

Configuring Port Channel Logical Interfaces for Layer 2 EtherChannels

To create a port channel interface for a Layer 2 EtherChannel, perform this task:

**SUMMARY STEPS**

1. configure terminal
2. [no] interface port-channel channel-group-number
3. switchport
4. switchport mode {access | trunk }
5. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>[no] interface port-channel channel-group-number</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport mode {access</td>
</tr>
</tbody>
</table>
Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels

To create a port channel interface for a Layer 3 EtherChannel, perform this task:

SUMMARY STEPS
1. configure terminal
2. interface port-channel interface-id
3. no switchport
4. ip address ip-address subnet_mask
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface port-channel interface-id</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 no switchport</td>
<td>Switches an interface that is in Layer 2 mode into Layer 3 mode for Layer 3 configuration.</td>
</tr>
<tr>
<td>Step 4 ip address ip-address subnet_mask</td>
<td>Assigns an IP address and subnet mask to the EtherChannel.</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Configuring MACsec Cipher Announcement

Configuring an MKA Policy for Secure Announcement

SUMMARY STEPS
1. configure terminal
2. mka policy policy-name
3. key-server priority
4. [no] send-secure-announcements
5. macsec-cipher-suite {gcm-aes-128 | gcm-aes-256}
6. end
7. show mka policy

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

| Step 2 | mka policy policy-name | Identify an MKA policy, and enter MKA policy configuration mode. The maximum policy name length is 16 characters. |

**Note**

The default MACsec cipher suite in the MKA policy will always be "GCM-AES-128". If the device supports both "GCM-AES-128" and "GCM-AES-256" ciphers, it is highly recommended to define and use a user defined MKA policy to include both 128 and 256 bits ciphers or only 256 bits cipher, as may be required.

| Step 3 | key-server priority | Configure MKA key server options and set priority (between 0-255). |

**Note**

When value of key server priority is set to 255, the peer cannot become the key server. The key server priority value is valid only for MKA PSK; and not for MKA EAPTLS.

| Step 4 | [no] send-secure-announcements | Enables sending of secure announcements. Use the no form of the command to disable sending of secure announcements. By default, secure announcements are disabled. |

| Step 5 | macsec-cipher-suite {gcm-aes-128 | gcm-aes-256} | Configures cipher suite for deriving SAK with 128-bit or 256-bit encryption. |

| Step 6 | end | Returns to privileged EXEC mode. |

| Step 7 | show mka policy | Verify your entries. |

### Configuring Secure Announcement Globally (Across all the MKA Policies)

**SUMMARY STEPS**

1. configure terminal
2. [no] mka defaults policy send-secure-announcements
3. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>[no] mka defaults policy send-secure-announcements</td>
</tr>
</tbody>
</table>
Configuring EAPoL Announcements on an interface

SUMMARY STEPS

1. configure terminal
2. interface interface-id
3. [no] eapol announcement
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1   configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2   interface interface-id</td>
<td>Identifies the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.</td>
</tr>
<tr>
<td>Step 3   [no] eapol announcement</td>
<td>Enable EAPoL announcements. Use the no form of the command to disable EAPoL announcements. By default, EAPoL announcements are disabled.</td>
</tr>
<tr>
<td>Step 4   end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Configuration Examples for MACsec Encryption

Configuring MACsec on an Interface

Follow these steps to configure MACsec on an interface with one MACsec session for voice and one for data:

SUMMARY STEPS

1. enable
2. configure terminal
3. interface interface-id
4. switchport access vlan vlan-id
5. switchport mode access
6. macsec
7. authentication event linksec fail action authorize vlan vlan-id
8. authentication host-mode multi-domain
9. authentication linksec policy must-secure
10. authentication port-control auto
11. authentication periodic
12. authentication timer reauthenticate
13. authentication violation protect
14. mka policy policy name
15. dot1x pae authenticator
16. spanning-tree portfast
17. end
18. show authentication session interface interface-id
19. show authentication session interface interface-id details
20. show macsec interface interface-id
21. show mka sessions
22. copy running-config startup-config

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter the password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt;enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch&gt;configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface interface-id</td>
<td>Identify the MACsec interface, and enter interface configuration mode. The interface must be a physical interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong> switchport access vlan vlan-id</td>
<td>Configure the access VLAN for the port.</td>
</tr>
<tr>
<td><strong>Step 5</strong> switchport mode access</td>
<td>Configure the interface as an access port.</td>
</tr>
<tr>
<td><strong>Step 6</strong> macsec</td>
<td>Enable 802.1ae MACsec on the interface. The macsec command enables MKA MACsec on switch-to-host links (downlink ports) only.</td>
</tr>
<tr>
<td><strong>Step 7</strong> authentication event linksec fail action authorize vlan vlan-id</td>
<td>(Optional) Specify that the switch processes authentication link-security failures resulting from unrecognized user credentials by authorizing a restricted VLAN on the port after a failed authentication attempt.</td>
</tr>
<tr>
<td><strong>Step 8</strong> authentication host-mode multi-domain</td>
<td>Configure authentication manager mode on the port to allow both a host and a voice device to be authenticated on the 802.1x-authorized port. If not configured, the default host mode is single.</td>
</tr>
<tr>
<td><strong>Step 9</strong> authentication linksec policy must-secure</td>
<td>Set the LinkSec security policy to secure the session with MACsec if the peer is available. If not set, the default is should secure.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>10</td>
<td>authentication port-control auto</td>
</tr>
<tr>
<td>11</td>
<td>authentication periodic</td>
</tr>
<tr>
<td>12</td>
<td>authentication timer reauthenticate</td>
</tr>
<tr>
<td>13</td>
<td>authentication violation protect</td>
</tr>
<tr>
<td>14</td>
<td>mka policy policy name</td>
</tr>
<tr>
<td>15</td>
<td>dot1x pae authenticator</td>
</tr>
<tr>
<td>16</td>
<td>spanning-tree portfast</td>
</tr>
<tr>
<td>17</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Example: Switch (config)#end</td>
</tr>
<tr>
<td>18</td>
<td>show authentication session interface interface-id</td>
</tr>
<tr>
<td>19</td>
<td>show authentication session interface interface-id details</td>
</tr>
<tr>
<td>20</td>
<td>show macsec interface interface-id</td>
</tr>
<tr>
<td>21</td>
<td>show mka sessions</td>
</tr>
<tr>
<td>22</td>
<td>copy running-config startup-config</td>
</tr>
<tr>
<td></td>
<td>Example: Switch#copy running-config startup-config</td>
</tr>
</tbody>
</table>
Example: Configuring MACsec MKA for Port Channel using PSK

Etherchannel Mode — Static/On

The following is a sample configuration on Device 1 and Device 2 with EtherChannel Mode on.

```
key chain KC macsec
key 1000
  cryptographic-algorithm aes-128-cmac
  key-string FC8F5B10557C192F03F60198413D7D45
end

mka policy POLICY
  key-server priority 0
  macsec-cipher-suite gcm-aes-128
  confidentiality-offset 0
end

interface Te1/0/1
  channel-group 2 mode on
  macsec
  mka policy POLICY
  mka pre-shared-key key-chain KC
end

interface Te1/0/2
  channel-group 2 mode on
  macsec
  mka policy POLICY
  mka pre-shared-key key-chain KC
end
```

Layer 2 EtherChannel Configuration

Device 1

```
interface port-channel 2
  switchport
  switchport mode trunk
  no shutdown
end
```

Device 2

```
interface port-channel 2
  switchport
  switchport mode trunk
  no shutdown
end
```

The following shows a sample output of `show etherchannel summary` command.

Flags:  D - down     P - bundled in port-channel
         I - stand-alone  S - suspended
         H - Hot-standby (LACP only)
         R - Layer3     S - Layer2
         U - in use     F - failed to allocate aggregator

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

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

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Po2(RU)</td>
<td>-</td>
<td>Te1/0/1(P) Te1/0/2(P)</td>
</tr>
</tbody>
</table>

Layer 3 EtherChannel Configuration

Device 1

```
interface port-channel 2
  no switchport
  ip address 10.25.25.3 255.255.255.0
  no shutdown
end
```

Device 2

```
interface port-channel 2
  no switchport
  ip address 10.25.25.4 255.255.255.0
  no shutdown
end
```

The following shows a sample output of `show etherchannel summary` command.

Flags:  
D - down  
P - bundled in port-channel  
I - stand-alone  
s - suspended  
H - Hot-standby (LACP only)  
R - Layer3  
S - Layer2  
U - in use  
f - failed to allocate aggregator  
M - not in use, minimum links not met  
u - unsuitable for bundling  
w - waiting to be aggregated  
d - default port  
A - formed by Auto LAG  

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

<table>
<thead>
<tr>
<th>Group</th>
<th>Port-channel</th>
<th>Protocol</th>
<th>Ports</th>
</tr>
</thead>
</table>
The following is a sample configuration on Device 1 and Device 2 with EtherChannel Mode as LACP.

```plaintext
cisco
tuple
key chain KC macsec
key 1000
    cryptographic-algorithm aes-128-cmac
    key-string FC8F5B10557C192F03F60198413D7D45
end

mka policy POLICY
key-server priority 0
macsec-cipher-suite gcm-aes-128
confidentiality-offset 0
end

interface Tel/0/1
    channel-group 2 mode active
    macsec
    mka policy POLICY
    mka pre-shared-key key-chain KC
end

interface Tel/0/2
    channel-group 2 mode active
    macsec
    mka policy POLICY
    mka pre-shared-key key-chain KC
end
```

Layer 2 EtherChannel Configuration

Device 1

```plaintext
interface port-channel 2
    switchport
    switchport mode trunk
    no shutdown
end
```

Device 2

```plaintext
interface port-channel 2
    switchport
    switchport mode trunk
    no shutdown
end
```

The following shows a sample output of `show etherchannel summary` command.

Flags: D – down P – bundled in port-channel
I – stand-alone s – suspended
H – Hot-standby (LACP only)
R – Layer3 S – Layer2
U – in use f – failed to allocate aggregator
Example: Configuring MACsec MKA for Port Channel using PSK

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

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

Layer 3 EtherChannel Configuration

Device 1

```plaintext
interface port-channel 2
  no switchport
  ip address 10.25.25.3 255.255.255.0
  no shutdown
end
```

Device 2

```plaintext
interface port-channel 2
  no switchport
  ip address 10.25.25.4 255.255.255.0
  no shut
```

The following shows a sample output of `show etherchannel summary` command.

Flags:  D - down             P - bundled in port-channel
        I - stand-alone          S - suspended
        H - Hot-standby (LACP only)
        R - Layer3             S - Layer2
        U - in use              f - failed to allocate aggregator

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

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

Group  Port-channel  Protocol  Ports
2 Po2(RU) LACP Tel1/1/1(P) Tel1/1/2(P)

Displaying Active MKA Sessions
The following shows all the active MKA sessions.

# show mka sessions interface Tel1/0/1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Local-TxSCI</th>
<th>Policy-Name</th>
<th>Inherited</th>
<th>Key-Server</th>
<th>Port-ID</th>
<th>Peer-RxSCI</th>
<th>MACsec-Peers</th>
<th>Status</th>
<th>CKN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tel1/0/1</td>
<td>00a3.d144.3364/0025</td>
<td>POLICY</td>
<td>NO</td>
<td>37</td>
<td>701f.539b.b0c6/0032</td>
<td>Secured</td>
<td>1000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Examples: Configuring MACsec Cipher Announcement

This example shows how to configure MKA policy for Secure Announcement:

# configure terminal
(config)# mka policy mka_policy
(config-mka-policy)# key-server 2
(config-mka-policy)# send-secure-announcements
(config-mka-policy)#macsec-cipher-suite gcm-aes-128 confidentiality-offset 0
(config-mka-policy)# end

This example shows how to configure Secure Announcement globally:

# configure terminal
(config)# mka defaults policy send-secure-announcements
(config)# end

This example shows how to configure EAPoL Announcements on an interface:

# configure terminal
(config)# interface GigabitEthernet 1/0/1
(config-if)# eapol announcement
(config-if)# end

The following is a sample output for show running-config interface interface-name command with EAPoL announcement enabled.

# show running-config interface GigabitEthernet 1/0/1
switchport mode access
macsec
access-session host-mode multi-host
access-session closed
access-session port-control auto
dot1x pae authenticator
dot1x timeout quiet-period 10
dot1x timeout tx-period 5
dot1x timeout supp-timeout 10
dot1x supplicant eap profile peap
eapol announcement
spanning-tree portfast
service-policy type control subscriber Dot1X

The following is a sample output of the `show mka sessions interface interface-name detail` command with secure announcement disabled.

```
# show mka sessions interface GigabitEthernet 1/0/1 detail

MKA Detailed Status for MKA Session
====================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI............. 204C.9E85.ED84/002b
Interface MAC Address.... 204C.9E85.ED84
MKA Port Identifier...... 43
Interface Name.......... GigabitEthernet1/0/1
Audit Session ID........
CAK Name (CKN).......... 0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBE05D5D67594543CEAE
Message Number (MN)..... 89567
EAP Role................ NA
Key Server............... YES
MKA Cipher Suite......... AES-128-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............. 0
Latest SAK KI (KN)........ D46CBE05D5D67594543CEA00000001 (1)
Old SAK Status........... FIRST-SAK
Old SAK AN............... 0
Old SAK KI (KN)........... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time......... 0s (No Old SAK to retire)

MKA Policy Name.......... p2
Key Server Priority...... 2
Delay Protection......... NO
Replay Protection........ YES
Replay Window Size....... 0
Confidentiality Offset... 0
Algorithm Agility........ 80C201
Send Secure Announcement.. DISABLED
SAK Cipher Suite......... 0080C20010000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired.......... YES

# of MACsec Capable Live Peers.......... 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
The following is a sample output of the `show mka sessions details` command with secure announcement disabled.

```plaintext
# show mka sessions details
MKA Detailed Status for MKA Session

Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI............. 204c.9e85.ede4/002b
Interface MAC Address.... 204c.9e85.ede4
MKA Port Identifier...... 43
Interface Name........... GigabitEthernet1/0/1
Audit Session ID..........
CAK Name (CKN)...........
0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5D67594543CEAE
Message Number (MN)...... 89572
EAP Role.................. NA
Key Server............... YES
MKA Cipher Suite......... AES-128-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............. 0
Latest SAK KI (KN)....... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status........... FIRST-SAK
Old SAK AN................. 0
Old SAK KI (KN).......... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)

MKA Policy Name.......... p2
Key Server Priority...... 2
Delay Protection.......... NO
Replay Protection........ YES
Replay Window Size....... 0
Confidentiality Offset... 0
Algorithm Agility......... 80C201
Send Secure Announcement.. DISABLED
SAK Cipher Suite......... 0080C200010000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
```
MACsec Desired........... YES

# of MACsec Capable Live Peers........... 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:

<table>
<thead>
<tr>
<th>MI</th>
<th>MN</th>
<th>Rx-SCI (Peer)</th>
<th>KS Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>38046BA37D7DA77E06D006A9</td>
<td>89560</td>
<td>c800.8459.e764/002a</td>
<td>10</td>
</tr>
</tbody>
</table>

Potential Peers List:

<table>
<thead>
<tr>
<th>MI</th>
<th>MN</th>
<th>Rx-SCI (Peer)</th>
<th>KS Priority</th>
</tr>
</thead>
</table>

Dormant Peers List:

<table>
<thead>
<tr>
<th>MI</th>
<th>MN</th>
<th>Rx-SCI (Peer)</th>
<th>KS Priority</th>
</tr>
</thead>
</table>

The following is a sample output of the `show mka policy policy-name detail` command with secure announcement disabled.

```
# show mka policy p2 detail
MKA Policy Configuration ("p2")
==========================================
MKA Policy Name....... p2
Key Server Priority.... 2
Confidentiality Offset. 0
Send Secure Announcement..DISABLED
Cipher Suite(s)........ GCM-AES-128

Applied Interfaces...
  GigabitEthernet1/0/1
```

**Support for Routed Ports**

A routed port is a physical port that acts like a port on a router. It does not have to be connected to a router. A routed port is not associated with a particular VLAN, as is an access port. A routed port behaves like a regular router interface, except that it does not support VLAN sub interfaces. Routed ports can be configured with a Layer 3 routing protocol. A routed port is a Layer 3 interface only and does not support Layer 2 protocols, such as STP. A routed interface that is an L3 interface will not be part of any vlan.

**Note**: Both IPv4 and IPv6 addresses can be configured on a Routed Port.

Interface can be modified from L2 to L3 mode using the CLI `no switchport` under interface configuration. Then assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the `ip routing` and `router protocol` global configuration commands.

**Note**: Entering a `no switchport interface` configuration command shuts down the interface and then re-enables it. This may generate messages on the device to which the interface is connected. Modifying an interface from L2 to L3 mode, the L2 configuration will be erased.
With respect to CIP, the IPv4 routing info will be added to the switch parameters object and the IPv4 routing object will be added.

**Command Line Interface**

The following is an example of the CLI:

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet1/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.20.135.21 255.255.255.0
```

**Feature Restrictions**

- Port channel is supported using L3 interfaces. The options are LACP (active and passive) and ON mode.
- SNMP MIB is not supported.
- OSPF is supported on port channel of type LACP and ON mode.
- No change in L3 route scale.

**USB Support**

Most IoT switches have USB 2.0 Type A connectors. These ports can be used for USB sticks and a Bluetooth dongle. They are not to be used in hazardous locations. Each USB port can provide a maximum current of 500mA at 5V, with 600mA total available for both ports. USB flash drives will only support the VFAT file system. There is no maximum limit for the USB flash to work in any of the platforms.

USB flash supports the data storage in IMSP. Data can be copied to/from the USB to the device. Booting a device with the image in the USB is not supported in release 16.12. Typically, the device will take 6 to 7 seconds to detect the USB after it is inserted.

USB hub and USB card reader support is not available. Support is only available for the USB stick which has the flash memory integrated in it.

**Layer 3 ACL Support**

Access control lists (ACLs) provide the ability to filter ingress and egress traffic based on security policy specified. Each ACL consists of one or more number of rules. Each rule is referred to as an Access Control Entry (ACE). Each ACE defines the rule to classify a packet and an action to be performed if the packet matches this classification. The rules of classification typically describe the packet fields to match on, and the action is either 'permit' or 'deny'. The semantics of the action may vary depending upon the type of security ACL. Layer 3 ACLs refer to providing security based on the packet's L3 and L4 fields.

The switch supports port based ACL for non-ip, ipv4 and ipv6 traffic types, and therefore covers requirements of L3-ACL. What is not supported is handling of PACL upon switchport configuration toggling.
When a port's mode is changed from switchport to no-switchport and vice-versa, applied ACLs will be moved to non-operational mode.

VACL rules are applied on per vlan basis in TCAM. This requires additional support from ASIC vendor. A packet ingresses switch with a vlan-id and may get a new vlan-id based on forwarding. For VACL support, regardless of whether packet ingressed with that vlan-id or received the vlan-id as part of forwarding, it matches filter rules when the packet enters that vlan-id.

**Support Details**

- VACL is not supported on the SVI interface.
- When VACL and PACL both are applicable for a packet, PACL takes precedence over VACL, and VACL is not applied in such a case.
- There is a maximum of 255 aces per VACL.
- There is no explicit limit on total VLANs defined, because TCAM is not present in components. Whenever enough space in TCAM isn’t available to accept the new configuration, an error is sent to syslog.
- Logging not supported on egress ACL.
- On L3-ACL, non-ip ACL is not supported.

**Resilient Ethernet Protocol (REP) Preferred**

Note

REP Preferred only works on uplink ports.

REP and Spanning Tree Protocol (STP) are two different loop avoidance protocols. REP has certain advantages over STP in terms of convergence time. REP can be configured to run in a ring topology in such a way that it can provide the redundant path in case of a single link failure in the ring.

Cisco switches are by default STP enabled. If a switch that is STP enabled is inserted in the already running REP ring (for addition of a new node or replacement of existing node) the following conditions apply:

- The new switch will cause a break in the REP ring.
- The new switch will not be able to communicate over the ring until it is configured to be part of the REP ring.

REP Preferred feature tries to solve these issues, by negotiating the REP status with the peers according to the following table:

<table>
<thead>
<tr>
<th>SELF REP Negotiated</th>
<th>PEERS REP Negotiated</th>
<th>Event Triggered</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
<td>True</td>
<td>REPN</td>
<td>Configure REP</td>
</tr>
<tr>
<td>True</td>
<td>False</td>
<td>REPNN</td>
<td>Configure STP</td>
</tr>
<tr>
<td>False</td>
<td>X</td>
<td>REPNN</td>
<td>Remain in STP</td>
</tr>
</tbody>
</table>
This feature depends on 3 different protocols to get the required data and decide the correct configuration. The different protocols involved, and their purpose is given below:

- **STP**: By default, STP is enabled on all the ports on the Cisco Switch.
- **REP**: The customer network is configured to form a REP ring to provide better convergence time and redundancy.
- **Cisco Discovery Protocol (CDP)**: The feature depends on user defined TLVs sent through CDP messages to negotiate the correct (STP or REP) configuration for the interface.

### Configuring a REP Interface

To configure REP, enable REP on each segment interface and identify the segment ID. This task is mandatory, and must be done before other REP configurations. You must also configure a primary and secondary edge port on each segment. All the other steps are optional.

Follow these steps to enable and configure REP on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface interface-id</td>
<td>Specifies the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface)</td>
</tr>
<tr>
<td>3</td>
<td>switchport mode trunk</td>
<td>Configures the interface as a Layer 2 trunk port.</td>
</tr>
</tbody>
</table>
### Configuring a REP Interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 4    | `rep segment segment-id [edge [no-neighbor ] [primary ]][preferred ]` | Enables REP on the interface and identifies a segment number. The segment ID range is from 1 to 1024.  
**Note:** You must configure two edge ports, including one primary edge port, for each segment.  
These optional keywords are available:  
(Optional) `edge` — Configures the port as an edge port. Each segment has only two edge ports. Entering the keyword edge without the keyword primary configures the port as the secondary edge port.  
(Optional) `primary` — Configures the port as the primary edge port, the port on which you can configure VLAN load balancing.  
(Optional) `no-neighbor` — Configures a port with no external REP neighbors as an edge port. The port inherits all the properties of an edge port, and you can configure the properties the same way you would for an edge port.  
**Note:** Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the keyword primary on both the switches, the configuration is valid. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by entering the `show rep topology` command in privileged EXEC mode.  
(Optional) `preferred` — Indicates that the port is the preferred alternate port or the preferred port for VLAN load balancing.  
**Note:** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives the port a slight edge over equal contenders. The alternate port is usually a previously failed port. |
| 5    | `rep stcn {interface interface-id | segment id-list | stp }` | (Optional) Configures the edge port to send segment topology change notices (STCNs).  
**interface interface-id** — Designates a physical interface or port channel to receive STCNs.  
**segment id-list** — Identifies one or more segments to receive STCNs. The range is from 1 to 1024.  
**stp** — Sends STCNs to STP networks.  
**Note:** Spanning Tree (MST) mode is required on edge no-neighbor nodes when `rep stcn stp` command is configured for sending STCNs to STP networks. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 6    | rep block port {id port-id | neighbor-offset | preferred } vlan {vlan-list | all } | (Optional) Configures VLAN load balancing on the primary edge port, identifies the REP alternate port in one of three ways (id port-id, neighbor_offset, preferred), and configures the VLANs to be blocked on the alternate port.  
  
  **id port-id** — Identifies the alternate port by port ID. The port ID is automatically generated for each port in the segment. You can view interface port IDs by entering the show interface type number rep [detail] privileged EXEC command.  
  
  **neighbor_offset** — Number to identify the alternate port as a downstream neighbor from an edge port. The range is from -256 to 256, with negative numbers indicating the downstream neighbor from the secondary edge port. A value of 0 is invalid. Enter -1 to identify the secondary edge port as the alternate port.  
  
  **preferred** — Selects the regular segment port previously identified as the preferred alternate port for VLAN load balancing.  
  
  **vlan vlan-list** — Blocks one VLAN or a range of VLANs.  
  
  **vlan all** — Blocks all the VLANs.  
  
  **Note:** Because you enter the rep block port command at the primary edge port (offset number 1), you cannot enter an offset value of 1 to identify an alternate port. |
| 7    | rep preempt delay seconds | (Optional) Configures a preempt time delay.  
  
  Use this command if you want VLAN load balancing to be automatically triggered after a link failure and recovery.  
  
  The time delay range is between 15 to 300 seconds. The default is manual preemption with no time delay.  
  
  **Note:** Enter this command only on the REP primary edge port. |
| 8    | rep isl-age-timer value | (Optional) Configures a time (in milliseconds) for which the REP interface remains up without receiving a hello from a neighbor.  
  
  The range is from 120 to 10000 ms in 40-ms increments. The default is 5000 ms (5 seconds).  
  
  **Note:** EtherChannel port channel interfaces do not support LSL age-timer values that are less than 1000 ms.  
  
  Both the ports on the link should have the same LSL age configured in order to avoid link flaps. |
| 9    | end | Returns to privileged EXEC mode. |
| 10   | show interface [interface-id] rep [detail] | (Optional) Displays the REP interface configuration. |
Parallel Redundancy Protocol (PRP) Support

Parallel Redundancy Protocol (PRP) support is introduced in 16.12.1 release as per IEC 62439-3 Edition 3.0 on Advanced IE3400 switches running IOS-XE. PRP functionality on IE3400 is in parity with IE4000 switches running latest classic IOS software with respect to configuration, scale of Node Table (512), VDAN table (512) per PRP channel and also supported interface combinations for PRP Channel 1 and 2.

- PRP-Channel 1: GigabitEthernet1/1 (LAN-A) and GigabitEthernet1/2 (LAN-B)
- PRP-Channel 2: GigabitEthernet1/3 (LAN-A) and GigabitEthernet1/3 (LAN-B)

For more information about PRP, Command Line Interface and configuration examples, Please refer to: https://www.cisco.com/c/en/us/td/docs/switches/lan/industrial/software/configuration/guide/b_prp_ie4k_5k.html

PRP functionality can be managed using CIP protocol and the following CIP Command line interface for PRP is available on IE3400:

- `show cip object prp <0-2>`
- `show cip object nodetable <0-2>`

Limitations:
- IE3400 does not have a separate PRP/HSR mode LED on the switches unlike IE4000
- PRP is not supported on IE3200 and IE3300 series of switches

Licensing:
PRP functionality works with both Network-Essentials and Network-Advantage Licenses

Precision Time Protocol (PTP) Enhancements

Network Time Protocol (NTP) is the traditional method of synchronizing clocks across packet-based networks. NTP uses a two-way time transfer mechanism, between a master and a slave. NTP is capable of synchronizing a device within a few 100 milliseconds across the internet, and within a few milliseconds in a tightly controlled LAN. IOS-XE currently implements an NTP stack which also controls the OS clock time. However, the generic NTP stack cannot source TAI time to other protocols.

Precision Time Protocol (PTP) is a time transfer protocol designed to improve the precision of NTP. There is an increased requirement for more precise time synchronization protocol than NTP in various environments like Industrial Ethernet, Telecommunications, Power generation, Transmission and distribution systems, etc. PTP uses hardware timestamps, new clock types, and new timing algorithms to achieve sub-microsecond precision. All IoT IE series platforms currently support PTP.
PTP Use Case

NTP to PTP Time Conversion is an industry wide requirement, and our most requested time service feature. In most cases, the use of GPS or atomic clock as PTP sources is not available. NTP can be used by the IE3x00 and ESS3300 switches as a reference clock source in place of other sources to drive the PTP time source for the network. While NTP is not as precise as GPS, it is more robust to malicious attacks and does not experience the same kinds of outages.

Feature Details

Users can configure PTP in Grandmaster clock mode (gmc-bc mode). Once configured in such a mode:

- The switch will behave as a Grandmaster clock as per IEEE 1588v2.
- If time is available via NTP (i.e., if the switch is an NTP client), the switch will source time via NTP and convert it to PTP to synchronize its PTP Slaves.
- If time is not available via NTP, the switch will source time from its local clock and convert it to PTP to synchronize its PTP Slaves.

Note: There is no hardware support for GPS on the switch and therefore GPS to PTP time conversion is not supported on the platform.

Details on configuring PTP can be found in the System Management Configuration Guide for the ESS3300 Switches.

Information About MRP

MRP, defined in International Electrotechnical Commission (IEC) standard 62439-2, provides fast convergence in a ring network topology for Industrial Automation networks. MRP Media Redundancy Manager (MRM) defines its maximum recovery times for a ring in the following range: 10 ms, 30 ms, 200 ms and 500 ms.

Note: The term switch refers to the IE3x00 unless otherwise noted. There is no support for MRP on the ESS3300 Switch.

MRP operates at the MAC layer and is commonly used in conjunction with the PROFINET standard for industrial networking in manufacturing.

Configuring MRP CLI Mode

To configure MRP on the IE3x00, configure the node as MRM or MRC, and specify the two MRP ports. There is no restriction related to licensing, except that with client license, Manager is not allowed.

The following CLI is used to configure the feature license:

```
Device(config)#platform license feature 
mrp-client mrp-manager
```

The following MRP configuration parameters are optional except for domain-id, which is required for multiple MRP rings, and priority, which is used for MRP on the IE3x00:
• domain-id—A unique ID that represents the MRP ring.
• domain-name—Logical name of the configured MRP domain-ID.
• profile—200 ms
• vlan-id—VLAN for sending MRP frames.
• default—in global MRP configuration, sets the mode to client.

Configuring MRP Manager

Follow this procedure to configure the IE3x00 switch.

Note
If the device is connected to a PLC module, please make sure “no device in the ring” is selected for MRP.

SUMMARY STEPS

1. Enter configuration mode:
2. Enable MRP:
3. Configure MRP manager mode:
4. (Optional for single MRP ring) Configure the domain ID:
5. (Optional for single MRP ring) Configure the domain name:
6. (Optional) Configure the VLAN ID:
7. (Optional) Configure the recovery profile:
8. On the switch configure the MRP priority:
9. Return to privileged EXEC mode:
10. Enter configuration mode:
11. Specify the ID of the port that serves as the first ring port:
12. Configure the interface mode:
13. Associate the interface to the MRP ring:
14. Return to global configuration mode:
15. Specify the ID of the port that serves as second ring port:
16. Configure the interface mode:
17. Associate the interface to the MRP ring:
18. Return to privileged EXEC mode:
19. (For multiple rings) Repeat step 2 through 15 for each additional ring:

DETAILED STEPS

Step 1
Enter configuration mode:

configure terminal

Step 2
Enable MRP:

mrp ring 1
Step 3 Configure MRP manager mode:

```
mode manager
```

Step 4 (Optional for single MRP ring) Configure the domain ID:

```
domain-id value
```

`value` — UUID string of 32 hexadecimal digits in five groups separated by hyphens

Example: 550e8400-e29b-41d4-a716-446655440000

The default domain ID for ring 1 is FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFF.

Step 5 (Optional for single MRP ring) Configure the domain name:

```
domain-name name
```

`name` — String of up to 32 characters

Step 6 (Optional) Configure the VLAN ID:

```
 vlan-id vlan
```

Step 7 (Optional) Configure the recovery profile:

```
profile {200 | 500}
```

- 200 — Maximum recovery time 200 milliseconds
- 500 — Maximum recovery time 500 milliseconds

Step 8 On the switch configure the MRP priority:

```
priority value
```

`value` — Range: `<0-32768>`. The default priority is 32768.

Step 9 Return to privileged EXEC mode:

```
end
```

Step 10 Enter configuration mode:

```
configure terminal
```

Step 11 Specify the ID of the port that serves as the first ring port:

```
interface port
```

Step 12 Configure the interface mode:

```
switchport mode { access | trunk }
```

**Note** You must specify `switchport mode access` when configuring MRP in access mode.

Step 13 Associate the interface to the MRP ring:

```
mrp ring 1
```

Step 14 Return to global configuration mode:
Step 15 Specify the ID of the port that serves as second ring port:

interface port

Step 16 Configure the interface mode:

switchport mode \{ access | trunk \}

Note You must specify switchport mode access at this step when configuring MRP in access mode.

Step 17 Associate the interface to the MRP ring:

mrp ring 1

Step 18 Return to privileged EXEC mode:

end

Step 19 (For multiple rings) Repeat step 2 through 15 for each additional ring:

• Assign ring number 2 for the second ring.
• Assign a unique domain ID for Ring 2. The default domain ID for ring 2 is FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFE.
• Assign ring number 3 for the third ring.
• Assign a unique domain ID for Ring 3. The default domain ID for ring 3 is FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFD.

Note Each ring should have its own domain ID. No two rings share the same domain ID.

Example

The following example shows configuring MRP manager:

```bash
Switch# configure terminal
Switch# no profinet mrp
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# mrp ring 1
Switch(config-mrp)# mode-manager
Switch(config-mrp-manager)# domain-id FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF
Switch(config-mrp-manager)# priority 32768
Switch(config-mrp-manager)# end
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# GigabitEthernet1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown all interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)# exit
Switch(config)# GigabitEthernet1/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown all interfaces which are not currently in use to prevent potential bridging loops.
```
interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)#exit
Switch(config-if)#end

Switch# show mrp ring 1
MRP ring 1
Profile : 200 ms
Mode : Manager
Priority : 32768
Operational Mode: Client
From : CLI
License : Active
Best Manager :
MAC Address : 00:78:88:5E:03:81
Priority : 36864

Network Topology: Ring
Network Status : OPEN
Port1: Port2:
MAC Address :84:B8:02:ED:E8:02 MAC Address :84:B8:02:ED:E8:01
Interface :GigabitEthernet1/2 Interface :GigabitEthernet1/1
Status :Forwarding Status :Forwarding

VLAN ID : 1
Domain Name : Cisco MRP Ring 1
Domain ID : FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF

Topology Change Request Interval : 10ms
Topology Change Repeat Count : 3
Short Test Frame Interval : 10ms
Default Test Frame Interval : 20ms
Test Monitoring Interval Count : 3
Test Monitoring Extended Interval Count : N/A
Switch#show mrp ports

Ring ID : 1
PortName Status
--------------------------------------
GigabitEthernet1/2 Forwarding
GigabitEthernet1/1 Forwarding

Configuring MRP Client

Follow this procedure to configure the switch as an MRP Client.

SUMMARY STEPS

1. Enter configuration mode:
2. Enable MRP:
3. Configure MRP client mode (if you do not specify the mode, client mode is the default):
4. (Optional) Configure the domain ID matching the one configured for this ring on MRM (Step 4 in Configuring MRP Manager, on page 50):
5. Return to privileged EXEC mode:
6. Enter configuration mode:
7. Specify the ID of the port that serves as the first ring port:
8. Configure the interface mode:
9. Associate the interface to the MRP ring:
10. Return to global configuration mode:
11. Specify the ID of the port that serves as second ring port:
12. Configure the interface mode:
13. Associate the interface to the MRP ring:
14. Return to privileged EXEC mode:

**DETAILED STEPS**

**Step 1**
Enter configuration mode:

```
configure terminal
```

**Step 2**
Enable MRP:

```
mrp ring 1
```

**Step 3**
Configure MRP client mode (if you do not specify the mode, client mode is the default):

```
mode client
```

**Step 4**
(Optional) Configure the domain ID matching the one configured for this ring on MRM (Step 4 in Configuring MRP Manager, on page 50):

```
domain-id value
```

*value* — UUID string of 32 hexadecimal digits in five groups separated by hyphens

Example: 550e8400-e29b-41d4-a716-446655440000

The default domain ID for ring 1 is FFFFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF.

**Step 5**
Return to privileged EXEC mode:

```
end
```

**Step 6**
Enter configuration mode:

```
configure terminal
```

**Step 7**
Specify the ID of the port that serves as the first ring port:

```
interface port
```

**Step 8**
Configure the interface mode:

```
switchport mode { access | trunk }
```

*Note* You must specify `switchport mode access` when configuring MRP in access mode.

**Step 9**
Associate the interface to the MRP ring:

```
mrp ring 1
```

**Step 10**
Return to global configuration mode:

```
exit
```

**Step 11**
Specify the ID of the port that serves as second ring port:
**interface** port

**Step 12** Configure the interface mode:
```
switchport mode { access | trunk }
```

**Note** You must specify `switchport mode access` when configuring MRP in access mode.

**Step 13** Associate the interface to the MRP ring:
```
mrp ring 1
```

**Step 14** Return to privileged EXEC mode:
```
end
```

---

**Example**

The following example shows configuring MRP client:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# mrp ring 1
Switch(config-mrp)# mode client
Switch(config-mrp-client)# end
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gi1/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# mrp ring 1
Switch(config-if)# exit
Switch(config)# interface gi1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# mrp ring 1
Switch(config-if)# exit
Switch(config)#
```

```
Switch# show mrp ring
MRP ring 1
Mode : Client
From : CLI
License : Active
Best Manager : 
MAC Address : Unknown
Priority : Unknown
Network Topology: Ring
Network Status : Unknown
Port1: Port2:
MAC Address :30:F7:0D:68:07:81 MAC Address :30:F7:0D:68:07:82
Interface :GigabitEthernet1/1 Interface :GigabitEthernet1/2
Status :Forwarding Status :Forwarding
VLAN ID : 1
Domain Name : Cisco MRP Ring 1
Domain ID : FFFFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF
Link Down Timer Interval : 20 ms
Link Up Timer Interval : 20 ms
```
Link Change (Up or Down) count: 4 ms
MRP ring 2 not configured
MRP ring 3 not configured

Configuring MRP Client
Infoomation About L2 Network Address Translation (NAT)

One-to-one (1:1) Layer 2 NAT is a service that allows the assignment of a unique public IP address to an existing private IP address (end device), so that the end device can communicate on both the private and public subnets. This service is configured in a NAT-enabled device and is the public “alias” of the IP address physically programmed on the end device. This is typically represented by a table in the NAT device.

Layer 2 NAT has two translation tables where private-to-public and public-to-private subnet translations can be defined. Layer 2 NAT is a hardware based implementation that provides the same high level of (bump-on-the-wire) wire-speed performance. This implementation also supports multiple VLANs through the NAT boundary for enhanced network segmentation.

In the following example, Layer 2 NAT translates addresses between sensors on a 192.168.1.x network and a line controller on a 10.1.1.x network.

1. The 192.168.1.x network is the inside/internal IP address space and the 10.1.1.x network is the outside/external IP address space.
2. The sensor at 192.168.1.1 sends a ping request to the line controller by using an “inside” address, 192.168.1.100.
3. Before the packet leaves the internal network, Layer 2 NAT translates the source address (SA) to 10.1.1.1 and the destination address (DA) to 10.1.1.100.
4. The line controller sends a ping reply to 10.1.1.1.
5. When the packet is received on the internal network, Layer 2 NAT translates the source address to 192.168.1.100 and the destination address to 192.168.1.1.
For large numbers of nodes, you can quickly enable translations for all devices in a subnet. In the scenario shown in the following figure, addresses from Inside Network 1 can be translated to outside addresses in the 10.1.1.0/28 subnet, and addresses from Inside Network 2 can be translated to outside addresses in the 10.1.1.16/28 subnet. All addresses in each subnet can be translated with one command.
The following figure shows an IE 3400 NAT configuration at the distribution level. In this example, the IE 3400 connects to devices in the private network through Catalyst 2960 switches. The Catalyst switches at the access layer are not performing NAT. The IE 3400 is performing L2 NAT on two interfaces for two different access switches. The IE switches are capable of supporting 128 instances of L2 NAT. In this example, only three of the 128 are shown. An entire subnet can be configured in a single L2 NAT instance.
Figure 5: NAT on the IE 3400

The IE 3400 NAT configuration for the diagram shown in the figure above is as follows:

Instance 10:
- inside from network 192.168.0.0 to 10.10.10.0 mask 255.255.255.0
- outside from host 10.10.10.254 to 192.168.9.254 gateway

Instance 11:
- inside from network 192.168.0.0 to 10.10.11.0 mask 255.255.255.0
- outside from host 10.10.11.254 to 192.168.9.254 gateway

Interface vlan 10
- ip address 10.10.10.254 mask 255.255.255.0

Interface vlan 11
- ip address 10.10.11.254 mask 255.255.255.0

Interface gig 1/1
- switchport access vlan 10
- l2nat instance 10

Interface gig 1/2
- switchport access vlan 11
- l2nat instance 11

- Prerequisites, on page 61
- Guidelines and Limitations, on page 61
- Default Settings, on page 61
- Configuring Layer 2 NAT, on page 62
- Verifying Configuration, on page 63
- Basic Inside-to-Outside Communications Example, on page 64
- Duplicate IP Addresses Example, on page 65
- Related Documents, on page 68
- Feature History, on page 68
Prerequisites

- IE 3300—L2NAT feature is supported only on uplink ports (Gig 1/1 and Gig 1/2) and available in both (essential and advantage) licenses.

- IE 3400—L2NAT feature is supported only on uplink ports (Gig 1/1 and Gig 1/2) and available in both (essential and advantage) licenses.

Guidelines and Limitations

- Only IPv4 addresses can be translated.

- Layer 2 NAT applies only to unicast traffic. You can permit or allow untranslated unicast traffic, multicast traffic, and IGMP traffic.

- Layer 2 NAT does not support one-to-many and many-to-one IP address mapping.

- Layer 2 NAT supports one-to-one mapping between external and internal IP addresses.

- Layer 2 NAT cannot save on public IP addresses.

- If you configure a translation for a Layer 2 NAT host, do not configure it as a DHCP client.

- Certain protocols such as ARP and ICMP do not work transparently across Layer 2 NAT but are “fixed up” by default. “Fixed up” means that changes are made to IP addresses embedded in the payload of IP packets for the protocols to work.

- The downlink port can be VLAN, trunk, or Layer 2 channel.

- You can configure 128 Layer 2 NAT instances on the switch.

- Up to 128 VLANs are allowed to have Layer 2 NAT configuration.

- The management interface is behind the Layer 2 NAT function. Therefore this interface should not be on the private network VLAN. If it is on the private network VLAN, assign an inside address and configure an inside translation.

- Because L2NAT is designed to separate outside and inside addresses, we recommend that you do not configure addresses of the same subnet as both outside and inside addresses.

- The interfaces that support NAT instance configurations are as follows:
  - IE-3300 and IE3400: Gig 1/1 and Gig 1/2 (uplinks)

Default Settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit or drop packets for unmatched traffic and traffic types that are not configured to be translated</td>
<td>Drop all unmatched, multicast, and IGMP packets</td>
</tr>
</tbody>
</table>
### Configuring Layer 2 NAT

You need to configure Layer 2 NAT instances that specify the address translations. Then you attach these instances to interfaces and VLANs. For unmatched traffic and traffic types that are not configured to be translated, you can choose to permit or drop the traffic. Layer 2 NAT instances can be configured from management interfaces (CLI/SNMP/CIP/WebUI). You can view detailed statistics about the packets sent and received (see Verifying Configuration, on page 63).

To configure Layer 2 NAT, follow these steps. Refer to the examples in Basic Inside-to-Outside Communications Example, on page 64 and Duplicate IP Addresses Example, on page 65 for more details.

#### SUMMARY STEPS

1. Enter global configuration mode:
   ```
   configure terminal
   ```
2. Create a new Layer 2 NAT instance:
   ```
   l2nat instance instance_name
   ```
   After creating an instance, you use this same command to enter the sub-mode for that instance.
3. Translate an inside address to an outside address:
   ```
   inside from [host | range | network ] original ip to translated ip [mask ] number | mask
   ```
   You can translate a single host address, a range of host addresses, or all of the addresses in a subnet. Translate the source address for outbound traffic and the destination address for inbound traffic.
4. Translate an outside address to an inside address:

#### DETAILED STEPS

**Step 1**

Enter global configuration mode:

```
configure terminal
```

**Step 2**

Create a new Layer 2 NAT instance:

```
l2nat instance instance_name
```
**Information About L2 Network Address Translation (NAT)**

Outside from

```
outside from [host | range | network ] original ip to translated ip [mask ] number | mask
```

You can translate a single host address, a range of host addresses, or all of the addresses in a subnet. Translate the destination address for outbound traffic and the source address for inbound traffic.

**Step 5**

Fix the translation for ICMP and IGMP through NAT translation. By default, fixups for both ARP and ICMP are enabled, so this command is not normally needed unless you change the defaults.

```
fixup arp | icmp | all
```

**Note** For ICMP, only fixups for ICMP Error messages are supported.

**Step 6**

(Optional) Permit untranslated unicast traffic (it is dropped by default):

```
permit { multicast | igmp | all }
```

**Step 7**

Exit config-l2nat mode:

```
exit
```

**Step 8**

Access interface configuration mode for the specified interface (uplink ports only on the IE 3400):

```
interface interface-id
```

**Step 9**

Apply the specified Layer 2 NAT instance to a VLAN or VLAN range. If this parameter is missing, the Layer 2 NAT instance applies to the native VLAN.

```
l2nat instance_name [vlan | vlan_range]
```

**Step 10**

Exit interface configuration mode:

```
end
```

---

**Verifying Configuration**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show l2nat instance</td>
<td>Displays the configuration details for a specified Layer 2 NAT instance.</td>
</tr>
<tr>
<td>show l2nat interface</td>
<td>Displays the configuration details for Layer 2 NAT instances on one or more interfaces.</td>
</tr>
<tr>
<td>show l2nat statistics</td>
<td>Displays the Layer 2 NAT statistics for all interfaces.</td>
</tr>
<tr>
<td>show l2nat statistics interface</td>
<td>Displays the Layer 2 NAT statistics for a specified interface.</td>
</tr>
<tr>
<td>debug l2nat</td>
<td>Enables showing real-time Layer 2 NAT configuration details when the configuration is applied.</td>
</tr>
</tbody>
</table>
Basic Inside-to-Outside Communications Example

In this scenario, A1 needs to communicate with a logic controller (LC) that is directly connected to the uplink port. An Layer 2 NAT instance is configured to provide an address for A1 on the outside network (10.1.1.1) and an address for the LC on the inside network (192.168.1.250).

Figure 6: Basic Inside-to-Outside Communications

Now this communication can occur:

2. Cisco Switch A fixes up the ARP request: SA: 10.1.1.1DA: 10.1.1.200.
3. LC receives the request and learns the MAC Address of 10.1.1.1.
6. A1 learns the MAC address for 192.168.1.250, and communication starts.

Note

The management interface of the switch must be on a different VLAN from the inside network 192.168.1.x.

The following table shows the configuration tasks for this scenario. The Layer 2 NAT instance is created, two translation entries are added, and the instance is applied to the interface. ARP fixups are enabled by default.

Table 3: Configuration of Cisco Switch A for Basic Inside-to-Outside Example

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Switch# configure</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Command | Purpose
--- | ---
2. Switch(config)# l2nat instance A-LC | Creates a new Layer 2 NAT instance called A-LC.
3. Switch(config-l2nat)# inside from host 192.168.1.1 to 10.1.1.1 | Translates A1’s inside address to an outside address.
4. Switch(config-l2nat)# inside from host 192.168.1.2 to 10.1.1.2 | Translates A2’s inside address to an outside address.
5. Switch(config-l2nat)# inside from host 192.168.1.3 to 10.1.1.3 | Translates A3’s inside address to an outside address.
6. Switch(config-l2nat)# outside from host 10.1.1.200 to 192.168.1.250 | Translates LC’s outside address to an inside address.
7. Switch(config-l2nat)# exit | Exits config-l2nat mode.
8. Switch(config)# interface Gi1/1 | Accesses interface configuration mode for the uplink port.
9. Switch(config-if)# l2nat A-LC | Applies this Layer 2 NAT instance to the native VLAN on this interface.  
**Note** For tagged traffic on a trunk, add the VLAN number when attaching the instance to an interface as follows:  
l2nat instance vlan
10. Switch# end | Returns to privileged EXEC mode.

### Duplicate IP Addresses Example

In this scenario, two machine nodes are preconfigured with addresses in the 192.168.1.x space. Layer 2 NAT translates these addresses to unique addresses on separate subnets of the outside network. In addition, for machine-to-machine communications, the Node A machines need unique addresses on the Node B space and the Node B machines need unique addresses in the Node A space.
Figure 7: Duplicate IP Addresses

- Switch C needs an address in the 192.168.1.x space. When packets come into Node A or Node B, the 10.1.1.254 address of Switch C is translated to 192.168.1.254. When packets leave Node A or Node B, the 192.168.1.254 address of Switch C is translated to 10.1.1.254.

- Node A and Node B machines need unique addresses in the 10.1.1.x space. For quick configuration and ease of use, the 10.1.1.x space is divided into subnets: 10.1.1.0, 10.1.1.16, 10.1.1.32, and so on. Each subnet can then be used for a different node. In this example, 10.1.1.16 is used for Node A, and 10.1.1.32 is used for Node B.

- Node A and Node B machines need unique addresses to exchange data. The available addresses are divided into subnets. For convenience, the 10.1.1.16 subnet addresses for the Node A machines are translated to 192.168.1.16 subnet addresses on Node B. The 10.1.1.32 subnet addresses for the Node B machines are translated to 192.168.1.32 addresses on Node A.

- Machines have unique addresses on each network:

Table 4: Translated IP Addresses

<table>
<thead>
<tr>
<th>Node</th>
<th>Address in Node A</th>
<th>Address in Outside Network</th>
<th>Address in Node B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch A network address</td>
<td>192.168.1.0</td>
<td>10.1.1.16</td>
<td>192.168.1.16</td>
</tr>
<tr>
<td>A1</td>
<td>192.168.1.1</td>
<td>10.1.1.17</td>
<td>192.168.1.17</td>
</tr>
<tr>
<td>A2</td>
<td>192.168.1.2</td>
<td>10.1.1.18</td>
<td>192.168.1.18</td>
</tr>
<tr>
<td>A3</td>
<td>192.168.1.3</td>
<td>10.1.1.19</td>
<td>192.168.1.19</td>
</tr>
</tbody>
</table>
### Table 5: Configuration of Switch A for Duplicate Addresses Example

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Switch(config)# l2nat instance A-Subnet</td>
<td>Creates a new Layer 2 NAT instance called A-Subnet.</td>
</tr>
<tr>
<td>Switch(config-l2nat)# inside from network 192.168.1.0 to 10.1.1.16 mask 255.255.255.240</td>
<td>Translates the Node A machines’ inside addresses to addresses in the 10.1.1.16 255.255.255.240 subnet.</td>
</tr>
<tr>
<td>Switch(config-l2nat)# outside from host 10.1.1.254 to 192.168.1.254</td>
<td>Translates the outside address of Switch C to an inside address.</td>
</tr>
<tr>
<td>Switch(config-l2nat)# outside from network 10.1.1.32 to 192.168.1.32 255.255.255.240</td>
<td>Translates the Node B machines’ outside addresses to their inside addresses.</td>
</tr>
<tr>
<td>Switch(config-l2nat)# exit</td>
<td>Exits config-l2nat mode.</td>
</tr>
<tr>
<td>Switch(config)# interface Gi1/1</td>
<td>Accesses interface configuration mode for the uplink port.</td>
</tr>
<tr>
<td>Switch(config-if)# l2nat A-Subnet</td>
<td>Applies this Layer 2 NAT instance to the native VLAN on this interface. <strong>Note</strong> For tagged traffic on a trunk, add the VLAN number when attaching the instance to an interface as follows: l2nat instance vlan</td>
</tr>
<tr>
<td>Switch# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Table 6: Configuration of Switch B for Subnet Example

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Switch# configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>2. Switch(config)# l2nat instance B-Subnet</td>
<td>Creates a new Layer 2 NAT instance called B-Subnet.</td>
</tr>
<tr>
<td>3. Switch(config-l2nat)# inside from network 192.168.1.0 to 10.1.1.32 255.255.255.240</td>
<td>Translates the Node B machines’ inside addresses to addresses in the 10.1.1.32 255.255.255.240 subnet.</td>
</tr>
<tr>
<td>4. Switch(config-l2nat)# outside from host 10.1.1.254 to 192.168.1.254</td>
<td>Translates the outside address of Switch C to an inside address.</td>
</tr>
<tr>
<td>5. Switch(config-l2nat)# outside from network 10.1.1.16 to 192.168.1.16 255.255.255.240</td>
<td>Translates the Node A machines’ outside addresses to their inside addresses.</td>
</tr>
<tr>
<td>6. Switch(config-l2nat)# exit</td>
<td>Exits config-l2nat mode.</td>
</tr>
<tr>
<td>7. Switch(config)# interface Gi1/1</td>
<td>Accesses interface configuration mode for the uplink port.</td>
</tr>
<tr>
<td>8. Switch(config-if)# l2nat name1</td>
<td>Applies this Layer 2 NAT instance to the native VLAN on this interface.</td>
</tr>
<tr>
<td></td>
<td>Note: For tagged traffic on a trunk, add the VLAN number when attaching the instance to an interface as follows:</td>
</tr>
<tr>
<td></td>
<td>l2nat instance vlan</td>
</tr>
<tr>
<td>9. Switch# show l2nat instance name1</td>
<td>Shows the configuration details for the specified Layer 2 NAT instance.</td>
</tr>
<tr>
<td>10. Switch# show l2nat statistics</td>
<td>Shows Layer 2 NAT statistics.</td>
</tr>
<tr>
<td>11. Switch# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Related Documents

- Cisco Industrial Ethernet 2000 Series Switches Configuration Guides

Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 NAT</td>
<td>IE 3x00 (IE-3300 and IE-3400)</td>
<td>Cisco IOS Release 16.12.1</td>
<td>Initial support</td>
</tr>
</tbody>
</table>
CHAPTER 4

Configuring Precision Time Protocol

- Information About Precision Time Protocol, on page 69
- Information About NTP to PTP Time Conversion, on page 80
- Prerequisites, on page 85
- Guidelines and Limitations, on page 86
- Default Settings, on page 88
- Configuring PTP on the Switch, on page 88
- Configuring NTP to PTP Time Conversion, on page 99
- Related Documents, on page 104
- Feature History, on page 104

Information About Precision Time Protocol

Precision Time Protocol (PTP) is defined in IEEE 1588 as Precision Clock Synchronization for Networked Measurements and Control Systems, and was developed to synchronize the clocks in packet-based networks that include distributed device clocks of varying precision and stability. PTP is designed specifically for industrial, networked measurement and control systems, and is optimal for use in distributed systems because it requires minimal bandwidth and little processing overhead.

Why PTP?

Smart grid power automation applications such as peak-hour billing, virtual power generators, and outage monitoring and management, require extremely precise time accuracy and stability. Timing precision improves network monitoring accuracy and troubleshooting ability.

In addition to providing time accuracy and synchronization, the PTP message-based protocol can be implemented on packet-based networks, such as Ethernet networks. The benefits of using PTP in an Ethernet network include:

- Low cost and easy setup in existing Ethernet networks
- Limited bandwidth is required for PTP data packets
Ethernet Switches and Delays

In an Ethernet network, switches provide a full-duplex communication path between network devices. Switches send data packets to packet destinations using address information contained in the packets. When the switch attempts to send multiple packets simultaneously, some of the packets are buffered by the switch so that they are not lost before they are sent. When the buffer is full, the switch delays sending packets. This delay can cause device clocks on the network to lose synchronization with one another.

Additional delays can occur when packets entering a switch are stored in local memory while the switch searches the MAC address table to verify packet CRC fields. This process causes variations in packet forwarding time latency, and these variations can result in asymmetrical packet delay times.

Adding PTP to a network can compensate for these latency and delay problems by correctly adjusting device clocks so that they stay synchronized with one another. PTP enables network switches to function as PTP devices, including boundary clocks (BCs) and transparent clocks (TCs).

Note
To learn more about PTP clock devices and their role in a PTP network, refer to PTP Clocks, on page 74.

Message-Based Synchronization

To ensure clock synchronization, PTP requires an accurate measurement of the communication path delay between the time source (master) and the receiver (slave). PTP sends messages between the master and slave device to determine the delay measurement. Then, PTP measures the exact message transmit and receive times and uses these times to calculate the communication path delay. PTP then adjusts current time information contained in network data for the calculated delay, resulting in more accurate time information.

This delay measurement principle determines path delay between devices on the network, and the local clocks are adjusted for this delay using a series of messages sent between masters and slaves. The one-way delay time is calculated by averaging the path delay of the transmit and receive messages. This calculation assumes a symmetrical communication path; however, switched networks do not necessarily have symmetrical communication paths, due to the buffering process.

PTP provides a method, using transparent clocks, to measure and account for the delay in a time-interval field in network timing packets, making the switches temporarily transparent to the master and slave nodes on the network. An end-to-end transparent clock forwards all messages on the network in the same way that a switch does.

Note
Cisco PTP supports multicast PTP messages only.

To read a detailed description of synchronization messages, refer to PTP Event Message Sequences, on page 71. To learn more about how transparent clocks calculate network delays, refer to Transparent Clock, on page 74.

The following figure shows a typical 1588 PTP network that includes grandmaster clocks, switches in boundary clock mode, and Intelligent Electronic Device (IEDs) such as digital relays or protection devices. In this diagram, Master 1 is the grandmaster clock. If Master 1 becomes unavailable, the boundary clock slaves switch to Master 2 for synchronization.
PTP Event Message Sequences

This section describes the PTP event message sequences that occur during synchronization.

Synchronizing with Boundary Clocks

The ordinary and boundary clocks configured for the delay request-response mechanism use the following event messages to generate and communicate timing information:

- Sync
- Delay_Req
- Follow_Up
- Delay_Resp

These messages are sent in the following sequence:

1. The master sends a Sync message to the slave and notes the time (t1) at which it was sent.
2. The slave receives the Sync message and notes the time of reception (t2).
3. The master conveys to the slave the timestamp t1 by embedding the timestamp t1 in a Follow_Up message.
4. The slave sends a Delay_Req message to the master and notes the time (t3) at which it was sent.
5. The master receives the Delay_Req message and notes the time of reception (t4).
6. The master conveys to the slave the timestamp t4 by embedding it in a Delay_Resp message.
After this sequence, the slave possesses all four timestamps. These timestamps can be used to compute the offset of the slave clock relative to the master, and the mean propagation time of messages between the two clocks.

The offset calculation is based on the assumption that the time for the message to propagate from master to slave is the same as the time required from slave to master. This assumption is not always valid on an Ethernet network due to asymmetrical packet delay times.

Figure 9: Detailed Steps—Boundary Clock Synchronization

Synchronizing with Peer-to-Peer Transparent Clocks

When the network includes multiple levels of boundary clocks in the hierarchy, with non-PTP enabled devices between them, synchronization accuracy decreases.

The round-trip time is assumed to be equal to mean_path_delay/2, however this is not always valid for Ethernet networks. To improve accuracy, the resident time of each intermediary clock is added to the offset in the end-to-end transparent clock. Resident time, however, does not take into consideration the link delay between peers, which is handled by peer-to-peer transparent clocks.

Peer-to-peer transparent clocks measure the link delay between two clock ports implementing the peer delay mechanism. The link delay is used to correct timing information in Sync and Follow_Up messages.

Peer-to-peer transparent clocks use the following event messages:

- Pdelay_Req
- Pdelay_RESP
- Pdelay_RESP_Follow_Up
These messages are sent in the following sequence:

1. Port 1 generates timestamp $t_1$ for a Pdelay_Req message.
2. Port 2 receives and generates timestamp $t_2$ for this message.
3. Port 2 returns and generates timestamp $t_3$ for a Pdelay_Resp message.

   To minimize errors due to any frequency offset between the two ports, Port 2 returns the Pdelay_Resp message as quickly as possible after the receipt of the Pdelay_Req message.
4. Port 2 returns timestamps $t_2$ and $t_3$ in the Pdelay_Resp and Pdelay_Resp_Follow_Up messages respectively.
5. Port 1 generates timestamp $t_4$ after receiving the Pdelay_Resp message. Port 1 then uses the four timestamps ($t_1, t_2, t_3,$ and $t_4$) to calculate the mean link delay.

\[ \text{Peer_link_delay} = \frac{(t_4 - t_1) - (t_3 - t_2)}{2} \]

**Synchronizing the Local Clock**

In an ideal PTP network, the master and slave clock operate at the same frequency. However, *drift* can occur on the network. Drift is the frequency difference between the master and slave clock. You can compensate for drift by using the time stamp information in the device hardware and follow-up messages (intercepted by the switch) to adjust the frequency of the local clock to match the frequency of the master clock.

**Best Master Clock Algorithm**

The Best Master Clock Algorithm (BMCA) is the basis of PTP functionality. The BMCA specifies how each clock on the network determines the best master clock in its subdomain of all the clocks it can see, including itself. The BMCA runs on the network continuously and quickly adjusts for changes in network configuration.

The BMCA uses the following criteria to determine the best master clock in the subdomain:
Clock quality (for example, GPS is considered the highest quality)
Clock accuracy of the clock’s time base
Stability of the local oscillator
Closest clock to the grandmaster

In addition to identifying the best master clock, the BMCA also ensures that clock conflicts do not occur on the PTP network by ensuring that:

- Clocks do not have to negotiate with one another
- There is no misconfiguration, such as two master clocks or no master clocks, as a result of the master clock identification process

### PTP Clocks

A PTP network is made up of PTP-enabled devices and devices that are not using PTP. The PTP-enabled devices typically consist of the following clock types.

**Grandmaster Clock**

Within a PTP domain, the grandmaster clock is the primary source of time for clock synchronization using PTP. The grandmaster clock usually has a very precise time source, such as a GPS or atomic clock. When the network does not require any external time reference and only needs to be synchronized internally, the grandmaster clock can free run.

**Ordinary Clock**

An ordinary clock is a PTP clock with a single PTP port. It functions as a node in a PTP network and can be selected by the BMCA as a master or slave within a subdomain. Ordinary clocks are the most common clock type on a PTP network because they are used as end nodes on a network that is connected to devices requiring synchronization. Ordinary clocks have various interface to external devices.

**Boundary Clock**

A boundary clock in a PTP network operates in place of a standard network switch or router. Boundary clocks have more than one PTP port, and each port provides access to a separate PTP communication path. Boundary clocks provide an interface between PTP domains. They intercept and process all PTP messages, and pass all other network traffic. The boundary clock uses the BMCA to select the best clock seen by any port. The selected port is then set as a slave. The master port synchronizes the clocks connected downstream, while the slave port synchronizes with the upstream master clock.

**Transparent Clock**

The role of transparent clocks in a PTP network is to update the time-interval field that is part of the PTP event message. This update compensates for switch delay and has an accuracy of within one picosecond.

There are two types of transparent clocks:

**End-to-end (E2E) transparent clocks** measure the PTP event message transit time (also known as resident time) for SYNC and DELAY_REQUEST messages. This measured transit time is added to a data field (correction field) in the corresponding messages:
• The measured transit time of a SYNC message is added to the correction field of the corresponding
SYNC or the FOLLOW_UP message.

• The measured transit time of a DELAY_REQUEST message is added to the correction field of the
corresponding DELAY_RESPONSE message.

The slave uses this information when determining the offset between the slave’s and the master’s time. E2E
transparent clocks do not provide correction for the propagation delay of the link itself.

**Peer-to-peer (P2P) transparent clocks** measure PTP event message transit time in the same way E2E
transparent clocks do, as described above. In addition, P2P transparent clocks measure the upstream link
delay. The upstream link delay is the estimated packet propagation delay between the upstream neighbor P2P
transparent clock and the P2P transparent clock under consideration.

These two times (message transit time and upstream link delay time) are both added to the correction field of
the PTP event message, and the correction field of the message received by the slave contains the sum of all
link delays. In theory, this is the total end-to-end delay (from master to slave) of the SYNC packet.

The following figure illustrates PTP clocks in a master-slave hierarchy within a PTP network.

*Figure 11: PTP Clock Hierarchy*

---

**PTP Profiles**

This section describes the following PTP profiles available on the switch:

- Power Profile
- Default Profile
- 802.1AS Profile (IE 4000 only)

The Power Profile is defined in PC37.238 - IEEE Draft Standard Profile for Use of IEEE 1588 Precision Time
Protocol in Power System Applications. This switch documentation uses the terms Power Profile mode and
Default Profile mode when referring to this IEEE 1588 profile and its associated configuration values.

The IEEE 1588 definition of a PTP profile is *the set of allowed PTP features applicable to a device*. A PTP
profile is usually specific to a particular type of application or environment and defines the following values:

- Best master clock algorithm options
Default Profile Mode

The default PTP profile mode on the switch is Default Profile mode. In this mode:

- The PTP mode of transport is Layer 3.
- The supported transparent clock mode is end-to-end (E2E).

Table 7: Configuration Values for the IEEE PTP Power Profile and Switch Modes, on page 76 lists the configuration values for the switch in Default Profile mode.

Power Profile Mode

The IEEE Power Profile defines specific or allowed values for PTP networks used in power substations. The defined values include the optimum physical layer, the higher level protocol for PTP messages, and the preferred best master clock algorithm. The Power Profile values ensure consistent and reliable network time distribution within substations, between substations, and across wide geographic areas.

The switch is optimized for PTP in these ways:

- Hardware—The switch uses FPGA and PHY for the PTP function. The PHY time stamps the Fast Ethernet and Gigabit Ethernet ports.
- Software—In Power Profile mode, the switch uses the configuration values defined in the IEEE 1588 Power Profile standard.

The following table lists the configuration values defined by the IEEE 1588 Power Profile and the values that the switch uses for each PTP profile mode.

Table 7: Configuration Values for the IEEE PTP Power Profile and Switch Modes

<table>
<thead>
<tr>
<th>PTP Field</th>
<th>Power Profile Value</th>
<th>Switch Configuration Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Power Profile Mode</td>
</tr>
<tr>
<td>Message transmission</td>
<td>Ethernet 802.3 with Ethertype 0X88F7. PTP messages are sent as 802.1Q tagged Ethernet frames with a default VLAN 0 and default priority 4.</td>
<td>Access Ports—Untagged Layer 2 packets. Trunk Ports—802.1Q tagged Layer 2 packets with native VLAN on the port and default priority value of 4.</td>
</tr>
<tr>
<td>MAC address—Non-peer delay messages</td>
<td>01-1B-19-00-00-00.</td>
<td>01-1B-19-00-00-00.</td>
</tr>
</tbody>
</table>
### 802.1AS Profile (IE 4000 only)

The 802.1AS Profile is supported for the IE 4000 only.

The IEEE 802.1AS standard "Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks" specifies the protocol and procedures used to ensure that synchronization requirements are met for time-sensitive applications across bridged and virtual bridged local area networks.

802.1AS specifies the use of IEEE 1588 (PTP) specifications where applicable in the context of IEEE Std 802.1D-2004 and IEEE Std 802.1Q-2005.1. The 802.1AS standard is one of three 802.1 AVB draft standards. 802.1AS over Ethernet (802.3) qualifies as a Profile of IEEE 1588-2008. It simplifies IEEE 1588 and defines synchronization over different types of media.

Key characteristics of 802.1AS are:

- For Ethernet full-duplex links, it uses the peer delay mechanism.
- All switches in the domain need to be 802.1AS capable.
- Transportation of 802.1AS packets is L2 multicast only, with no VLAN tag.
- It requires two-step processing (use of Follow_Up and Pdelay_Resp_Follow_Up messages to communicate timestamps).

<table>
<thead>
<tr>
<th>PTP Field</th>
<th>Power Profile Value</th>
<th>Switch Configuration Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Power Profile Mode</td>
<td>Default Profile Mode</td>
</tr>
<tr>
<td>MAC address—Peer delay messages</td>
<td>01-80-C2-00-00-0E.</td>
<td>01-80-C2-00-00-0E.</td>
</tr>
<tr>
<td></td>
<td>Not applicable to this mode.</td>
<td></td>
</tr>
<tr>
<td>Domain number</td>
<td>0.</td>
<td>0.</td>
</tr>
<tr>
<td></td>
<td>0.</td>
<td>0.</td>
</tr>
<tr>
<td>Path delay calculation</td>
<td>Peer-to-peer transparent clocks.</td>
<td>Peer-to-peer transparent clocks using the peer_delay mechanism.</td>
</tr>
<tr>
<td></td>
<td>End-to-end transparent clocks using the delay_request mechanism.</td>
<td></td>
</tr>
<tr>
<td>BMCA</td>
<td>Enabled.</td>
<td>Enabled.</td>
</tr>
<tr>
<td></td>
<td>Enabled.</td>
<td>Enabled.</td>
</tr>
<tr>
<td>Clock type</td>
<td>Two-step clocks are supported.</td>
<td>Two-step.</td>
</tr>
<tr>
<td>Time scale</td>
<td>Epoch.(^1)</td>
<td>Epoch.(^1)</td>
</tr>
<tr>
<td></td>
<td>Epoch.</td>
<td>Epoch.(^1)</td>
</tr>
<tr>
<td>Grandmaster ID and local time determination</td>
<td>PTP-specific TLV (type, length, value) to indicate Grandmaster ID.</td>
<td>PTP-specific TLV to indicate Grandmaster ID.</td>
</tr>
<tr>
<td></td>
<td>PTP-specific type, length, and value to indicate Grandmaster ID.</td>
<td></td>
</tr>
<tr>
<td>Time accuracy over network hops</td>
<td>Over 16 hops, slave device synchronization accuracy is within 1 usec (1 microsecond).</td>
<td>Over 16 hops, slave device synchronization accuracy is within 1 usec (1 microsecond).</td>
</tr>
<tr>
<td></td>
<td>Not applicable in this mode.</td>
<td></td>
</tr>
</tbody>
</table>

\(^1\) Epoch = Elapsed time since epoch start.
• There is only a single active grandmaster in a time-aware network. That is, there is only a single 802.1AS domain.

• The BMCA (Best Master Clock Algorithm) is same as that used in IEEE 1588 with the following exceptions:
  • Announce messages received on a slave port that were not sent by the receiving time-aware system are used immediately; that is, there is no foreign-master qualification.
  • A port that the BMCA determines should be a master port enters the master state immediately; that is, there is no pre-master state.
  • The uncalibrated state is not needed and therefore not used.
  • All time-aware systems are required to participate in best master selection (even if the system is not grandmaster capable).

802.1AS on the IE 4000

On the IE 4000, 802.1AS is used in the Time Sensitive Network (TSN) feature. However, as a precise timing distribution mechanism, 802.1AS runs by itself without TSN configuration or inputs. The 802.1AS feature software implementation is based on the existing timestamping functionality of FPGA and has no new requirement on hardware beyond other PTP profiles.

The end-to-end time-synchronization performance of 802.1AS on the IE 4000 is as follows:
  • Any two time-aware systems separated by six or fewer time-aware systems (that is, seven or fewer hops) will be synchronized to within 1 μs peak-to-peak of each other during steady-state operation.
  • Performance beyond 7 hops is not defined.

802.1AS Profile Comparison

<table>
<thead>
<tr>
<th>Profile</th>
<th>Default (*)</th>
<th>Power</th>
<th>802.1AS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>IEEE1588 v2 (J.3)</td>
<td>IEEE C37.238</td>
<td>IEEE802.1AS</td>
</tr>
<tr>
<td>Mode</td>
<td>Boundary</td>
<td>End-to-End transparent</td>
<td>Boundary</td>
</tr>
<tr>
<td>Path Delay</td>
<td>Delay req/res</td>
<td>Delay req/res</td>
<td>Peer delay req/res</td>
</tr>
<tr>
<td>Non-PTP device allowed in PTP domain</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Transport</td>
<td>UDP over IP (multicast and unicast)</td>
<td>L2 Multicast</td>
<td>L2 Multicast</td>
</tr>
</tbody>
</table>

* Delay Request-Response Default PTP profile (as defined in IEEE1588 J.3).
** There is no mode setting for 802.1AS. Mathematically it is equivalent to P2P transparent, but it works differently from a transparent clock.

**Tagging Behavior for PTP Packets**

The following table describes the switch tagging behavior in Power Profile and Default Profile modes.

<table>
<thead>
<tr>
<th>Switch Port Mode</th>
<th>Configuration</th>
<th>Power Profile Mode</th>
<th>Default Profile Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trunk Port</td>
<td>vlan dot1q tag native enabled</td>
<td>Switch tags packets</td>
<td>Switch tags packets</td>
</tr>
<tr>
<td>Trunk Port</td>
<td>vlan dot1q tag native disabled</td>
<td>PTP software tags packets</td>
<td>Untagged</td>
</tr>
<tr>
<td>Access Port</td>
<td>N/A</td>
<td>Untagged</td>
<td>None</td>
</tr>
</tbody>
</table>

**PTP Clock Modes Supported on the Switch**

PTP synchronization behavior depends on the PTP clock mode that you configure on the switch. You can configure the switch for one of the following global modes.

See [Guidelines and Limitations, on page 86](#) for guidelines for configuring each of the clock modes.

**Boundary Clock Mode**

A switch configured for boundary clock mode participates in selecting the best master clock on the subdomain, selecting from all clocks it can see, including itself. If the switch does not detect a more accurate clock than itself, then the switch becomes the master clock. If a more accurate clock is detected, then the switch synchronizes to that clock and becomes a slave clock.

After initial synchronization, the switch and the connected devices exchange PTP timing messages to correct the changes caused by clock offsets and network delays.

**Forward Mode**

A switch configured for forward mode passes incoming PTP packets as normal multicast traffic.

**E2E Transparent Clock Mode**

A switch configured for end-to-end transparent clock mode does not synchronize its clock with the master clock. A switch in this mode does not participate in master clock selection and uses the default PTP clock mode on all ports.
P2P Transparent Clock Mode

A switch configured for peer-to-peer transparent clock mode does not synchronize its clock with the master clock. A switch in this mode does not participate in master clock selection and uses the default PTP clock mode on all ports.

Configurable Boundary Clock Synchronization Algorithm

You can configure the BC synchronization algorithm to accommodate various PTP use cases, depending on whether you need to prioritize filtering of input time errors or faster convergence. A PTP algorithm that filters packet delay variation (PDV) converges more slowly than a PTP algorithm that does not.

By default, the BC uses a linear feedback controller (that is, a servo) to set the BC's time output to the next clock. The linear servo provides a small amount of PDV filtering and converges in an average amount of time. For improved convergence time, BCs can use the TC feedforward algorithm to measure the delay added by the network elements forwarding plane (the disturbance) and use that measured delay to control the time output.

While the feedforward BC dramatically speed up the boundary clock, the feedforward BC does not filter any PDV. The adaptive PDV filter provides high quality time synchronization in the presence of PDV over wireless access points (APs) and enterprise switches that do not support PTP and that add significant PDV.

Three options are available for BC synchronization (all are compliant with IEEE 1588-2008):

- Feedforward—For very fast and accurate convergence; no PDV filtering.
- Adaptive—Filters as much PDV as possible, given a set of assumptions about the PDV characteristics, the hardware configuration, and the environmental conditions.

Note

With the adaptive filter, the switch does not meet the time performance requirements specified in ITU-T G.8261.

- Linear—Provides simple linear filtering (the default).

Adaptive mode (ptp transfer filter adaptive) is not available in Power Profile mode.

For configuration information, see.

Information About NTP to PTP Time Conversion

NTP to PTP Time Conversion allows you to use Network Time Protocol (NTP) as a time source for PTP. Customers who use PTP for very precise synchronization within a site can use NTP across sites, where precise synchronization is not required.

NTP is the traditional method of synchronizing clocks across packet based networks. NTP uses a two-way time transfer mechanism, between a master and a slave. NTP is capable of synchronizing a device within a few 100 milliseconds across the Internet, and within a few milliseconds in a tightly controlled LAN. The ability to use NTP as a time source for PTP allows customers to correlate data generated in their PTP network with data in their enterprise data centers running NTP.

The following figure shows an example of an industrial network based on the Industrial Automation and Control System Reference Model. The enterprise zone and demilitarized zone run NTP, and the manufacturing
zone and cell/area zone run PTP with NTP as the time source. The switch with the NTP to PTP conversion feature can be either the Layer 2 Switch or the Distribution Switch in the Cell/Area Zone.
Figure 12: Industrial Network with NTP and PTP
Grandmaster Boundary Clock Hybrid

The NTP to PTP conversion feature adds grandmaster clock functionality to Cisco PTP, so the switch can be a time source as well as forward time. A new PTP clock type, grandmaster boundary clock (GMC-BC), provides the NTP time source for PTP. The GMC-BC acts like a BC, which is a multi-port device, with a single-port GMC connected to a virtual port on the BC. The GMC-BC switches between acting like a GMC when the GMC-BC is the primary GMC, and acting like a BC when the GMC-BC is a backup. This ensures that all devices on the PTP network remain synchronized in a failover scenario. The following figure shows a PTP network with redundant GMC-BCs. GMC-BC 1 is the grandmaster clock, and GMC-BC 2 is both backup GMC and BC.

Figure 13: Redundant GMC-BC Configuration

In a network with two GMC-BCs, the secondary GMC-BC can synchronize to both the NTP reference and the PTP reference at the same time, so the secondary GMC-BC can immediately take over when the primary GMC-BC fails. The GMC-BC instantly updates the time during a switchover.

Clock Manager

The clock manager is the component in the Cisco NTP to PTP software architecture that keeps track of the various time services and selects the clock that actively provides time. The clock manager notifies the time services of important changes, such as state changes, leap seconds, or daylight saving time.

The clock manager selects the NTP or manually-set clock first, followed by PTP and the real-time clock if NTP is not active. The following table shows the results of the clock selection process.

Table 10: Time Service Selection

<table>
<thead>
<tr>
<th>NTP (Active) or Manually Set</th>
<th>PTP (Active)</th>
<th>Real-Time Clock</th>
<th>Selected Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
<td>Don’t care</td>
<td>Don’t care</td>
<td>NTP or Manually Set</td>
</tr>
<tr>
<td>False</td>
<td>True</td>
<td>Don’t care</td>
<td>PTP</td>
</tr>
<tr>
<td>False</td>
<td>False</td>
<td>True</td>
<td>Real-Time Clock</td>
</tr>
</tbody>
</table>
In general, the clock manager ensures that the time displayed in the Cisco IOS commands `show ptp clock` and `show clock` match. The `show clock` command always follows this priority, but there are two corner cases where the `show ptp clock` time may differ:

- The switch is either a TC or a BC, and there is no other active reference on the network. To preserve backwards compatibility, the TC and BC never take their time from the clock manager, only from the network’s PTP GMC. If there is no active PTP GMC, then the time displayed in the `show clock` and the `show ptp clock` command output may differ.

- The switch is a syntonizing TC, a BC with a slave port, or a GMC-BC with slave port, and the time provided by the PTP GMC does not match the time provided by NTP or the user (that is, manually set). In this case, the PTP clock must forward the time from the PTP GMC. If the PTP clock does not follow the PTP GMC, then the PTP network will end up with two different time bases, which would break any control loops or sequence of event applications using PTP.

The following table shows how the Cisco IOS and PTP clocks behave given the various configurations. Most of the time, the two clocks match. Occasionally, the two clocks are different; those configurations are highlighted in the table.

### Table 11: Expected Time Flow

<table>
<thead>
<tr>
<th>IOS Clock Configuration</th>
<th>PTP Clock Configuration</th>
<th>IOS Clock Source</th>
<th>PTP Clock Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendar</td>
<td>PTP BC, E2E TC, or GMC-BC in BC Mode</td>
<td>PTP</td>
<td>PTP</td>
</tr>
<tr>
<td>Manual</td>
<td>PTP BC, E2E TC, or GMC-BC in BC Mode</td>
<td>Manual</td>
<td>PTP</td>
</tr>
<tr>
<td>NTP</td>
<td>PTP BC, E2E TC, or GMC-BC in BC Mode</td>
<td>NTP</td>
<td>PTP</td>
</tr>
<tr>
<td>Calendar</td>
<td>GMC-BC in GM Mode</td>
<td>Calendar</td>
<td>Calendar</td>
</tr>
<tr>
<td>NTP</td>
<td>GMC-BC in GM Mode</td>
<td>NTP</td>
<td>NTP</td>
</tr>
</tbody>
</table>

### Prerequisites

- Review the Guidelines and Limitations, on page 86.
- To use the NTP to PTP conversion feature, the switch must have an IP address for NTP to function.
- To use the NTP to PTP conversion feature, you must configure at least one NTP server. Configuring three or more NTP servers allows NTP to ignore bad clocks.

**Note**

For information about configuring NTP, see the section Configuring NTP in the *Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(55)SE*.
Guidelines and Limitations

PTP Messages

• The Cisco PTP implementation supports only the two-step clock and not the one-step clock. If the switch receives a one-step message from the Grand Master Clock, it will convert it into a two-step message.

• Cisco PTP supports multicast PTP messages only.

PTP Mode and Profile

• The switch and the grandmaster clock must be in the same PTP domain.

• When Power Profile mode is enabled, the switch drops the PTP announce messages that do not include these two Type, Length, Value (TLV) message extensions: Organization_extension and Alternate_timescale.

If the grandmaster clock is not compliant with PTP and sends announce messages without these TLVs, configure the switch to process the announce message by entering the `ptp allow-without-tlv` command.

• When the switch is in Power Profile mode, only the peer_delay mechanism is supported.

To change to Boundary Clock Mode, on page 79 and the peer_delay mechanism, enter the `ptp mode boundary pdelay-req` command.

• To disable Power Profile mode and return the switch to E2E Transparent Clock Mode, on page 79, enter the `no ptp profile power` command.

• In Default Profile mode, only the delay_request mechanism is supported.

To change to Boundary Clock Mode, on page 79 with the delay_request mechanism, enter the `ptp mode boundary delay-req` command.

Packet Format

• The packet format for PTP messages can be 802.1q tagged packets or untagged packets.

• The switch does not support 802.1q QinQ tunneling.

• In switch Power Profile mode:
  • When the PTP interface is configured as an access port, PTP messages are sent as untagged, Layer 2 packets.
  • When the PTP interface is configured as a trunk port, PTP packets are sent as 802.1q tagged Layer 2 packets over the port native VLAN.

• Slave IEDs must support tagged and untagged packets.

• When PTP packets are sent on the native VLAN in E2E Transparent Clock Mode, on page 79, they are sent as untagged packets. To configure the switch to send them as tagged packets, enter the global `vlan dot1q tag native` command.
VLAN Configuration

- Sets the PTP VLAN on a trunk port. The range is from 1 to 4094. The default is the native VLAN of the trunk port.
- In boundary mode, only PTP packets in PTP VLAN will be processed, PTP packets from other VLANs will be dropped.
- Before configuring the PTP VLAN on an interface, the PTP VLAN must be created and allowed on the trunk port.
- Most grandmaster clocks use the default VLAN 0. In Power Profile mode, the switch default VLAN is VLAN 1 and VLAN 0 is reserved. When you change the default grandmaster clock VLAN, it must be changed to a VLAN other than 0.
- When VLAN is disabled on the grandmaster clock, the PTP interface must be configured as an access port.

Clock Configuration

- All PHY PTP clocks are synchronized to the grandmaster clock. The switch system clock is not synchronized as part of PTP configuration and processes.
- When VLAN is enabled on the grandmaster clock, it must be in the same VLAN as the native VLAN of the PTP port on the switch.
- Grandmaster clocks can drop untagged PTP messages when a VLAN is configured on the grandmaster clock. To force the switch to send tagged packets to the grandmaster clock, enter the global `vlan dot1q tag native` command.

Clock Modes

Note: The 802.1AS profile does not have a clock mode setting.

- Boundary Clock Mode
  - You can enable this mode when the switch is in Power Profile Mode, on page 76 (Layer 2) or in Default Profile Mode, on page 76 (Layer 3).
- Forward Mode
  - You can enable this mode when the switch is in Power Profile Mode, on page 76 (Layer 2) or in Default Profile Mode, on page 76 (Layer 3).
  - When the switch is in Forward mode, the only global configuration available is the CLI command to switch to a different PTP mode (that is, boundary, e2etransparent, or p2ptransparent).
- E2E Transparent Clock Mode
  - You can enable this mode only when the switch is in Default Profile Mode, on page 76 (Layer 3).
  - When the switch is in E2E Transparent mode, the only global configuration available is the CLI command to switch to a different PTP mode (that is, boundary, p2ptransparent, or forward).
• P2P Transparent Clock Mode
  • You can enable this mode only when the switch is in Power Profile Mode, on page 76 (Layer 2).
  • When the switch is in P2P Transparent mode, the only global configuration available is the CLI command to switch to a different PTP mode (that is, boundary, e2etransparent, or forward).

PDV Filtering
Adaptive mode (ptp transfer filter adaptive) is not available in Power Profile mode.

PTP Interaction with Other Features
• The following PTP clock modes do not support EtherChannels:
  • e2etransparent
  • p2ptransparent
  • boundary
• The following PTP clock modes only operate on a single VLAN:
  • e2etransparent
  • p2ptransparent

Default Settings
• PTP is enabled on the switch by default.
• By default, the switch uses configuration values defined in the Default Profile (Default Profile mode is enabled).
• The switch default PTP clock mode is E2E Transparent Clock Mode, on page 79.
• The default BC synchronization algorithm is linear filter.

Configuring PTP on the Switch
Use one of the following procedures in this section to configure the switch for PTP.

Note
To configure the switch for grandmaster-boundary clock mode (gmc-bc), see Configuring NTP to PTP Time Conversion, on page 99.
Configuring PTP Power Profile Mode on the Switch

This section describes how to configure the switch to use the PTP Power Profile and operate in Power Profile mode.

Before you begin

These are some guidelines for configuring the Power Profile on the switch:

- When you enter `no` with PTP port configuration commands, the specified port property is set to the default value.
- To determine the value in seconds for the `interval` variable, use a logarithmic scale. Below are examples of the `interval` variable value converted to seconds with a logarithmic scale:

<table>
<thead>
<tr>
<th>Value Entered</th>
<th>Logarithmic Calculation</th>
<th>Value in Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>$2^{-1}$</td>
<td>1/2</td>
</tr>
<tr>
<td>0</td>
<td>$2^0$</td>
<td>1</td>
</tr>
</tbody>
</table>

SUMMARY STEPS

1. Enter global configuration mode:

2. Set the Power Profile:

3. Specify the synchronization clock mode:

4. (Optional, BC and TC mode) Specify TLV settings:

5. (Optional, BC and TC mode) Specify the PTP clock domain:

6. (Optional, BC and TC mode) Specify the packet priority:

7. (Optional, BC mode only) Specify the BMCA priority:

8. (Optional, BC mode only) Specify time-property preservation:

9. (Optional, BC mode only) Specify the BC synchronization algorithm:

10. (Optional) Enter interface configuration mode:

11. (Optional) Specify port settings:

12. Return to privileged EXEC mode:

13. Verify your entries:

14. (Optional) Save your entries in the configuration file:

DETAILED STEPS

Step 1 Enter global configuration mode:

```
configure terminal
```

Step 2 Set the Power Profile:

```
ptp profile power
```

Step 3 Specify the synchronization clock mode:
Configuring Precision Time Protocol

ptp mode \{boundary pdelay-req | p2ptransparent | forward\}

- **mode boundary pdelay-req**—Configures the switch for boundary clock mode using the delay-request mechanism. In this mode, the switch participates in the selection of the most accurate master clock. Use this mode when overload or heavy load conditions produce significant delay jitter.

- **mode p2ptransparent**—Configures the switch for peer-to-peer transparent clock mode and synchronizes all switch ports with the master clock. The link delay time between the participating PTP ports and the message transit time is added to the resident time. Use this mode to reduce jitter and error accumulation. This is the default in Power Profile mode.

- **mode forward**—Configures the switch to pass incoming PTP packets as normal multicast traffic.

**Step 4**
(Optional, BC and TC mode) Specify TLV settings:

```
ptp allow-without-tlv
```

**Step 5**
(Optional, BC and TC mode) Specify the PTP clock domain:

```
ptp domain domain-number
```

*domain-number*—A number from 0 to 255.

The participating grandmaster clock, switches, and slave devices should be in the same domain.

**Step 6**
(Optional, BC and TC mode) Specify the packet priority:

```
ptp packet priority
```

The PTP packets have a default priority of 4. Lower values take precedence.

**Step 7**
(Optional, BC mode only) Specify the BMCA priority:

```
ptp priority1 priority priority2 priority
```

- **priority1**—Overrides the default criteria (such as clock quality and clock class) for the most accurate master clock selection.

- **priority2**—Breaks the tie between two switches that match the default criteria. For example, enter 2 to give a switch priority over identical switches.

*priority*—A priority number from 0 to 255. The default is 128.

**Step 8**
(Optional, BC mode only) Specify time-property preservation:

```
ptp time-property persist \{value | infinite\}
```

- **value**—Time duration, in seconds, from 0-100000. The default is 300.

- **infinite**—Time properties are preserved indefinitely.

Preserving the time properties prevents slave clocks from detecting a variance in the time values when the redundant GMC comes out of standby.

**Step 9**
(Optional, BC mode only) Specify the BC synchronization algorithm:

```
ptp transfer \{feedforward | filter linear\}
```

- **feedforward**—Very fast and accurate. No PDV filtering.

- **filter linear**—Provides a simple linear filter (default).
Step 10  (Optional) Enter interface configuration mode:

```
interface interface-id
```

Step 11  (Optional) Specify port settings:

Boundary pdelay-req mode:

```
ptp {announce {interval value | timeout value} | pdelay-req interval value | enable | sync {interval value | limit value} | vlan value}
```

```
p2p transparent mode:

ptp {pdelay-req interval value | enable | sync limit value | vlan value}
```

- **announce interval value**—Sets the logarithmic mean interval in seconds to send announce messages. The range is 0 to 4. The default is 1 (2 seconds).
- **announce timeout value**—Sets the logarithmic mean interval in seconds to announce timeout messages. The range is 2 to 10. The default is 3 (8 seconds).
- **pdelay-req interval value**—Sets the logarithmic mean interval in seconds for slave devices to send pdelay request messages when the port is in the master clock state. The range is -3 to 5. The default is 0 (1 second).
- **enable**—Enables PTP on the port base module.
- **sync interval value**—Sets the logarithmic mean interval in seconds to send synchronization messages. The range is −2 to 1. The default is 1 second.
- **sync limit value**—Sets the maximum clock offset value before PTP attempts to resynchronize. The range is from 50 to 500000000 nanoseconds. The default is 10000 nanoseconds.
- **vlan value**—Sets the PTP VLAN on a trunk port. The range is from 1 to 4094. The default is the native VLAN of the trunk port. In boundary mode, only PTP packets in PTP VLAN will be processed, PTP packets from other VLANs will be dropped. Before configuring the PTP VLAN on an interface, the PTP VLAN must be created and allowed on the trunk port.

Step 12  Return to privileged EXEC mode:

```
end
```

Step 13  Verify your entries:

```
show running-config
```

Step 14  (Optional) Save your entries in the configuration file:

```
copy running-config startup-config
```

---

**Example**

The following example configures the switch for P2P transparent mode (the default in Power Profile mode), specifies `allow-without-tlv` PTP message processing, and uses default values for all PTP interval settings:

```
switch(config)# ptp allow-without-tlv
```
The following example configures the switch for boundary clock mode using the peer delay request (pdelay-req) mechanism and uses default values for all PTP interval settings:

```
switch(config)# ptp mode boundary pdelay-req
```

**Configuring Default Profile Mode on the Switch**

This section describes how to configure the switch to operate in Default Profile mode.

**Before you begin**

The switch sends untagged PTP packets on the native VLAN when the switch port connected to the grandmaster clock is configured as follows:

- Switch is in Default Profile mode.
- Switch is in trunk mode.
- VLAN X is configured as the native VLAN.

When the grandmaster clock requires tagged packets, make one of the following configuration changes:

- Force the switch to send tagged frames by entering the global ` vlan dot1q tag native ` command.
- Configure the grandmaster clock to send and receive untagged packets. If you make this configuration change on the grandmaster clock, you can configure the switch port as an access port.

These are some guidelines for configuring the Default Profile on the switch:

- When you enter `no` with PTP port configuration commands, the specified port property is set to the default value.
- To determine the value in seconds for the ptp global command `interval` variable, use a logarithmic scale. Below are examples of the `interval` variable value converted to seconds with a logarithmic scale:

<table>
<thead>
<tr>
<th>Value Entered</th>
<th>Logarithmic Calculation</th>
<th>Value in Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>$2^{-1}$</td>
<td>1/2</td>
</tr>
<tr>
<td>0</td>
<td>$2^{0}$</td>
<td>1</td>
</tr>
</tbody>
</table>

**SUMMARY STEPS**

1. Enter global configuration mode:
2. Configure the switch for Default Profile mode when the switch is in Power Profile mode. If the switch is already in Default Profile mode, this command has no effect.
3. Specify the synchronization clock mode:
4. (Optional, BC and TC mode) Specify the PTP clock domain:
5. (Optional, BC mode only) Specify the BMCA priority:
6. (Optional, BC mode only) Specify time-property preservation:
7. (Optional, BC mode only) Specify the BC synchronization algorithm:
8. (Optional) Enter interface configuration mode:

9. (Optional) Specify port settings:

10. Return to privileged EXEC mode:

11. Verify your entries:

12. (Optional) Save your entries in the configuration file:

DETAILED STEPS

Step 1
Enter global configuration mode:
`configure terminal`

Step 2
Configure the switch for Default Profile mode when the switch is in Power Profile mode. If the switch is already in Default Profile mode, this command has no effect.
`no ptp profile power`

Step 3
Specify the synchronization clock mode:
`ptp {mode boundary delay-req | e2etransparent | forward | gmc-bc}`
- **mode boundary delay-req**—Configures the switch for boundary clock mode using the delay-request mechanism. In this mode, the switch participates in the selection of the most accurate master clock. Use this mode when overload or heavy load conditions produce significant delay jitter.
- **mode e2etransparent**—Configures the switch for end-to-end transparent clock mode. A switch clock in this mode synchronizes all switch ports with the master clock. This switch does not participate in master clock selection and uses the default PTP clock mode on all ports. This is the default clock mode. The message transit time is added to the resident time. Use this mode to reduce jitter and error accumulation.
- **mode forward**—Configures the switch to pass incoming PTP packets as normal multicast traffic.
- **mode gmc-bc**—Configures the switch for grandmaster-boundary clock mode. See Configuring NTP to PTP Time Conversion, on page 99 to configure the switch for this mode.

Step 4
(Optional, BC and TC mode) Specify the PTP clock domain:
`ptp domain domain-number`
`domain-number — A number from 0 to 255.

The participating grandmaster clock, switches, and slave devices should be in the same domain.

Step 5
(Optional, BC mode only) Specify the BMCA priority:
`ptp priority1 priority priority2 priority`
- **priority1 priority**— Overrides the default criteria (such as clock quality and clock class) for the most accurate master clock selection.
- **priority2 priority**— Breaks the tie between two switches that match the default criteria. For example, enter 2 to give a switch priority over identical switches. `priority — A priority number from 0 to 255. The default is 128.`

Step 6
(Optional, BC mode only) Specify time-property preservation:
`ptp time-property persist {value | infinite}`
• value—Time duration, in seconds, from 0-100000. The default is 300.
• infinite—Time properties are preserved indefinitely.

Preserving the time properties prevents slave clocks from detecting a variance in the time values when the redundant GMC comes out of standby.

**Step 7**  
(Optional, BC mode only) Specify the BC synchronization algorithm:

```plaintext
ptp transfer {feedforward | filter {adaptive | linear}}
```

• **feedforward**—Very fast and accurate. No PDV filtering.
• **filter adaptive**—Automatically filters as much PDV as possible.
• **filter linear**—Provides a simple linear filter (default).

**Step 8**  
(Optional) Enter interface configuration mode:

```plaintext
interface interface-id
```

**Step 9**  
(Optional) Specify port settings:

- **Boundary delay-req mode:**
  ```plaintext
  ptp {announce {interval value | timeout value} | delay-req interval value | enable | sync {interval value | limit value}} | vlan value
  ```

- **e2e transparent mode:**
  ```plaintext
  ptp {enable | sync {interval value | limit value}}
  ```

• **announce interval value**—Sets the logarithmic mean interval in seconds to send announce messages. The range is 0 to 4. The default is 1 (2 seconds).
• **announce timeout value**—Sets the logarithmic mean interval in seconds to announce timeout messages. The range is 2 to 10. The default is 3 (8 seconds).
• **delay-req interval value**—Sets the logarithmic mean interval in seconds for slave devices to send delay request messages when the port is in the master clock state. The range is -2 to 6. The default is -5 (1 packet every 1/32 seconds, or 32 packets per second).
• **enable**—Enables PTP on the port base module.
• **sync interval value**—Sets the logarithmic mean interval in seconds to send synchronization messages. The range is -2 to 1. The default is 1 second.
• **sync limit value**—Sets the maximum clock offset value before PTP attempts to resynchronize. The range is from 50 to 500000000 nanoseconds. The default is 500000000 nanoseconds.
• **vlan value**—Sets the PTP VLAN on a trunk port. The range is from 1 to 4094. The default is the native VLAN of the trunk port. In boundary mode, only PTP packets in PTP VLAN will be processed, PTP packets from other VLANs will be dropped. Before configuring the PTP VLAN on an interface, the PTP VLAN must be created and allowed on the trunk port.

**Step 10**  
Return to privileged EXEC mode:

```plaintext
end
```
Step 11 Verify your entries:
   show running-config

Step 12 (Optional) Save your entries in the configuration file:
   copy running-config startup-config

Example
The following example configures the switch to operate in Default Profile mode and end-to-end transparent mode, and uses default values for all PTP interval settings:

switch(config)# no ptp profile
switch(config)# ptp mode e2etransparent

The following example configures the switch for Default Profile mode and boundary clock mode with the delay_request mechanism, and uses default values for all PTP interval settings:

switch(config)# no ptp profile
switch(config)# ptp mode boundary delay-req

Configuring 802.1AS Profile Mode on the Switch (IE 4000 only)
This section describes how to configure the IE 4000 switch to use the 802.1AS Profile and operate in 802.1AS Profile mode.

SUMMARY STEPS
1. Enter global configuration mode:
2. Set the 802.1AS Profile:

DETAILED STEPS

Step 1 Enter global configuration mode:
   configure terminal

Step 2 Set the 802.1AS Profile:
   ptp profile dot1as

Example
The following example shows configuring the IE 4000 switch to use the 802.1AS Profile:

IE4000-SW2(config)# ptp profile dot1as
802.1AS Troubleshooting

Refer to the following to troubleshoot 802.1AS issues:

- New Syslogs (Informational)—Parent and Grandmaster clock change syslogs notify user about the parent/grandmaster reselection. If that change happens frequently, or does not meet system expectation, further investigation should be taken. The following shows example log entries:
  - Mar 24 21:22:40.702: %PTP-6-PARENT_CLOCK_CHANGE: Old parent clock identity: 0x0:0:0:0:0:0:0:0 port number: 0, New parent clock identity: 0x0:35:1A:FF:FE:DA:12:80 port number: 9
  - Mar 24 21:22:40.702: %PTP-6-GRANDMASTER_CLOCK_CHANGE: Old grandmaster clock identity: 0x0:0:0:0:0:0:0:0, New grandmaster clock identity: 0x0:35:1A:FF:FE:DA:12:80

- SyncReceive TimeOut
  - 802.1AS added a new timer to detect sync receive timeout. If the next sync message does not arrive within 3 x sync interval (specified in the header of first sync message) on a PTP SLAVE port, sync receive timeout occurs.
  - This can be learned by turning on `debug ptp event` and observing "PTP (Interface GigabitEthernet1/1): sync receipt timeout" on the console.
  - At SyncReceive Timeout, the state of that PTP port will no longer be SLAVE. The next BMCA will re-select the new SLAVE port.

Verifying Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`show ptp [clock</td>
<td>foreign-master-records</td>
</tr>
<tr>
<td><code>clock</code></td>
<td>Displays PTP clock information.</td>
</tr>
<tr>
<td><code>foreign-master-records</code></td>
<td>Displays PTP foreign-master-records.</td>
</tr>
<tr>
<td><code>parent</code></td>
<td>Displays PTP parent properties.</td>
</tr>
<tr>
<td><code>port FastEthernet</code></td>
<td>Displays PTP properties for the FastEthernet IEEE 802.3 interfaces.</td>
</tr>
<tr>
<td><code>port GigabitEthernet</code></td>
<td>Displays PTP properties for the GigabitEthernet IEEE 802.3z interfaces.</td>
</tr>
<tr>
<td><code>time-property</code></td>
<td>Displays PTP clock-time properties.</td>
</tr>
</tbody>
</table>
Power Profile Example

switch# show ptp parent
PTP PARENT PROPERTIES
Parent Clock:
  Parent Clock Identity: 0xA4:C3:FF:BF:40
  Parent Port Number: 23
Observed Parent Offset (log variance): N/A
Observed Parent Clock Phase Change Rate: N/A
Grandmaster Clock:
  Grandmaster Clock Identity: 0xA4:C3:FF:BF:2B:0
  Grandmaster Clock Quality:
    Class: 248
    Accuracy: Unknown
    Offset (log variance): N/A
    Priority1: 128
    Priority2: 128

switch# show ptp clock
PTP CLOCK INFO
PTP Device Type: Boundary clock
PTP Device Profile: Power Profile
Clock Identity: 0xA4:C3:FF:BF:E0:80
Clock Domain: 0
Number of PTP ports: 26
PTP Packet priority: 4
Priority1: 128
Priority2: 128
Clock Quality:
  Class: 248
  Accuracy: Unknown
  Offset (log variance): N/A
Offset From Master(ns): 25
Mean Path Delay(ns): 705
Steps Removed: 4
Local clock time: 14:23:56 PST Apr 5 2013

switch# show ptp foreign-master-record
PTP FOREIGN MASTER RECORDS
Interface GigabitEthernet1/1
  Foreign master port identity: clock id: 0xF4:4E:5:FF:FE:E5:82:0
  Foreign master port identity: port num: 1
  Number of Announce messages: 4
  Message received port: 1
  Time stamps: 1999872004, 1999870997
Interface GigabitEthernet1/2
  Empty
Interface GigabitEthernet1/3
  Empty
Interface GigabitEthernet1/4
  Empty
Interface GigabitEthernet1/5
  Empty
Interface GigabitEthernet1/6
  Empty
Interface GigabitEthernet1/7
  Empty
Interface GigabitEthernet1/8
  Empty
Interface GigabitEthernet1/9
  Empty
Interface GigabitEthernet1/10
  Empty
Interface GigabitEthernet1/11
  Empty
Interface GigabitEthernet1/12
   Empty
Interface GigabitEthernet1/13
   Empty
Interface GigabitEthernet1/14
   Empty
Interface GigabitEthernet1/15
   Empty
Interface GigabitEthernet1/16
   Empty
Interface GigabitEthernet1/17
   Empty
Interface GigabitEthernet1/18
   Empty
Interface GigabitEthernet1/19
   Empty
Interface GigabitEthernet1/20
   Empty
switch#
switch# show ptp ?
   clock show ptp clock information
   foreign-master-record show PTP foreign master records
   parent show PTP parent properties
   port show PTP port properties
   time-property show PTP clock time property
switch# show ptp time-property
   PTP CLOCK TIME PROPERTY
   Current UTC offset valid: 0
   Current UTC offset: 35
   Leap 59: 0
   Leap 61: 0
   Time Traceable: 16
   Frequency Traceable: 32
   PTP Timescale: 1
   Time Source: Internal Osciliator
   Time Property Persistence: 300 seconds
switch# show ptp port GigabitEthernet 1/1
   PTP PORT DATASET: GigabitEthernet1/1
   Port identity: port number: 1
   PTP version: 2
   Port state: UNCALIBRATED
   Delay request interval(log mean): 5
   Announce receipt time out: 3
   Peer mean path delay(ns): 0
   Announce interval(log mean): 0
   Sync interval(log mean): 0
   Delay Mechanism: Peer to Peer
   Peer delay request interval(log mean): 0
   Sync fault limit: 500000000
switch#

802.1AS Profile Example
IE4000-SW2#show ptp clock //check profile, and clock offset
   PTP CLOCK INFO PTP
   Device Type: 802.1AS - Time Aware Bridge
   PTP Device Profile: 802.1AS Profile
   Clock Domain: 0
   ... Offset From Master(ns): 3 // this should be less than 1uS
IE4000-SW2#show ptp port FastEthernet 1/9
   PTP PORT DATASET: FastEthernet1/9
Neighbor Rate Ratio: 1 (+0 PPM) // this should be within +/-100PPM
Port 802.1AS capable: TRUE // 802.1AS capable

IE4000-SW2#show ptp parent
PTP PARENT PROPERTIES

... Clock Identity Path Trace: // path trace TLV list – the clock IDs of nodes on the clock
distribution chain from the grandmaster
Clock Identity 0: 0x0:00:00:11:11:11:11:01 // grandmaster
Clock Identity 1: 0x0:35:1A:FF:FE:DA:12:80 // 2nd clock in the path

Configuration Example

The following example configures the switch for P2P transparent mode, specifies allow-without-tlv PTP
message processing, and uses default values for all PTP interval settings:

switch(config)# ptp allow-without-tlv

The following example configures the switch for boundary clock mode using the peer delay request (pdelay-req)
mechanism and uses default values for all PTP interval settings:

switch(config)# ptp mode boundary pdelay-req

The following example configures the switch to operate in Default Profile mode and end-to-end transparent
mode and uses default values for all PTP interval settings:

switch(config)# no ptp profile
switch(config)# ptp mode e2etransparent

The following example configures the switch for Default Profile mode and boundary clock mode with the
delay_request mechanism, and uses default values for all PTP interval settings:

switch(config)# no ptp profile
switch(config)# ptp mode boundary delay-req

Configuring NTP to PTP Time Conversion

Before you begin

• Review the Guidelines and Limitations, on page 86.
• To use the NTP to PTP conversion feature, the switch must have an IP address for NTP to function.
• To use the NTP to PTP conversion feature, you must configure at least one NTP server. Configuring
three or more NTP servers allows NTP to ignore bad clocks.

Note

For information about configuring NTP, see the section Configuring NTP in the Catalyst 3750-X and 3560-X
Switch Software Configuration Guide, Release 12.2(55)SE.
• When you enter `no` with PTP port configuration commands, the specified port property is set to the default value.

• To determine the value in seconds for the `ptp` global command `interval` variable, use a logarithmic scale. Below are examples of the `interval` variable value converted to seconds with a logarithmic scale:

<table>
<thead>
<tr>
<th>Value Entered</th>
<th>Logarithmic Calculation</th>
<th>Value in Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>( 2^{-1} )</td>
<td>1/2</td>
</tr>
<tr>
<td>0</td>
<td>( 2^0 )</td>
<td>1</td>
</tr>
</tbody>
</table>

**SUMMARY STEPS**

1. Enter global configuration mode:
2. Configure the switch for Default Profile mode when the switch is in Power Profile mode. If the switch is already in Default Profile mode, this command has no effect.
3. Specify GMC-BC as the synchronization clock:
4. (Optional) Specify the BMCA priority:
5. (Optional) Specify the BC synchronization algorithm:
6. Enter interface configuration mode:
7. (Optional) Specify port settings:
8. Return to privileged EXEC mode:
9. Verify your entries:
10. (Optional) Save your entries in the configuration file:

**DETAILED STEPS**

**Step 1**
Enter global configuration mode:
```
configure terminal
```

**Step 2**
Configure the switch for Default Profile mode when the switch is in Power Profile mode. If the switch is already in Default Profile mode, this command has no effect.

```
o ptp profile power
```

**Step 3**
Specify GMC-BC as the synchronization clock:
```
ptp mode gmc-bc delay-req
```
The GMC-BC automatically selects NTP as the time source if it is available.

**Step 4**
(Optional) Specify the BMCA priority:
```
ptp priority1 priority priority2 priority
```
  • `priority1 priority`—Overides the default criteria (such as clock quality and clock class) for the most accurate master clock selection.
  • `priority2 priority`—Breaks the tie between two switches that match the default criteria. For example, enter 2 to give a switch priority over identical switches. `priority`—A priority number from 0 to 255. The default is 128.
Step 5  (Optional) Specify the BC synchronization algorithm:

```plaintext
ptp transfer {feedforward | filter {adaptive | linear}}
```

- **feedforward**—Very fast and accurate. No PDV filtering.
- **filter adaptive**—Automatically filters as much PDV as possible.
- **filter linear**—Provides a simple linear filter (default).

Step 6  Enter interface configuration mode:

```plaintext
interface interface-id
```

Step 7  (Optional) Specify port settings:

```plaintext
ptp {announce {interval value | timeout value} | delay-req interval value | enable | sync {interval value | limit value} | vlan value}
```

- **announce interval value**—Sets the logarithmic mean interval in seconds to send announce messages. The range is 0 to 4. The default is 1 (2 seconds).
- **announce timeout value**—Sets the time to announce timeout messages. The range is 2 to 10 seconds. The default is 3 (8 seconds).
- **delay-req interval value**—Sets the logarithmic mean interval in seconds for slave devices to send delay request messages when the port is in the master clock state. The range is -2 to 6. The default is -5 (1 packet every 1/32 seconds, or 32 packets per second).
- **enable**—Enables PTP on the port base module.
- **sync interval value**—Sets the logarithmic mean interval in seconds to send synchronization messages. The range is -2 to 1. The default is 1 second.
- **sync limit value**—Sets the maximum clock offset value before PTP attempts to resynchronize. The range is from 50 to 500000000 nanoseconds. The default is 500000000 nanoseconds.
- **vlan value**—Sets the PTP VLAN on a trunk port. The range is from 1 to 4094. The default is the native VLAN of the trunk port. In boundary mode, only PTP packets in PTP VLAN will be processed, PTP packets from other VLANs will be dropped. Before configuring the PTP VLAN on an interface, the PTP VLAN must be created and allowed on the trunk port.

Step 8  Return to privileged EXEC mode:

```plaintext
derend
```

Step 9  Verify your entries:

```plaintext
show running-config
```

Step 10 (Optional) Save your entries in the configuration file:

```plaintext
copy running-config startup-config
```
Example
The following example configures the switch to use the Default Profile, act as Grandmaster Clock with NTP as the time source, and use the feedforward BC synchronization algorithm:

```
switch(config)# no ptp profile power
switch(config)# ptp mode gmc-bc
switch(config)# ptp transfer feedforward
```

Verifying Configuration
Perform these steps to verify that switch is running as GMC-BC, and that NTP and PTP are synchronized:

**SUMMARY STEPS**

1. Monitor the status of NTP until NTP locks:
2. Display the status of each individual NTP server:
3. After NTP is up and running, verify that the NTP clock and the PTP clock are in sync.

**DETAILED STEPS**

**Step 1** Monitor the status of NTP until NTP locks:

```
show ntp status
```

Note especially the following fields:

- Clock is synchronized/unsynchronized.
- System poll interval—how often the NTP client sends messages in seconds.
- Last update—how many seconds since the last clock adjustment.

**Example:**

```
switch# show ntp status
Clock is synchronized, stratum 2, reference is 72.163.32.43
nominal freq is 286.1023 Hz, actual freq is 286.0738 Hz, precision is 2**21
ntp uptime is 58682700 (1/100 of seconds), resolution is 3496
clock offset is 0.0459 msec, root delay is 16.19 msec
root dispersion is 15.07 msec, peer dispersion is 0.10 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000099341 s/s
system poll interval is 1024, last update was 925 sec ago.
```

**Step 2** Display the status of each individual NTP server:

```
show ntp association
```

- The sys.peer is the currently selected reference.
- Candidates are fallback references.
- Falsetickers are bad clocks that are ignored.
Note There is a delay of several seconds from NTP picking an association to NTP declaring lock.

Example:

```
switch# show ntp association
address ref clock st when poll reach delay offset disp
+~171.68.38.65 .GPS. 1 706 1024 377 60.318 -0.255 0.166
+~171.68.38.66 .GPS. 1 450 1024 377 60.333 -0.096 0.121
-~10.81.254.202 .GPS. 1 555 1024 377 48.707 2.804 0.111
x~173.38.201.115 .GPS. 1 322 1024 377 293.19 74.409 0.107
*~72.163.32.43 .GPS. 1 37 1024 375 17.110 -0.410 0.081
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Step 3 After NTP is up and running, verify that the NTP clock and the PTP clock are in sync.

- **show clock detail** shows the NTP time.
- **show ptp clock** shows the PTP time and the BMCA dataset details.

**Example:**

```
show clock detail
Time source is NTP
show ptp clock
  PTP CLOCK INFO
  PTP Device Type: Grand Master clock - Boundary clock
  PTP Device Profile: Default Profile
  Clock Identity: 0xF4:4E:5:FF:FE:E5:95:0
  Clock Domain: 0
  Number of PTP ports: 20

  Time Transfer: Linear Filter <<< Displayed when the clock is configured as a BC or a GMC-BC
  Priority1: 128
  Priority2: 128
  Clock Quality:
    Class: 13
    Accuracy: Within 1s
    Offset (log variance): N/A
    Offset From Master(ns): 0
    Mean Path Delay(ns): 0

  Steps Removed: 0
  Local clock time: 23:16:53 UTC Jul 15 2015
```

---

### Configuration Example

```
switch# conf t
switch(config)# no ptp profile power
switch(config)# ptp mode gmc-bc
switch(config)# ptp transfer feedforward
switch(config)# end
```
Related Documents

- Cisco Industrial Ethernet 4000 switch product documentation
- Cisco Industrial Ethernet 5000 switch product documentation
- Converged Plantwide Ethernet (CPwE) Design and Implementation Guide

Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1AS Profile</td>
<td>15.2(5)E2</td>
<td>Initial support on IE 4000 switches.</td>
</tr>
<tr>
<td>Time Service Enhancements</td>
<td>15.2(4)EA1</td>
<td>Initial support on IE 5000 switches for NTP to PTP Time Conversion, Feedforward BC, and PDV Filtering.</td>
</tr>
<tr>
<td></td>
<td>15.2(4)EA</td>
<td>Initial support on IE 4000 switches for NTP to PTP Time Conversion, Feedforward BC, and PDV Filtering.</td>
</tr>
<tr>
<td>Precision Time Protocol</td>
<td>15.2(4)EC</td>
<td>Initial support of the feature on the IE 4010.</td>
</tr>
<tr>
<td></td>
<td>15.2(2)EB1</td>
<td>Initial support of the feature on the IE 5000.</td>
</tr>
<tr>
<td></td>
<td>15.2(2)EA</td>
<td>Initial support of the feature on the IE 4000.</td>
</tr>
</tbody>
</table>
Configuring SD Swap Drive

- Overview, on page 105
- Inserting and Removing the Flash Memory (SD) Card, on page 105
- Boot Loader Operation, on page 106
- IOS XE Operation, on page 106

Overview

The SD card can be used instead of the internal flash memory of the switch to update or restore configuration settings. In addition, the SD card can be used to boot the switch. You can also copy IOS software and switch configuration settings from a PC or from the switch to the SD card, and then use the SD card to copy this software and settings to other switches.

When an SD card is formatted on the switch, the card is formatted with the Disk Operating System Filing System (DOSFS), a platform-independent industry-standard file system that is supported on various Cisco switches and routers.

The switch does not support third-party SD cards or SD High Capacity (SDHC) cards. Attempting to operate the switch with a non-supported card causes the following message to be displayed:

WARNING: Non-IT SD flash detected.
Use of this card during normal operation can impact and severely degrade performance of the system.
Please use supported SD flash cards only.

If the write-protect switch on the SD card is in the lock position, the switch can read data on the card and boot from the card, but updates and files cannot be written to the card.

Inserting and Removing the Flash Memory (SD) Card

To put an SD card in the switch, make sure that the card is oriented properly, and press it into the SD card slot on the switch until the card is seated. To remove the card, press it to release it, then pull it out of the slot.

The SD card is hot-swappable, but it should not be removed from the switch during the boot process or while sdflash write is in progress.

When an SD card is inserted, a syslog message similar to the following is logged:

Mar 30 01:38:51.965: %FLASH-6-DEVICE_INSERTED: Flash device inserted
When an SD card is removed, a syslog message similar to the following is logged:

Mar 30 01:39:12.467: %FLASH-1-DEVICE_REMOVED: Flash device removed

Boot Loader Operation

The following boot loader commands can be executed on the SD card:

- **boot**—Load and boot an executable IOS image
- **cat**—Concatenate (type) file or files
- **copy**—Copy a file
- **delete**—Delete file of files
- **dir**—List files in directories
- **fsck**—Check file system consistency
- **format**—Format a file system
- **mkdir**—Create directories
- **more**—Concatenate (display) file
- **rename**—Rename a file
- **rmdir**—Delete empty directories
- **sd_init**—Initialize sd flash file systems

Note

The switch can be booted from its internal flash memory or from an SD card. The SD card takes precedence over internal flash memory. If an SD card is installed in the switch, the switch attempts to boot in the following order:

1. From the IOS image that is specified in the SD card system boot path
2. From the first IOS image in the SD card
3. From the IOS image that is specified in the internal flash memory system boot path
4. From the first IOS image in the internal flash

IOS XE Operation

You can insert or remove an SD card while the IOS is running. If you insert a supported Cisco SD card while the IOS is running, the switch validates the Cisco embedded string in the Product Name (PNM) field and displays the product number and the flash capacity of the SD card. If you remove an SD card while the IOS is running, the switch displays a warning message to alert you that the SD card has been removed.

If syslog is enabled, the system also sends a message when the SD card is inserted or removed.
When an SD card is installed in a switch, the following IOS commands operate as described:

- **write** command—Saves the running configuration. If the system boots from an SD card and you run a **write** command, the system saves the running configuration to the SD card, if the card is still installed. If the SD card has been removed, the system saves the running configuration to the internal flash memory and displays this message:
  
  WARNING: The SD flash is not present.
The running-config is saved to the on-board flash.

  NOTE: This warning message is displayed only once.

If the system boots from the internal flash memory and you then insert an SD card and run the **write** command, the system saves the running configuration to the internal flash memory.

- **boot** command—Lets you change the system boot parameters.

  If the system boots from an SD card and you run a **boot** command, the following behavior applies:

  - If the SD card is installed and the system boot path or configuration file path points to the SD card, the system boot path or configuration file path is saved to the SD card
  
  - If the SD card is installed and the system boot path or configuration file path points to the internal flash memory, the system boot path or configuration file path is saved to the internal flash memory
  
  - If the SD card has been removed and the system boot path or configuration file path points to the SD card, the system boot path or configuration file path is not saved and the following message displays:
  
  WARNING: The BOOT/config file path points to the SD flash card and the SD flash card is not present.
The environment variable(s) is not saved.

  NOTE: This warning message is displayed only once.

  If the system boots from the internal flash memory and you then insert an SD card and run the **boot** command, the following behavior applies:

  - If the system boot path or configuration file path points to the internal flash memory, the system boot path or configuration file path is saved to the internal flash memory
  
  - If the system boot path or configuration file path points to the SD card, the system boot path or configuration file path is saved to the SD card and the following message is displayed:
  
  WARNING: The BOOT/config file path points to the SD flash card.
The environment variable(s) is saved onto the SD flash card.

  NOTE: This warning message is displayed only once.

  - If the SD card has been removed and the system boot path or configuration file path points to the SD card, the system boot path or configuration file path is not saved and the following message is displayed:
  
  WARNING: The BOOT/config file path points to the SD flash card and the SD flash card is not present.
The environment variable(s) is not saved.

  NOTE: This warning message is displayed only once.
- **sync** command—Copies the IOS image directory (which includes the IOS image file, FPGA image files, Device Manager files, and Profinet/CIP configuration files), the config.text IOS configuration file, the vlan.dat VLAN configuration file, and IOS boot parameters from the internal flash memory to the SD card or from the SD card to the internal flash memory. This command verifies that the IOS image is appropriate for the switch model and that enough destination flash memory is present, and aborts the sync process if a potential problem is detected. The **sync** command obtains the source IOS image directory path and source IOS configuration files path from the IOS boot parameters on the source flash device that is specified in the **sync** command. By default, this command overwrites the destination IOS image directory and IOS configuration files. The “save-old-files” option can be used to override this default behavior. If the running configuration has not been saved and you run the **sync** command, the switch provides the option for you to save the running configuration before the command executes.

The **sync** command options are:

- Switch# **sync flash: sdflash:** —Sync IOS image directory, configuration files, and boot parameters from internal flash memory to SD card.
- Switch# **sync sdflash: flash:** —Sync IOS image directory, configuration files, and boot parameters from SD card to internal flash memory.
- Switch# **sync flash: sdflash: ios-image-name** —Sync boot IOS image from Flash to SDFlash.
- Switch# **sync sdflash: flash: ios-image-name** —Sync boot IOS image from SDFlash to Flash.
- Switch# **sync sdflash: flash: skip [config|env-variable|ios-image]** —Sync either the IOS Config, the environment variables, or IOS image directory from SD card to internal flash memory.
CHAPTER 6

Configuring Resilient Ethernet Protocol

- Finding Feature Information, on page 109
- Resilient Ethernet Protocol Overview, on page 109
- How to Configure Resilient Ethernet Protocol, on page 114
- Monitoring Resilient Ethernet Protocol Configurations, on page 122

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Resilient Ethernet Protocol Overview

Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, handle link failures, and improve convergence time. REP controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment. REP provides a basis for constructing more complex networks and supports VLAN load balancing.

Note

REP configuration on downlink ports is supported starting with Cisco IOS XE Fuji 16.9.1.

REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (non-edge) segment ports and two user-configured edge ports. A switch can have no more than two ports that belong to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium, but on any link, only two ports can belong to the same segment. REP is supported only on Trunk ports.

The figure below shows an example of a segment consisting of six ports spread across four switches. Ports E1 and E2 are configured as edge ports. When all ports are operational (as in the segment on the left), a single
port is blocked, shown by the diagonal line. This blocked port is also known as the Alternate port (ALT port). When there is a failure in the network, the blocked port returns to the forwarding state to minimize network disruption.

*Figure 14: REP Open Segment*

The segment shown in the figure above is an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop, and you can safely connect the segment edges to any network. All hosts connected to switches inside the segment have two possible connections to the rest of the network through the edge ports, but only one connection is accessible at any time. If a failure occurs on any segment or on any port on a REP segment, REP unblocks the ALT port to ensure that connectivity is available through the other gateway.

The segment below is a closed segment, also known as Ring Segment, with both edge ports located on the same router. With this configuration, you can create a redundant connection between any two routers in the segment.

*Figure 15: REP Ring Segment*

REP segments have the following characteristics:

- If all ports in a segment are operational, one port (referred to as the ALT port) is in the blocked state for each VLAN. If VLAN load balancing is configured, two ALT ports in the segment control the blocked state of VLANs.

- If a port is not operational, and cause a link failure, all ports forward traffic on all VLANs to ensure connectivity.

- In case of a link failure, alternate ports are unblocked as quickly as possible. When the failed link is restored, a logically blocked port per VLAN is selected with minimal disruption to the network.

You can construct almost any type of network based on REP segments.
In access ring topologies, the neighboring switch might not support REP as shown in the figure below. In this case, you can configure the non-REP facing ports (E1 and E2) as edge no-neighbor ports. The edge no-neighbor port can be configured to send an STP topology change notice (TCN) towards the aggregation switch.

*Figure 16: Edge No-Neighbor Ports*

REP has these limitations:

- You must configure each segment port; an incorrect configuration can cause forwarding loops in the networks.
- REP can manage only a single failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.
- You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

**Link Integrity**

REP does not use an end-to-end polling function between edge ports to verify link integrity. It implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All the VLANs are blocked on an interface until the neighbor is detected. After the neighbor is identified, REP determines which neighbor port should become the alternate port and which ports should forward traffic.

Each port in a segment has a unique port ID. The port ID format is similar to that used by the spanning tree algorithm: a port number (unique on the bridge) associated to a MAC address (unique in the network). When a segment port is coming up, its LSL starts sending packets that include the segment ID and the port ID. The port is declared as operational after it performs a three-way handshake with a neighbor in the same segment.

A segment port does not become operational if:

- No neighbor has the same segment ID.
- More than one neighbor has the same segment ID.
- A neighbor does not acknowledge a local port as a peer.

Each port creates an adjacency with its immediate neighbor. After the neighbor adjacencies are created, the ports negotiate with each other to determine the blocked port for the segment, which will function as the
alternate port. All the other ports become unblocked. By default, REP packets are sent to a bridge protocol 
data unit-class MAC address. The packets can also be sent to a Cisco multicast address, which is used only 
to send blocked port advertisement (BPA) messages when there is a failure in the segment. The packets are 
dropped by the devices not running REP.

**Fast Convergence**

REP runs on a physical link basis and not on a per-VLAN basis. Only one hello message is required for all 
the VLANs, and this reduces the load on the protocol. We recommend that you create VLANs consistently 
on all the switches in a given segment and configure the same allowed VLANs on the REP trunk ports. To 
avoid the delay introduced by relaying messages in software, REP also allows some packets to be flooded to 
a regular multicast address. These messages operate at the hardware flood layer (HFL) and are flooded to the 
entire network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. 
You can control flooding of these messages by configuring an administrative VLAN for the entire domain or 
for a particular segment.

**VLAN Load Balancing**

One edge port in the REP segment acts as the primary edge port; and another as the secondary edge port. It 
is the primary edge port that always participates in VLAN load balancing in the segment. REP VLAN balancing 
is achieved by blocking some VLANs at a configured alternate port and all the other VLANs at the primary 
edge port. When you configure VLAN load balancing, you can specify the alternate port in one of three ways:

- By entering the port ID of the interface. To identify the port ID of a port in the segment, enter the `show 
  interface rep detail` interface configuration command for the port.
- By entering the `preferred` keyword to select the port that you previously configured as the preferred 
  alternate port with the `rep segment segment-id preferred` interface configuration command.
- By entering the neighbor offset number of a port in the segment, which identifies the downstream neighbor 
  port of an edge port. The neighbor offset number range is \(-256\) to \(+256\); a value of \(0\) is invalid. The 
  primary edge port has an offset number of \(1\); positive numbers above \(1\) identify downstream neighbors 
  of the primary edge port. Negative numbers indicate the secondary edge port (offset number \(-1\)) and its 
  downstream neighbors.

**Note**

Configure offset numbers on the primary edge port by identifying a port’s 
downstream position from the primary (or secondary) edge port. Never enter an 
offset value of \(1\) because that is the offset number of the primary edge port.

The following figure shows neighbor offset numbers for a segment, where E1 is the primary edge port 
and E2 is the secondary edge port. The red numbers inside the ring are numbers offset from the primary 
edge port; the black numbers outside of the ring show the offset numbers from the secondary edge port. 
Note that you can identify all the ports (except the primary edge port) by either a positive offset number 
(downstream position from the primary edge port) or a negative offset number (downstream position 
from the secondary edge port). If E2 became the primary edge port, its offset number would then be \(1\) 
and E1 would be \(-1\).
When the REP segment is complete, all the VLANs are blocked. When you configure VLAN load balancing, you must also configure triggers in one of two ways:

- Manually trigger VLAN load balancing at any time by entering the `rep preempt segment segment-id` privileged EXEC command on the switch that has the primary edge port.
- Configure a preempt delay time by entering the `rep preempt delay seconds` interface configuration command. After a link failure and recovery, VLAN load balancing begins after the configured preemption time period elapses. Note that the delay timer restarts if another port fails before the time has elapsed.

**Note**

When VLAN load balancing is configured, it does not start working until triggered by either manual intervention or a link failure and recovery.

When VLAN load balancing is triggered, the primary edge port sends out a message to alert all the interfaces in the segment about the preemption. When the secondary port receives the message, the message is sent to the network to notify the alternate port to block the set of VLANs specified in the message and to notify the primary edge port to block the remaining VLANs.

You can also configure a particular port in the segment to block all the VLANs. Only the primary edge port initiates VLAN load balancing, which is not possible if the segment is not terminated by an edge port on each end. The primary edge port determines the local VLAN load-balancing configuration.

Reconfigure the primary edge port to reconfigure load balancing. When you change the load-balancing configuration, the primary edge port waits for the `rep preempt segment` command or for the configured preempt delay period after a port failure and recovery, before executing the new configuration. If you change an edge port to a regular segment port, the existing VLAN load-balancing status does not change. Configuring a new edge port might cause a new topology configuration.

**Spanning Tree Interaction**

REP does not interact with STP, but it can coexist. A port that belongs to a segment is removed from spanning tree control and STP BPDUs are not accepted or sent from segment ports. Therefore, STP cannot run on a segment.

To migrate from an STP ring configuration to REP segment configuration, begin by configuring a single port in the ring as part of the segment and continue by configuring contiguous ports to minimize the number of segments. Each segment always contains a blocked port, so multiple segments means multiple blocked ports.
and a potential loss of connectivity. When the segment has been configured in both directions up to the location of the edge ports, you then configure the edge ports.

**REP Ports**

REP segments consist of Failed, Open, or Alternate ports:

- A port configured as a regular segment port starts as a failed port.
- After the neighbor adjacencies are determined, the port transitions to alternate port state, blocking all the VLANs on the interface. Blocked-port negotiations occur, and when the segment settles, one blocked port remains in the alternate role and all the other ports become open ports.
- When a failure occurs in a link, all the ports move to the Failed state. When the Alternate port receives the failure notification, it changes to the Open state, forwarding all the VLANs.

A regular segment port converted to an edge port, or an edge port converted to a regular segment port, does not always result in a topology change. If you convert an edge port into a regular segment port, VLAN load balancing is not implemented unless it has been configured. For VLAN load balancing, you must configure two edge ports in the segment.

A segment port that is reconfigured as a spanning tree port restarts according to the spanning tree configuration. By default, this is a designated blocking port. If PortFast is configured or if STP is disabled, the port goes into the forwarding state.

**How to Configure Resilient Ethernet Protocol**

A segment is a collection of ports connected to one another in a chain and configured with a segment ID. To configure REP segments, configure the REP administrative VLAN (or use the default VLAN 1) and then add the ports to the segment, using interface configuration mode. You should configure two edge ports in a segment, with one of them being the primary edge port and the other the secondary edge port by default. A segment should have only one primary edge port. If you configure two ports in a segment as primary edge ports, for example, ports on different switches, the REP selects one of them to serve as the segment's primary edge port. If required, you can configure the location to which segment topology change notices (STCNs) and VLAN load balancing are to be sent.

**Default REP Configuration**

REP is disabled on all the interfaces. When enabled, the interface is a regular segment port unless it is configured as an edge port.

When REP is enabled, the task of sending segment topology change notices (STCNs) is disabled, all the VLANs are blocked, and the administrative VLAN is VLAN 1.

When VLAN load balancing is enabled, the default is manual preemption with the delay timer disabled. If VLAN load balancing is not configured, the default after manual preemption is to block all the VLANs in the primary edge port.

**REP Configuration Guidelines**

Follow these guidelines when configuring REP:
• We recommend that you begin by configuring one port and then configure contiguous ports to minimize the number of segments and the number of blocked ports.

• If more than two ports in a segment fail when no external neighbors are configured, one port goes into a forwarding state for the data path to help maintain connectivity during configuration. In the `show rep interface` command output, the Port Role for this port shows as “Fail Logical Open”; the Port Role for the other failed port shows as “Fail No Ext Neighbor”. When the external neighbors for the failed ports are configured, the ports go through the alternate port state transitions and eventually go to an open state or remain as the alternate port, based on the alternate port selection mechanism.

• REP ports must be Layer 2 IEEE 802.1Q or Trunk ports.

• We recommend that you configure all trunk ports in the segment with the same set of allowed VLANs.

• Be careful when configuring REP through a Telnet connection. Because REP blocks all VLANs until another REP interface sends a message to unblock it. You might lose connectivity to the router if you enable REP in a Telnet session that accesses the router through the same interface.

• You cannot run REP and STP on the same segment or interface.

• If you connect an STP network to a REP segment, be sure that the connection is at the segment edge. An STP connection that is not at the edge could cause a bridging loop because STP does not run on REP segments. All STP BPDU’s are dropped at REP interfaces.

• You must configure all trunk ports in the segment with the same set of allowed VLANs, or a misconfiguration occurs.

• If REP is enabled on two ports on a switch, both ports must be either regular segment ports or edge ports. REP ports follow these rules:
  • There is no limit to the number of REP ports on a switch; however, only two ports on a switch can belong to the same REP segment.
  • If only one port on a switch is configured in a segment, the port should be an edge port.
  • If two ports on a switch belong to the same segment, they must be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.
  • If two ports on a switch belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

• REP interfaces come up in a blocked state and remain in a blocked state until they are safe to be unblocked. You need to be aware of this status to avoid sudden connection losses.

• REP sends all LSL PDUs in untagged frames on the native VLAN. The BPA message sent to the Cisco multicast address is sent on the administration VLAN, which is VLAN 1 by default.

• You can configure how long a REP interface remains up without receiving a hello from a neighbor. You can use the `rep lsl-age-timer` value interface configuration command to set the time from 120 ms to 10000 ms. The LSL hello timer is then set to the age-timer value divided by 3. In normal operation, three LSL hellos are sent before the age timer on the peer switch expires and checks for hello messages.
  • EtherChannel port channel interfaces do not support LSL age-timer values less than 1000 ms. If you try to configure a value less than 1000 ms on a port channel, you receive an error message and the command is rejected.
Configuring the REP Administrative VLAN

To avoid the delay created by link-failure messages, and VLAN-blocking notifications during load balancing, REP floods packets to a regular multicast address at the hardware flood layer (HFL). These messages are flooded to the whole network, and not just the REP segment. You can control the flooding of these messages by configuring an administrative VLAN for the whole domain or for a particular segment.

Follow these guidelines when configuring the REP administrative VLAN:

- If you do not configure an administrative VLAN, the default is VLAN 1.
- You can configure one admin VLAN on the switch for all segments or configure an admin VLAN per segment.
- The administrative VLAN cannot be the RSPAN VLAN.

To configure the REP administrative VLAN, follow these steps, beginning in privileged EXEC mode:

**SUMMARY STEPS**

1. configure terminal
2. rep admin vlan vlan-id
3. end
4. show interface [interface-id] rep detail
5. copy running-config startup config

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Example:</td>
<td><strong>device# configure terminal</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>rep admin vlan vlan-id</strong></td>
</tr>
<tr>
<td>Example:</td>
<td><strong>device(config)# rep admin vlan 2</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
</tr>
<tr>
<td>3</td>
<td><code>end</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>device(config)# end</code></td>
</tr>
<tr>
<td>4</td>
<td><code>show interface [interface-id] rep detail</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>device# show interface gigabitethernet1/1 rep detail</code></td>
</tr>
<tr>
<td>5</td>
<td><code>copy running-config startup config</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>device# copy running-config startup config</code></td>
</tr>
</tbody>
</table>

### Configuring a REP Interface

To configure REP, enable REP on each segment interface and identify the segment ID. This task is mandatory, and must be done before other REP configurations. You must also configure a primary and secondary edge port on each segment. All the other steps are optional.

Follow these steps to enable and configure REP on an interface:

**SUMMARY STEPS**

1. `configure terminal`
2. `interface interface-id`
3. `switchport mode trunk`
4. `rep segment segment-id [edge [no-neighbor] [primary]] [preferred]`
5. `rep stcn [interface interface id] [segment id-list | stp]`
6. `rep block port [id port-id | neighbor-offset | preferred] vlan {vlan-list | all}`
7. `rep preempt delay seconds`
8. `rep isl-age-timer value`
9. `end`
10. `show interface [interface-id] rep [detail]`
11. `copy running-config startup-config`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>device# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>interface interface-id</td>
<td>Specifies the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface).</td>
</tr>
<tr>
<td></td>
<td>Example: device# interface gigabitethernet1/1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode trunk</td>
<td>Configures the interface as a Layer 2 trunk port.</td>
</tr>
<tr>
<td></td>
<td>Example: device# switchport mode trunk</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>rep segment segment-id [edge [no-neighbor] [primary]] [preferred]</td>
<td>Enables REP on the interface and identifies a segment number. The segment ID range is from 1 to 1024.</td>
</tr>
<tr>
<td></td>
<td>Example: device# rep segment 1 edge no-neighbor primary</td>
<td></td>
</tr>
</tbody>
</table>

**Note** You must configure two edge ports, including one primary edge port, for each segment.

These optional keywords are available:

- (Optional) **edge**—Configures the port as an edge port. Each segment has only two edge ports. Entering the keyword `edge` without the keyword `primary` configures the port as the secondary edge port.

- (Optional) **primary**—Configures the port as the primary edge port, the port on which you can configure VLAN load balancing.

- (Optional) **no-neighbor**—Configures a port with no external REP neighbors as an edge port. The port inherits all the properties of an edge port, and you can configure the properties the same way you would for an edge port.

**Note** Although each segment can have only one primary edge port, if you configure edge ports on two different switches and enter the keyword `primary` on both the switches, the configuration is valid. However, REP selects only one of these ports as the segment primary edge port. You can identify the primary edge port for a segment by entering the `show rep topology` privileged EXEC command.

- (Optional) **preferred**—Indicates that the port is the preferred alternate port or the preferred port for VLAN load balancing.

**Note** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives the port a slight edge over equal contenders. The alternate port is usually a previously failed port.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5</strong></td>
<td>`rep stcn {interface interface id</td>
<td>segment id-list</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>device# rep stcn segment 25-50</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
<td>Spanning Tree (MST) mode is required on edge no-neighb or nodes when <code>rep stcn stp</code> command is configured for sending STCNs to STP networks.</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>`rep block port {id port-id</td>
<td>neighbor-offset</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>device# rep block port id 0009001818D68700 vlan 1-100</code></td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
<td>Because you enter the <code>rep block port</code> command at the primary edge port (offset number 1), you cannot enter an offset value of 1 to identify an alternate port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Because you enter the <code>rep block port</code> command at the primary edge port (offset number 1), you cannot enter an offset value of 1 to identify an alternate port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Setting Manual Preemption for VLAN Load Balancing

If you do not enter the `rep preempt delay seconds` interface configuration command on the primary edge port to configure a preemption time delay, the default is to manually trigger VLAN load balancing on the segment. Be sure that all the other segment configurations have been completed before manually preempting VLAN load balancing. When you enter the `rep preempt delay segment segment-id` command, a confirmation message is displayed before the command is executed because preemption might cause network disruption.
SUMMARY STEPS

1. configure terminal
2. rep preempt segment segment-id
3. show rep topology segment segment-id
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>rep preempt segment segment-id</td>
<td>Manually triggers VLAN load balancing on the segment.</td>
</tr>
<tr>
<td></td>
<td>Example: device# rep preempt segment 100</td>
<td>The command will cause a momentary traffic disruption. Do you still want to continue? [confirm]</td>
</tr>
<tr>
<td>3.</td>
<td>show rep topology segment segment-id</td>
<td>(Optional) Displays REP topology information.</td>
</tr>
<tr>
<td></td>
<td>Example: device# show rep topology segment 100</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>end</td>
<td>Exits privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: device# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuring SNMP Traps for REP

You can configure a router to send REP-specific traps to notify the Simple Network Management Protocol (SNMP) server of link-operational status changes and port role changes.

SUMMARY STEPS

1. configure terminal
2. snmp mib rep trap-rate value
3. end
4. show running-config
5. copy running-config startup-config
### Monitoring Resilient Ethernet Protocol Configurations

You can display the rep interface and rep topology details using the commands in this topic.

#### SUMMARY STEPS

1. `show interface [interface-id] rep [detail]`
2. `show rep topology [segment segment-id] [archive] [detail]`

#### DETAILED STEPS

**Step 1**

`show interface [interface-id] rep [detail]`

Displays REP configuration and status for an interface or for all the interfaces.

- (Optional) `detail`—Displays interface-specific REP information.

**Example:**
Device# show interfaces TenGigabitEthernet4/1 rep detail

TenGigabitEthernet4/1 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136

Step 2

show rep topology [segment segment-id] [archive] [detail]

Displays REP topology information for a segment or for all the segments, including the primary and secondary edge ports in the segment.

• (Optional) archive—Displays the last stable topology.

  Note An archive topology is not retained when the switch reloads.

• (Optional) detail—Displays detailed archived information.

Example:

Device# show rep topology

REP Segment 1
BridgeName PortName Edge Role
----------------- --------- ---- ----
10.64.106.63 Te5/4 Pri Open
10.64.106.228 Te3/4 Open
10.64.106.228 Te3/3 Open
10.64.106.67 Te4/3 Open
10.64.106.67 Te4/4 Alt
10.64.106.63 Te4/4 Sec Open

REP Segment 3
BridgeName PortName Edge Role
----------------- --------- ---- ----
10.64.106.63 Gi50/1 Pri Open
SVT_3400_2 Gi0/3 Open
SVT_3400_2 Gi0/4 Open
10.64.106.68 Gi40/2 Open
10.64.106.68 Gi40/1 Open
10.64.106.63 Gi50/2 Sec Alt
Common Industrial Protocol (CIP)

- CIP Restrictions, on page 125
- Enabling CIP, on page 125
- Additional References, on page 126

CIP Restrictions

CIP can be enabled on only one VLAN on the switch.

Enabling CIP

Before you begin

By default, CIP is not enabled.

SUMMARY STEPS

1. Configure Terminal
2. cip security  { password password | window timeout value }
3. interface vlan 20
4. cip enable
5. end
6. show running-config
7. copy running-config startup-config
8. show cip  { connection | faults | file | miscellaneous | object | security | session | status }
9. debug cip  { assembly | connection manager | errors | event | file | io | packet | request response | security | session | socket }

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure Terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>`cip security { password password</td>
<td>window timeout value }`</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface vlan 20</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>cip enable</td>
<td>Enables CIP on a VLAN.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show running-config</td>
<td>Verifies your entries.</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
<tr>
<td>Step 8</td>
<td>show cip { connection</td>
<td>faults</td>
</tr>
<tr>
<td>Step 9</td>
<td>debug cip { assembly</td>
<td>connection manager</td>
</tr>
</tbody>
</table>

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS basic commands</td>
<td><em>Cisco IOS Configuration Fundamentals Command Reference</em></td>
</tr>
</tbody>
</table>

#### Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td></td>
</tr>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td></td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIBs Link</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</td>
<td><a href="https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index?dtid=ossdcde000283">https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index?dtid=ossdcde000283</a></td>
</tr>
</tbody>
</table>
## Technical Assistance

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

---

---
Modicon Communication Bus (MODBUS)

- MODBUS Overview, on page 129
- Configuring MODBUS, on page 129
- Displaying MODBUS Information, on page 130

MODBUS Overview

Modicon Communication Bus (MODBUS) is an application layer protocol for client-server communication between a switch (server) and a device in the network running MODBUS client software (client). You can use MODBUS over a serial line to connect a computer to a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems.

MODBUS also runs on Ethernet TCP/IP networks. Use MODBUS TCP over an Ethernet network when connecting the switch to devices such as intelligent electronic devices (IEDs), distributed controllers, substation routers, IP phones, Wireless Access Points, and other network devices such as redundant substation switches.

The client can be an IED or a human machine interface (HMI) application that remotely configures and manages devices running MODBUS TCP. The switch functions as the server.

The switch encapsulates a request or response message in a MODBUS TCP application data unit (ADU). A client sends a message to a TCP port on the switch.

Configuring MODBUS

The MODBUS TCP server listens for MODBUS client requests on TCP port 502 by default. Port 502 is enabled when MODBUS server is started unless you configure a different port for MODBUS communications.

The MODBUS server is disabled by default.

To configure MODBUS:

Before you begin

If a firewall or other security services are enabled, the switch TCP port might be blocked, and the switch and the client cannot communicate. If a firewall and other security services are disabled, a denial-of-service attack might occur on the switch. To add security when using MODBUS TCP, configure an ACL to permit traffic from specific clients or configure QoS to rate-limit traffic.
**Step 1** Enter global configuration mode:

`configure terminal`

**Step 2** Enable MODBUS TCP on the switch:

`scada modbus tcp server`

To disable MODBUS on the switch and return to the default settings, enter the `no scada modbus tcp server` global configuration command.

The system displays a message to warn you that starting the MODBUS TCP server is a security risk:

`WARNING: Starting Modbus TCP server is a security risk. Please understand the security issues involved before proceeding further. Do you still want to start the server? [yes/no]:`

**Step 3** Enter `yes` to confirm that you understand the security issues and to proceed with starting the server.

**Step 4** (Optional) Set the TCP port to which clients send messages:

`scada modbus tcp server port tcp-port-number`

The range for `tcp-port-number` is 1 to 65535. The default is 502.

**Step 5** (Optional) Set the number of simultaneous connection requests sent to the switch:

`scada modbus tcp server connection connection-requests`

The range for `connection-requests` is 1 to 5. The default is 1.

**Step 6** Return to privileged EXEC mode:

`end`

---

**Example**

```bash
Switch# configure terminal
Switch(config)# scada modbus tcp server
WARNING: Starting Modbus TCP server is a security risk. Please understand the security issues involved before proceeding further. Do you still want to start the server? [yes/no]: y
Switch(config)# end
```

---

**Displaying MODBUS Information**

Use the commands listed below to display information for MODBUS TCP.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show scada modbus tcp server</code></td>
<td>Displays the server information and statistics</td>
</tr>
<tr>
<td><code>show scada modbus tcp server connections</code></td>
<td>Shows information and statistics for each client connection</td>
</tr>
</tbody>
</table>
### Command

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear scada modbus tcp server statistics</td>
<td>Clears all the statistics for the Modbus server, including statistics for each client connection</td>
</tr>
</tbody>
</table>

Switch# `show scada modbus tcp server`
Summary: enabled, running, process id 142
Conn Stats: listening on port 801, 4 max simultaneous connections
0 current client connections
0 total accepted connections, 0 accept connection errors
0 closed connections, 0 close connection errors
Send Stats: 0 tcp msgs sent, 0 tcp bytes sent, 0 tcp errors
0 responses sent, 0 exceptions sent, 0 send errors
Recv Stats: 0 tcp msgs received, 0 tcp bytes received, 0 tcp errors
0 requests received, 0 receive errors
Displaying MODBUS Information
Serviceability and Zeroization Features for IoT

The following features are included in the Cisco IOS-XE release 16.11.1 for the Internet of Things (IoT) products.

Serviceability Features

Cisco IOS-XE `show tech-support` functionality is extensively used by technical support for various platforms that run IOS-XE and comprises of a library of shell scripts that spawn various show commands to obtain the state of the device for debugging purposes. The tech-support output is very critical in debugging various problems in the system and has been a key component in debug infrastructure.

The `show tech-support` series of commands has been a part of the Cisco IOS and IOS-XE releases since release 4.0(0)N1(1a). The IoT products follow the core IOS-XE software functionality.

The output from the `show tech-support` command is very long. To better manage this output, you can redirect the output to a file (for example, `show tech-support > filename`) in the local writable storage file system or the remote file system.

You can use one of the following redirection methods:
- `>` filename — Redirects the output to a file.
- `>>` filename — Redirects the output to a file in append mode.

Examples

This example shows how to display technical support information:

```
device# show tech-support
```

This example shows how to redirect the technical support information to a file:

```
device# show tech-support > bootflash:TechSupport.txt
```

This example shows how to display the brief technical support information for the device:
device# show tech-support brief

This example shows how to display the technical support information for a specific feature:

device# show tech-support aaa

This example shows how to display the commands used to generate the technical support information:

device# show tech-support commands

For Cisco IOS-XE release 16.11.1, improvements were made to improve the monitoring capabilities of forwarding plane (QFP) using CLI and SNMP. show platform resources would display QFP details and an SNMP MIB walk would include all QFP objects including memory related MIB objects. show inventory and show inventory oid will display the related Forwarding processor and its OID information.

show tech-support is enhanced to include the following CLIs:

show platform hardware qfp active infrastructure punt config cause
show platform hardware qfp active infrastructure punt internal-interface
show platform hardware qfp active interface if-name internal10/0/rp:0
show platform hardware qfp active interface if-name internal10/0/recycle:0
show platform hardware qfp active interface if-name internal10/0/crypto:0
show platform hardware qfp active infrastructure udb internal10/0/rp:0 input config
show platform hardware qfp active infrastructure udb internal10/0/recycle:0 input config
show platform hardware qfp active infrastructure udb internal10/0/crypto:0 input config
show platform hardware qfp active infrastructure udb internal10/0/rp:0 output config
show platform hardware qfp active infrastructure udb internal10/0/recycle:0 output config
show platform hardware qfp active infrastructure udb internal10/0/crypto:0 output config
show platform hardware qfp active infrastructure punt statistics interface 1
show platform hardware qfp active infrastructure punt statistics interface 2
show platform hardware qfp active interface if-name internal10/0/rp:0 statistics
show platform hardware qfp active interface if-name internal10/0/recycle:0 statistics
show platform hardware qfp active interface if-name internal10/0/crypto:0 statistics
show platform hardware qfp active infrastructure punt statistics type per-cause
show platform hardware qfp active infrastructure punt statistics type global-drop
show platform hardware qfp active infrastructure punt statistics type punt-drop
show platform hardware qfp active infrastructure punt statistics type inject-drop
show platform hardware qfp active statistics drop
show platform hardware qfp active system state
show platform hardware qfp active system transactions
show platform hardware qfp active datapath infrastructure time basic
show platform hardware qfp active infrastructure exmem statistics
show platform hardware qfp active infrastructure exmem statistics user
show platform hardware qfp active infrastructure exmem resource
show platform hardware qfp active infrastructure exmem region
show platform hardware qfp active infrastructure exmem table
show platform hardware qfp active infrastructure bqs status
show platform hardware qfp active feature acl control
show platform hardware qfp active feature acl tree
show platform hardware qfp active feature tunnel state
show platform hardware qfp active feature etspan state
show platform hardware qfp active feature ess state
show platform hardware qfp active feature ipfrag global
show bootlog FP active
show bootlog RP active
show platform software diagnostic chassis-manager R0 cpld
show platform software diagnostic chassis-manager R0 status
show platform software ipc queue-based chassis-manager R0 connection
show platform software ipc stream-based ios RP active connection
show platform software ipc stream-based ios RP active manager
show platform software process environment ios rp active
show power
show license tech support
show license summary

New CLIs that have been added are:

show tech-support l2
show tech-support acl
show tech-support dhcp
show tech-support port-channel
show tech-support private-vlan
show tech-support vlan
show tech-support confidential

Detailed information on all of these commands can be found in the Catalyst 9500 Switches Command Reference:

Device Zeroization or Declassification

Zeroization consists of erasing any and all potentially sensitive information in the device. This function is also referred to as Declassification. This includes erasure of Main memory, cache memories, and other memories containing packet data, NVRAM, and Flash memory. The process of zeroization is launched upon the initiation of a user command and a subsequent trigger.

On the device, the Reset button is used exclusively for triggering the Zeroization/Declassification process which zeroize and erase device configuration files or entire flash file system depending on the option provided under "service declassify".

The zeroization process starts as soon as the reset button is pressed down. The CLI command, "service declassify", is used to set the desired action in response to reset button press. To prevent accidental erasure of the system configuration/image, the default setting is set to "no service declassify".

Command Line Interface

There are two levels of zeroization actions, erase-nvram and erase-all. The following CLI shows the options:

device(config)#service declassify ?
erase-nvram Enable erasure of device configuration as declassification action. Default is no erasure.
erase-all Enable erasure of both flash and nvram file systems as part of declassification. Default is no erasure

The “erase-nvram” level of declassification process searches for the following files, and erases the ones found.

• flash:/nvram_config
• flash:/vlan.dat

This also erases the complete NVRAM filesystem, therefore, all configurations, including startup and running configurations will get deleted.

The perma-locked bootable image(s) in the flash file system will still be available and can be used for booting the device.

The “erase-all” level of zeroization process erases the entire flash file system. This also wipes out all files and perma-locked bootable image(s). All interfaces are shut down before this process. Here, erasure of individual files in the flash file system is not possible and the only option is to erase the entire flash file system. This also erases packet data, ASIC data and processors related caches along with scrubbing Main memory.
With any level of zeroization, the device always fall back to the ROMMON prompt on the console after the erasure of configuration files or flash file system.

**Zeroization Trigger**

The user needs to press the button after configuring the level of erasure required by the above CLI commands. To make sure that the button press has been identified by underlying software, the user needs to press and hold it for ONE second, or at least till the zero LED starts blinking.

**Zeroization Support in bootloader**

The zeroization process may take several minutes, depending on several system parameters such as the size of DDR memory, EMMC disk size, etc.

It is possible that the zeroization may get interrupted by a power cycle before it completes. Since the primary OS image on EMMC itself gets purged during zeroization, it becomes impossible to continue zeroization after a power cycle. To solve this, zeroization support has been in the bootloader and will run it to completion even if it gets interrupted by power cycles.

The IOS-XE sets a flag in the PMU persistent register before relinquishing control to the bootloader through a reboot. The bootloader then sets an internal variable in QSPI flash so that it is persistent even across power cycles.
Embedded Packet Capturer

- Embedded Packet Capturer Overview, on page 137
- Configuring Embedded Packet Capture, on page 137
- Monitoring and Maintaining Captured Data, on page 138
- Feature History, on page 139

Embedded Packet Capturer Overview

Embedded Packet Capture (EPC) is an onboard packet capture facility that allows network administrators to capture packets flowing to, through, and from the device and to analyze them locally or save and export them for offline analysis. The captured data is stored in .pcap file format, which can be analyzed by using a standard packet analysis tool such as Wireshark. This feature facilitates troubleshooting by gathering information about the packet format. This feature also facilitates application analysis and security.

Embedded Packet Capture (EPC) provides an embedded systems management facility that helps in tracing and troubleshooting packets. The network administrator may define the capture buffer size and the maximum number of bytes of each packet to capture. The packet capture rate can be throttled using further administrative controls. For example, options allow for filtering the packets to be captured using an Access Control List and, optionally, further defined by specifying a maximum packet capture rate or by specifying a sampling interval.

Note
Packet Capture is supported only on physical interfaces with the ingress direction.

Configuring Embedded Packet Capture

Follow these steps to configure Embedded Packet Capture:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enable privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>monitor capture</td>
<td>Configure a monitor capture specifying an access list as the core filter for the packet capture.</td>
</tr>
</tbody>
</table>

access-list access-list-name

monitor capture capture-name access-list access-list-name
### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Enable privileged EXEC mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>show monitor capture capture-buffer-name buffer dump</td>
</tr>
<tr>
<td>(Optional) Display a hexadecimal dump of captured packet and its metadata.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>show monitor capture capture-buffer-name parameter</td>
</tr>
<tr>
<td>(Optional) Display a list of commands that were used to specify the capture.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>debug epc capture-point</td>
</tr>
<tr>
<td>(Optional) Enable packet capture point debugging.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>debug epc provision</td>
</tr>
<tr>
<td>(Optional) Enables packet capture provisioning debugging.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>exit</td>
</tr>
<tr>
<td>Exit privileged EXEC mode.</td>
<td></td>
</tr>
</tbody>
</table>
### Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded Packet Capture</td>
<td>Cisco IOS XE 16.11.1</td>
<td>Initial support on Cisco Catalyst IE 3200, 3300, 3400, and Cisco Embedded Service 3300 Series Switches</td>
</tr>
</tbody>
</table>
REP Fast Overview

The Resilient Ethernet Protocol (REP) Fast feature allows faster link failure detection and convergence on the switch copper Gigabit Ethernet (GE) ports.

This document describes only REP Fast. For complete information about REP and how to configure it, refer to Configuring Resilient Ethernet Protocol.

REP was originally designed for Fast Ethernet (FE 10/100) ports. Link down detection time on FE ports is 10 milliseconds (ms) and convergence time is about 50 ms. On Fiber GE ports, link down time is 10 ms, but on GE copper interfaces, the IEEE 802.3 specification mandates the link drop detection and recovery times to be 750 ms for a master and 350 ms for a slave. As a result, link loss and recovery can be detected a lot more quickly on GE fiber interfaces than on corresponding copper interfaces. This in turn means that the convergence time for REP is a lot higher when using GE copper interfaces.

To improve link down detection time, a real-time operating system (RTOS)/beacon mechanism is implemented to trigger faster link failure detection (within 5-10 ms) when a REP interface is configured for REP Fast mode. RTOS has two timers for each REP interface. The first timer is triggered every 3 ms to transmit the beacon frame to the neighbor node. After successful transmission and reception of the frame, both the timers are reset. If the packet is not received after the transmission, then the second timer is triggered to check the reception within 10 ms. If the packet is not received, upon the timer expiry, a link down packet is sent to the switch.

If the neighbor acknowledges and is configured for REP Fast mode, convergence occurs within 50 ms. If a neighbor switch does not support RTOS, normal REP mode must be used for link up/down detection. In this case, you need to disable fastmode on both ends of the link.

Configuring REP Fast

Follow these steps to configure REP Fast:
Before you begin

Enable REP on the switch and configure the REP topology as described in Configuring Resilient Ethernet Protocol.

---

**Step 1**
Enter global configuration mode:

```
configure terminal
```  

**Step 2**
Specify the interface and enter interface configuration mode:

```
interface interface-id
```  

**Step 3**
Enable REP Fast:

```
rep fastmode
```  

**Step 4**
Return to privileged exec mode:

```
end
```  

---

**Example**

```
Switch# configure terminal
Switch(config)# int gi 1/4
Switch(config-if)# rep fastmode
Switch(config-if)# end
Switch# sh run int gi 1/4
interface GigabitEthernet1/4
switchport trunk allowed vlan 1-10
switchport mode trunk
rep segment 1 edge
rep fastmode
```  

---

### Displaying REP Fast Beacon Information

When REP Fast is enabled, the system sends beacon frames to the neighbor node for link status detection. Use the following command to display the number of beacon frames sent and received on an interface.

In privileged exec mode, enter:

```
show platform rep beacon interface interface-id
```  

---

**Example**

```
Switch# sh platform rep beacon GigabitEthernet 1/4
Beacon RX : 43984
Beacon TX : 46826
```
## Feature History

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Release</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>REP Fast</td>
<td>Cisco IOS XE 16.11.1</td>
<td>Initial support on Cisco Catalyst IE 3200, 3300, 3400, and Cisco Embedded Service 3300 Series Switches</td>
</tr>
</tbody>
</table>
Configuring QoS

This section includes information about these topics:

• Configuring QoS, on page 145

Configuring QoS

This document describes how to configure quality of service (QoS) by using the modular QoS command-line interface (CLI), or MQC, commands on the Cisco IE-3X00 and ESS3300 switch platforms. With QoS, you can provide preferential treatment to certain types of traffic at the expense of others. When QoS is not configured, the switch offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput. MQC provides a comprehensive hierarchical configuration framework for prioritizing or limiting specific streams of traffic.

This guide includes information about these topics:

Modular QoS CLI, on page 145
Input and Output Policies, on page 147
Classification, on page 148
Policing, on page 154
Marking, on page 156
Congestion Management and Scheduling, on page 157
Congestion Avoidance and Queuing, on page 160
Restrictions and Limitations, on page 193

Modular QoS CLI

Modular QoS CLI (MQC) allows users to create traffic policies and attach these policies to interfaces. A traffic policy contains a traffic class and one or more QoS features. You use a traffic class to classify traffic, and the QoS features in the traffic policy determine how to treat the classified traffic.

Modular QoS CLI configuration includes these steps:

Step 1. Define a traffic class.
Use the class-map [match-all | match-any] class-map-name global configuration command to define a traffic class and to enter class-map configuration mode. A traffic class contains three elements: a name, an instruction on how to evaluate the configured match commands (if more than one match command is configured in the class map), and a series of match commands.

- You name the traffic class in the class-map command line to enter class-map configuration mode.
- You can optionally include keywords to evaluate these match commands by entering class-map match-any or class-map match-all. If you specify match-any, the traffic being evaluated must match one of the specified criteria. If you specify match-all, the traffic being evaluated must match all of the specified criteria. A match-all class map can contain only one match statement, but a match-any class map can contain multiple match statements.

If you do not enter match-all or match-any, the default is to match all.

- You use the match class-map configuration commands to specify criteria for classifying packets. If a packet matches the specified criteria, that packet is considered a member of the class and is forwarded according to the QoS specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class.

**Step 2. Create a traffic policy to associate the traffic class with one or more QoS features.**

You use the policy-map policy-map-name global configuration command to create a traffic policy and to enter policy-map configuration mode. A traffic policy defines the QoS features to associate with the specified traffic class. A traffic policy contains three elements: a name, a traffic class (specified with the class policy-map configuration command), and the QoS policies configured in the class.

- You name the traffic policy in the policy-map command line to enter policy-map configuration mode.
- In policy-map configuration mode, enter the name of the traffic class used to classify traffic to the specified policy, and enter policy-map class configuration mode.
- In policy-map class configuration mode, you can enter the QoS features to apply to the classified traffic. These include using the set, police, or police aggregate commands for input policy maps or the bandwidth, priority, queue-limit or shape average commands for output policy maps.

**Note**

A packet can match only one traffic class within a traffic policy. If a packet matches more than one traffic class in the traffic policy, the first traffic class defined in the policy is used. To configure more than one match criterion for packets, you can associate multiple traffic classes with a single traffic policy.

**Step 3. Attach the traffic policy to an interface.**

You use the service-policy interface configuration command to attach the policy map to an interface for packets entering or leaving the interface. You must specify whether the traffic policy characteristics should be applied to incoming or outgoing packets. For example, entering the service-policy output class1 interface configuration command attaches all the characteristics of the traffic policy named class1 to the specified interface. All packets leaving the specified interface are evaluated according to the criteria specified in the traffic policy named class1.
If you enter the no policy-map configuration command or the no policy-map policy-map-name global configuration command to delete a policy map that is attached to an interface, a warning message appears that lists any interfaces from which the policy map is being detached. The policy map is then detached and deleted. For example:

Note

Warning: Detaching Policy test1 from Interface GigabitEthernet1/17

Input and Output Policies

Policy maps are either input policy maps or output policy maps, attached to packets as they enter or leave the switch by service policies applied to interfaces. Input policy maps perform policing and marking on received traffic. Policed packets can be dropped or reduced in priority (marked down) if they exceed the maximum permitted rates. Output policy maps perform scheduling and queuing on traffic as it leaves the switch.

Input policies and output policies have the same basic structure; the difference is in the characteristics that they regulate. You can configure a maximum of 200 policy maps.

Figure 18: Input and Output Policy Relationship

Input Policy Maps

Input policy map classification criteria include matching a CoS, vlan, DSCP, or matching an access control list (ACL). Input policy maps can have any of these actions:

- Setting or marking a CoS, or DSCP
- Policing

Only input policies provide matching on access groups and only output policies provide matching on QoS groups. You can assign a QoS group number in an input policy and match it in the output policy. The class class-default is used in a policy map for any traffic that does not explicitly match any other class in the policy map. Input policy maps do not support queuing and scheduling keywords, such as bandwidth, queue-limit, priority, and shape average.

An input policy map can have a maximum of 7 classes plus class-default. You can configure a maximum of 7 classes in an input policy.
Output Policy Maps

Output policy map classification criteria include matching a CoS, or DSCP. Output policy maps can have any of these actions:

- Queuing (queue-limit)
- Scheduling (bandwidth, priority, and shape average)

Output policy maps do not support matching of access groups.

Output policies do not support marking or policing (except in the case of priority with policing). There is no egress packet marking on the switch (no set command in an output policy).

The class class-default is used in a policy map for any traffic that does not explicitly match any other class in the policy map. There can be a maximum of eight classes in the output policy map (including class-default) because egress ports have a maximum of eight queues.

You can attach an output policy map to any or all ports on the switch. The switch supports configuration and attachment of a unique output policy map for each port. However, these output policy maps can contain only three unique configurations of queue limits. These three unique queue-limit configurations can be included in as many output policy maps as there are ports on the switch. There are no limitations on the configurations of bandwidth, priority, or shaping.

Classification

Classification distinguishes one kind of traffic from another by examining the fields in the packet header. When a packet is received, the switch examines the header and identifies all key packet fields. A packet can be classified based on an ACL, on the DSCP, CoS, or VLAN.

- On ports configured as Layer 2 IEEE 802.1Q trunks, all traffic is in 802.1Q frames except for traffic in the native VLAN. Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value, called the User Priority bits, in the three most-significant bits, and the VLAN ID value in the 12 least-significant bits. Other frame types cannot carry Layer 2 CoS values.

- Layer 2 CoS values range from 0 to 7.

- Both IPv4 and IPv6 packets can carry a DSCP value. QoS supports only the use of DSCP values.

- Use match on access-group for matching on dscp for ipv6 traffic. The access-group to be used is ipv6 acl.
Figure 19: QoS Classification Layers in Frames and Packets

Layer 2 IEEE 802.1Q and IEEE 802.1p Frame

<table>
<thead>
<tr>
<th>Preamble</th>
<th>Start frame delimiter</th>
<th>DA</th>
<th>SA</th>
<th>Type</th>
<th>TAG 2 Bytes</th>
<th>PT</th>
<th>Data</th>
<th>FCS</th>
</tr>
</thead>
</table>

3 bits used for CoS (IEEE 802.1p user priority)

PRI | CFI | VLAN ID

Layer 3 IPv4 Packet:

<table>
<thead>
<tr>
<th>Version length</th>
<th>ToS 1 Byte</th>
<th>Len</th>
<th>I D</th>
<th>Offset</th>
<th>TTL</th>
<th>Proto</th>
<th>FCS</th>
<th>IP-SA</th>
<th>IP-DA</th>
<th>Data</th>
</tr>
</thead>
</table>

These sections contain additional information about classification:

Class Maps, on page 149
The match Command, on page 150
Classification Based on Layer 2 CoS, on page 150
Classification Based on IP DSCP, on page 150
Classification Comparisons, on page 151
Classification Based on QoS ACLs, on page 152

Class Maps

As explained previously, you use an MQC class map to name a specific traffic flow (or class) and to isolate it from all other traffic. A class map defines the criteria used to match against a specific traffic flow to further classify it. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name. When you enter the class-map command with a class-map name, the switch enters the class-map configuration mode. In this mode, you define the match criterion for the traffic by using the match class-map configuration command. After a packet is matched against the class-map criteria, it is acted on by the associated action specified in a policy map.

You can match more than one criterion for classification. You criteria in the class map be in the packet header by using the command to enter class map configuration mode.

You can use the class map match-any class-map name global configuration command to define a classification with any of the listed criteria.
Note: If you do not enter match-all or match-any, the default is to match all. A match-all class map cannot have more than one classification criterion (match statement). A class map with no match condition has a default of match all.

The match Command

To configure the type of content used to classify packets, you use the match class-map configuration command to specify the classification criteria. If a packet matches the configured criteria, it belongs to a specific class and is forwarded according to the specified policy. For example, you can use the match class-map command with CoS, IP DSCP, and IP precedence values. These values are referred to as markings on a packet. You can also match an access group, or a QoS group.

- For an input policy map, you cannot configure an IP classification (match ip dscp, match access-group for an IP ACL) and a non-IP classification (match cos or match access-group for a MAC ACL) in the same policy map or class map.

- In an output policy map, no two class maps can have the same classification criteria, that is, the same match qualifiers and values.

This example shows how to create a class map example to define a class that matches any of the listed criteria. In this example, if a packet is received with the DSCP equal to 32 or 40, the packet is identified (classified) by the class map.

```
Switch(config)# class-map match-any example
Switch(config-cmap)# match ip dscp 32
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# exit
```

Classification Based on Layer 2 CoS

You can use the match command to classify Layer 2 traffic based on the CoS value, which ranges from 0 to 7.

Note: A match cos command is supported only on Layer 2 802.1Q trunk ports.

This example shows how to create a class map to match a CoS value of 5:

```
Switch(config)# class-map premium
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
```

Classification Based on IP DSCP

When you classify IPv4 traffic based on IP DSCP value, and enter the match ip dscp class-map configuration command, you have several classification options:

- Entering a specific DSCP value (0 to 63).

- Using the Default service, which corresponds to an IP precedence and DSCP value of 0. The default per-hop behavior (PHB) is usually best-effort service.

- Using Assured Forwarding (AF) by entering the binary representation of the DSCP value. AF sets the relative probability that a specific class of packets is forwarded when congestion occurs and the traffic does not exceed the maximum permitted rate. AF per-hop behavior provides delivery of IP packets in four different AF classes: AF11-13 (the highest), AF21-23, AF31-33, and AF41-43 (the lowest). Each AF class could be allocated a specific amount of buffer space and drop probabilities, specified by the
binary form of the DSCP number. When congestion occurs, the drop precedence of a packet determines the relative importance of the packet within the class. An AF41 provides the best probability of a packet being forwarded from one end of the network to the other.

- Entering Class Selector (CS) service values of 1 to 7, corresponding to IP precedence bits in the ToS field of the packet.

- Using Expedited Forwarding (EF) to specify a low-latency path. This corresponds to a DSCP value of 46. EF services use priority queuing to preempt lower priority traffic classes.

This display shows the available classification options:

```
Switch(config-cmap)# match ip dscp ?
<0-63> Differentiated services codepoint value
af11 Match packets with AF11 dscp (001010)
af12 Match packets with AF12 dscp (001100)
af13 Match packets with AF13 dscp (001110)
af21 Match packets with AF21 dscp (010010)
af22 Match packets with AF22 dscp (010100)
af23 Match packets with AF23 dscp (010110)
af31 Match packets with AF31 dscp (011010)
af32 Match packets with AF32 dscp (011100)
af33 Match packets with AF33 dscp (011110)
af41 Match packets with AF41 dscp (100010)
af42 Match packets with AF42 dscp (100100)
af43 Match packets with AF43 dscp (100110)
cs1 Match packets with CS1(precedence 1) dscp (001000)
cs2 Match packets with CS2(precedence 2) dscp (010000)
cs3 Match packets with CS3(precedence 3) dscp (011000)
cs4 Match packets with CS4(precedence 4) dscp (100000)
cs5 Match packets with CS5(precedence 5) dscp (101000)
cs6 Match packets with CS6(precedence 6) dscp (110000)
cs7 Match packets with CS7(precedence 7) dscp (111000)
default Match packets with default dscp (000000)
ef Match packets with EF dscp (101110)
```

For more information on DSCP prioritization, see RFC-2597 (AF per-hop behavior), RFC-2598 (EF), or RFC-2475 (DSCP).

### Classification Comparisons

**Table 12: Typical Traffic Classifications**, on page 151 shows suggested IP DSCP, IP precedence, and CoS values for typical traffic types.

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>DSCP per-hop</th>
<th>DSCP (decimal)</th>
<th>IP Precedence</th>
<th>CoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice-bearer - Traffic in a priority queue or the queue with the highest service weight and lowest drop priority.</td>
<td>EF</td>
<td>46</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Voice control - Signaling traffic, related to call setup, from a voice gateway or a voice application server.</td>
<td>AF31</td>
<td>26</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Video conferencing - in most networks, video conferencing over IP has similar loss, delay, and delay variation requirements as voice over IP traffic.</td>
<td>AF41</td>
<td>34</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>
### Traffic Type

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>DSCP per-hop</th>
<th>DSCP (decimal)</th>
<th>IP Precedence</th>
<th>QoS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Streaming video - relatively high bandwidth applications with a high tolerance for loss, delay, and delay variation. Usually considered more important than regular background applications such as e-mail and web browsing.</td>
<td>AF13</td>
<td>14</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Mission critical date (gold data) - delay-sensitive applications critical to the operation of an enterprise.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Level 1</td>
<td>AF21</td>
<td>18</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Level 2</td>
<td>AF22</td>
<td>20</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Level 3</td>
<td>AF23</td>
<td>22</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Less critical data (silver data) - noncritical, but relatively important data.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Level 1</td>
<td>AF11</td>
<td>10</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Level 2</td>
<td>AF12</td>
<td>12</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Level 3</td>
<td>AF13</td>
<td>14</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Best-effort data (bronze data) - other traffic, including all Default 0 0 0 non interactive traffic, regardless of importance.</td>
<td>Default</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Less than best-effort data—noncritical, bandwidth-intensive data traffic given the least preference. This is the first traffic type to be dropped.</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Level 1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Level 2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Level 3</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Classification Based on QoS ACLs

Packets can also be classified in input policy maps based on an ACL lookup. The ACL classification is communicated to an output policy by assigning a QoS group or number in the input policy map. To classify based on ACL lookup, you first create an IP or MAC ACL. Configure a class map and use the match access-group \{acl-number | acl name\} class-map configuration command, and attach the class map to a policy map.

**Note**

You cannot configure match access-group for an output policy map.

You can use IP standard, IP extended, or Layer 2 MAC ACLs to define a group of packets with the same characteristics (a class). You use the access-list global configuration command to configure IP ACLs to classify IP traffic based on Layer 3 and Layer 4 parameters. You use the mac access-list extended global
configuration command to configure Layer 2 MAC ACLs to classify IP and non-IP traffic based on Layer 2 parameters.

**Note**

You cannot match IP fragments against configured IP extended ACLs to enforce QoS. IP fragments are sent as best-effort. IP fragments are denoted by fields in the IP header.

You can use only ACLs with a permit action in a match access-group command. ACLs with a deny action are never matched in a QoS policy.

**Note**

Only one access-group is supported per class for an input policy map.

**Note**

A per-port, per-VLAN parent-level class map supports only a child-policy association; it does not allow any actions to be configured. In addition, for a parent-level class map, you cannot configure an action or a child-policy association for the class class-default.

Per-port, per-VLAN QoS has these limitations:

- You can configure classification based on VLAN ID only in the parent level of a per-port.

- When the child policy map attached to a VLAN or set of VLANs contains only Layer 3 classification (match ip dscp, match ip precedence, match IP ACL), you must be careful to ensure that these VLANs are not carried on any port other than the one on which this per-port, per-VLAN policy is attached. Not following this restriction could result in improper QoS behavior for traffic ingressing the switch on these VLANs.

- We also recommend that you restrict VLAN membership on the trunk ports to which the per-port, per-VLAN is applied by using the switchport trunk allowed vlan interface configuration command. Overlapping VLAN membership between trunk ports that have per-port, per-VLAN policies with Layer 3 classification could also result in unexpected QoS behavior.

In this example, the class maps in the child-level policy map specify matching criteria for voice, data, and video traffic, and the child policy map sets the action for input policing each type of traffic. The parent-level policy map specifies the VLANs to which the child policy maps are applied on the specified port.

```
Switch(config)# class-map match-any dscp-1 data
Switch(config-cmap)# match ip dscp 1
Switch(config-cmap)# exit
Switch(config)# class-map match-any dscp-23 video
Switch(config-cmap)# match ip dscp 23
Switch(config-cmap)# exit
Switch(config)# class-map match-any dscp-63 voice
Switch(config-cmap)# match ip dscp-63
Switch(config-cmap)# exit
Switch(config)# class-map match-any customer-1-vlan
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# match vlan 200
Switch(config-cmap)# match vlan 300
Switch(config-cmap)# exit
```
You can also enter the match criteria as match vlan 100 200 300 with the same result.

Switch(config)# policy-map child policy-1
Switch(config-pmap)# class dscp-63 voice
Switch(config-pmap-c)# police cir 10000000 bc 50000
Switch(config-pmap-c)# conform-action set-cos-transmit 5
Switch(config-pmap-c)# exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-1 data
Switch(config-pmap-c)# set cos 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class dscp-23 video
Switch(config-pmap-c)# set cos 4
Switch(config-pmap-c)# exit

Policing

After a packet is classified, you can use policing as shown in to regulate the class of traffic. The policing function limits the amount of bandwidth available to a specific traffic flow or prevents a traffic type from using excessive bandwidth and system resources. A policer identifies a packet as in or out of profile by comparing the rate of the inbound traffic to the configuration profile of the policer and traffic class. Packets that exceed the permitted average rate or burst rate are out of profile or nonconforming. These packets are dropped or modified (marked for further processing), depending on the policer configuration.

Policing is used primarily on receiving interfaces. You can attach a policy map with a policer only in an input service policy.

*Figure 20: Policing of Classified Packets*

The only policing allowed in an output policy map is in priority classes.

Individual Policing

Individual policing applies only to input policy maps. In policy-map configuration mode, you enter the class command followed by class-map name, and enter policy-map class configuration mode.

Cisco Industrial Ethernet Switches support 1-rate, 2-color ingress policing and 2-rate, 3-color policing for individual or aggregate policing.
For 1-rate, 2-color policing, you use the police policy-map class configuration command to define the policer, the committed rate limitations of the traffic, committed burst size limitations of the traffic, and the action to take for a class of traffic that is below the limits (conform-action) and above the limits (exceed-action). If you do not specify burst size (bc), the system calculates an appropriate burst size value. The calculated value is appropriate for most applications.

When you configure a 2-rate policer, in addition to configuring the committed information rate (CIR) for updating the first token bucket, you also configure the peak information rate (PIR) at which the second token bucket is updated. If you do not configure a PIR, the policer is a standard 1-rate, 2-color policer.

For 2-rate, 3-color policing, you can then optionally set actions to perform on packets that conform to the specified CIR and PIR (conform-action), packets that conform to the PIR, but not the CIR (exceed-action), and packets that exceed the PIR value (violate-action).

- If you set the CIR value equal to the PIR, a traffic rate that is less than or equal to the CIR is in the conform range. Traffic that exceeds the CIR is in the violate range.
- If you set the PIR greater than the CIR, a traffic rate less than the CIR is in the conform range. A traffic rate that exceeds the CIR but is less than or equal to the PIR is in the exceed range. A traffic rate that exceeds the PIR is in the violate range.
- If you do not configure a PIR, the policer is configured as a 1-rate, 2-color policer.

Setting the burst sizes too low can reduce throughput in situations with bursty traffic. Setting burst sizes too high can allow too high a traffic rate.

---

**Note**

The switch supports byte counters for byte-level statistics for conform, exceed, and violate classes in the show policy-map interface privileged EXEC command output.

To make the policy map effective, you attach it to a physical port by using the service-policy input interface configuration command. Policing is done only on received traffic, so you can only attach a policer to an input service policy.

You can use the conform-action and exceed-action policy-map class configuration commands or the conform-action and exceed-action policy-map class police configuration commands to specify the action to be taken when the packet conforms to or exceeds the specified traffic rate.

Conform actions are to send the packet without modifications, to set a new CoS, DSCP, or IP precedence value, or to set a QoS group value for classification at the egress. Exceed actions are to drop the packet, to send the packet without modification, to set a new CoS, DSCP, or IP precedence to a value, or to set a QoS group value for classification at the egress.

You can use the conform-action, exceed-action, and violate-action policy-map class configuration commands or the conform-action, exceed-action, and violate-action policy-map class police configuration commands to specify the action to be taken when the packet conforms to or exceeds the specified traffic rates. Conform, exceed, and violate actions are to drop the packet, to send the packet without modifications, to set a new CoS, DSCP, or IP precedence value, or to set a QoS group value for classification at the egress.

You can configure multiple conform and exceed actions simultaneously for each service class. You can configure multiple conform, exceed, and violate actions simultaneously for each service class. If you do not configure a violate-action, by default the violate class is assigned the same action as the exceed-action.

To configure multiple actions in a class, you can enter multiple conform or exceed action entries conform, exceed, or violate action entries in policy-map class police configuration mode, as in this example:
Marking

You can use packet marking in input policy maps to set or modify the attributes for traffic belonging to a specific class. After network traffic is organized into classes, you use marking to identify certain traffic types for unique handling. For example, you can change the CoS value in a class or set IP DSCP or IP precedence values for a specific type of traffic. These new values are then used to determine how the traffic should be treated. You can also use marking to assign traffic to a QoS group within the switch.

Traffic marking is typically performed on a specific traffic type at the ingress port. The marking action can cause the CoS, DSCP, or precedence bits to be rewritten or left unchanged, depending on the configuration. This can increase or decrease the priority of a packet in accordance with the policy used in the QoS domain so that other QoS functions can use the marking information to judge the relative and absolute importance of the packet. The marking function can use information from the policing function or directly from the classification function.

You can specify and mark traffic by using the set commands in a policy map for all supported QoS markings (CoS, IP DSCP, IP precedence, and QoS groups). A set command unconditionally marks the packets that match a specific class. You then attach the policy map to an interface as an input policy map.

You can simultaneously configure actions to modify DSCP, precedence, and COS markings in the packet for the same service along with QoS group marking actions. You can use the QoS group number defined in the marking action for egress classification.

The following figure shows the steps for marking traffic.

Figure 21: Marking of Classified Traffic

This example uses a policy map to remark a packet. The first marking (the set command) applies to the QoS default class map that matches all traffic not matched by class AF31-AF33 and sets all traffic to an IP DSCP value of 1. The second marking sets the traffic in classes AF31 to AF33 to an IP DSCP of 3.

Switch(config)# policy-map Example
Switch(config-pmap)# class class-default
Congestion Management and Scheduling

Cisco Modular QoS CLI (MQC) provides several related mechanisms to control outgoing traffic flow. They are implemented in output policy maps to control output traffic queues. The scheduling stage holds packets until the appropriate time to send them to one of the four traffic queues. Queuing assigns a packet to a particular queue based on the packet class, and is enhanced by the WTD algorithm for congestion avoidance. You can use different scheduling mechanisms to provide a guaranteed bandwidth to a particular class of traffic while also serving other traffic in a fair way. You can limit the maximum bandwidth that can be consumed by a particular class of traffic and ensure that delay-sensitive traffic in a low-latency queue is sent before traffic in other queues.

The switch supports these scheduling mechanisms:

Traffic shaping

You use the shape average policy map class configuration command to specify that a class of traffic should have a maximum permitted average rate. You specify the maximum rate in bits per second.

Class-based-weighted-fair-queuing (CBWFQ)

You can use the bandwidth policy-map class configuration command to control the bandwidth allocated to a specific class. Minimum bandwidth can be specified as a bit rate or a percentage of total bandwidth or of remaining bandwidth.

Priority queuing or class-based priority queuing

You use the priority policy-map class configuration command to specify the priority of a type of traffic over other types of traffic. You can specify strict priority for the high-priority traffic and allocate any excess bandwidth to other traffic queues, or specify priority with unconditional policing of high-priority traffic and allocate the known remaining bandwidth among the other traffic queues.

- To configure strict priority, use only the priority policy-map class configuration command to configure the priority queue. Use the bandwidth remaining percent policy-map class configuration command for the other traffic classes to allocate the excess bandwidth in the desired ratios.

- To configure priority with unconditional policing, configure the priority queue by using the priority policy-map class configuration command and the police policy-map class configuration command to unconditionally rate-limit the priority queue. In this case, you can configure the other traffic classes with bandwidth or shape average, depending on requirements.

Traffic Shaping

Traffic shaping is a traffic-control mechanism similar to traffic policing. While traffic policing is used in input policy maps, traffic shaping occurs as traffic leaves an interface. The switch can apply class-based shaping.
to classes of traffic leaving an interface and port shaping to all traffic leaving an interface. Configuring a queue for traffic shaping sets the maximum bandwidth or peak information rate (PIR) of the queue.

**Note**  
Shape and priority cannot be configured within the same class in an output policymap. However, shape and bandwidth can be configured together.

### Class-Based Shaping

Class-based shaping uses the shape average policy-map class configuration command to limit the rate of data transmission as the number of bits per second to be used for the committed information rate for a class of traffic. The switch supports separate queues for three classes of traffic. The fourth queue is always the default queue for class class-default, unclassified traffic.

```plaintext
Switch(config)# policy-map out-policy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

### Class-Based Weighted Fair Queuing

You can configure class-based weighted fair queuing (CBWFQ) to set the relative precedence of a queue by allocating a portion of the total bandwidth that is available for the port. You use the `bandwidth` policy-map class configuration command to set the output bandwidth for a class of traffic as a rate (kilobits per second), a percentage of total bandwidth, or a percentage of remaining bandwidth.

- When you use the bandwidth policy-map class configuration command to configure a class of traffic as an absolute rate (kilobits per second) or a percentage of total bandwidth, this represents the minimum bandwidth guarantee (CIR) for that traffic class. This means that the traffic class gets at least the bandwidth indicated by the command, but is not limited to that bandwidth. Any excess bandwidth on the port is allocated to each class in the same ratio in which the CIR rates are configured.

  You cannot configure bandwidth as an absolute rate or a percentage of total bandwidth when strict priority (priority without police) is configured for another class in the output policy.

- When you use the bandwidth policy-map class configuration command to configure a class of traffic as a percentage of remaining bandwidth, this represents the portion of the excess bandwidth of the port that is allocated to the class. This means that the class is allocated bandwidth only if there is excess bandwidth on the port, and if there is no minimum bandwidth guarantee for this traffic class.

  You can configure bandwidth as percentage of remaining bandwidth only when strict priority (priority without police) is configured for another class in the output policy map.

**Note**  
You cannot configure bandwidth and traffic shaping (shape average) or priority queuing (priority) for the same class in an output policy map.
When you configure CIR bandwidth for a class as an absolute rate or percentage of the total bandwidth, any excess bandwidth remaining after servicing the CIR of all the classes in the policy map is divided among the classes in the same proportion as the CIR rates. If the CIR rate of a class is configured as 0, that class is also not eligible for any excess bandwidth and as a result receives no bandwidth.

Note

You can use the priority policy-map class configuration command to ensure that a particular class of traffic is given preferential treatment. With strict priority queuing, the priority queue is constantly serviced. All packets in the queue are scheduled and sent until the queue is empty. Priority queuing allows traffic for the associated class to be sent before packets in other queues are sent.

Note

You should exercise care when using the priority command. Excessive use of strict priority queuing might cause congestion in other queues.

Priority Queuing

You can use the priority policy-map class configuration command to ensure that a particular class of traffic is given preferential treatment. With strict priority queuing, the priority queue is constantly serviced. All packets in the queue are scheduled and sent until the queue is empty. Priority queuing allows traffic for the associated class to be sent before packets in other queues.

The switch supports strict priority queuing or priority used with the police policy-map command.

• Strict priority queuing (priority without police) assigns a traffic class to a low-latency queue to ensure that packets in this class have the lowest possible latency. When this is configured, the priority queue is continually serviced until it is empty, possibly at the expense of packets in other queues.

• You can use priority with the police policy-map command, or unconditional priority policing, to reduce the bandwidth used by the priority queue. This is the only form of policing that is supported in output policy maps. Using this combination of commands configures a maximum rate on the priority queue, and you can use the bandwidth and shape average policy-map commands for other classes to allocate traffic rates on other queues.

When priority is configured in an output policy map without the police command, you can only configure the other queues for sharing by using the bandwidth remaining percent policy-map command to allocate excess bandwidth.

Priority queuing has these restrictions:

• You can associate the priority command with a single unique class for all attached output polices on the switch.

• You cannot configure priority and any other scheduling action (shape average or bandwidth) in the same class.

• You cannot configure priority queuing for the class-default of an output policy map.

This example shows how to configure the class out-class1 as a strict priority queue so that all packets in that class are sent before any other class of traffic. Other traffic queues are configured so that out-class-2 gets 50 percent of the remaining bandwidth and out-class3 gets 20 percent of the remaining bandwidth. The class class-default receives the remaining 30 percent with no guarantees.

Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit

Congestion Avoidance and Queuing

Congestion avoidance uses algorithms such as tail drop to control the number of packets entering the queuing and scheduling stage to avoid congestion and network bottlenecks. The switch uses weighted tail drop (WTD) to manage the queue sizes and provide a drop precedence for traffic classifications. You set the queue size limits depending on the markings of the packets in the queue. Each packet that travels through the switch can be assigned to a specific queue and threshold. For example, specific DSCP or CoS values can be mapped to a specific egress queue and threshold.

WTD is implemented on traffic queues to manage the queue size and to provide drop precedence for different traffic classifications. As a frame enters a particular queue, WTD uses the packet classification to subject it to different thresholds. If the total destination queue size is greater than the threshold of any reclassified traffic, the next frame of that traffic is dropped.

The following figure shows an example of WTD operating on a queue of 1000 frames. Three drop percentages are configured: 40 percent (400 frames), 60 percent (600 frames), and 100 percent (1000 frames). These percentages mean that traffic reclassified to the 40-percent threshold is dropped when the queue depth exceeds 400 frames, traffic reclassified to 60 percent is dropped when the queue depth exceeds 600 frames, and traffic up to 400 frames can be queued at the 40-percent threshold, up to 600 frames at the 60-percent threshold, and up to 1000 frames at the 100-percent threshold.

Figure 22: Queue Operation

In this example, CoS values 6 and 7 have a greater importance than the other CoS values, and they are assigned to the 100-percent drop threshold (queue-full state). CoS values 4 and 5 are assigned to the 60-percent threshold, and CoS values 0 to 3 are assigned to the 40-percent threshold.
If the queue is already filled with 600 frames, and a new frame arrives containing CoS values 4 and 5, the frame is subjected to the 60-percent threshold. When this frame is added to the queue, the threshold would be exceeded, so the switch drops it.

WTD is configured by using the queue-limit policy-map class command. The command adjusts the queue size (buffer size) associated with a particular class of traffic. You specify the threshold as the number of packets, where each packet is a fixed unit of 256 bytes. You can specify different queue sizes for different classes of traffic (CoS, DSCP, precedence, or QoS group) in the same queue. Setting a queue limit establishes a drop threshold for the associated traffic when congestion occurs.

You cannot configure queue size by using the queue-limit policy map class command without first configuring a scheduling action (bandwidth, shape average, or priority). The only exception to this is when you configure queue-limit for the class-default of an output policy map.

The switch supports up to three unique queue-limit configurations across all output policy maps. Within an output policy map, only four queues (classes) are allowed, including the class default. Each queue has two thresholds defined. Only two unique threshold value configurations are allowed on the switch. However, multiple policy maps can share the same queue-limits. When two policy maps share a queue-limit configuration, all threshold values must be the same for all the classes in both policy maps.

This example configures class A to match DSCP values and a policy map, PM1. The DSCP values of 30 and 50 are mapped to unique thresholds (32 and 64, respectively). The DSCP values of 40 and 60 are mapped to the maximum threshold of 112 packets.

```
Switch(config)# class-map match-any classA
Switch(config-cmap)# match ip dscp 30 40 50 60
Switch(config-cmap)# exit
Switch(config)# policy-map PM1
Switch(config-pmap)# class classA
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 112
Switch(config-pmap-c)# queue-limit dscp 30 32
Switch(config-pmap-c)# queue-limit dscp 50 64
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output PM1
Switch(config-if)# exit
```

You can use these same queue-limit values in multiple output policy maps on the switch. However, changing one of the queue-limit values in a class creates a new, unique queue-limit configuration. You can attach only three unique queue-limit configurations in output policy maps to interfaces at any one time. If you attempt to attach an output policy map with a fourth unique queue-limit configuration, you see this error message:

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit configurations exceeded.
```
When you configure a queue limit for a class in an output policy map, all other output policy maps must use the same qualifier type and qualifier value format. Only the queue-limit threshold values can be different. For example, when you configure class A queue limit thresholds for dscp 30 and dscp 50 in policy map PM1, and you configure class A queue limits in policy map PM2, you must use dscp 30 and dscp 50 as qualifiers. You cannot use dscp 20 and dscp 40. The threshold values can be different, but different threshold values creates a new queue-limit configuration.

By default, the total amount of buffer space is divided equally among all ports and all queues per port, which is adequate for many applications. You can decrease the queue size for latency-sensitive traffic or increase the queue size for bursty traffic.

When you use the queue-limit command to configure queue thresholds for a class, the WTD thresholds must be less than or equal to the queue maximum threshold. A queue size configured with no qualifier must be larger than any queue sizes configured with qualifiers.

Per cos/dscp thresholds for queue-limit is not supported with the current release.

When you configure queue limit, the range for the number of packets is from 16 to 544, in multiples of 16, where each packet is a fixed unit of 256 bytes.

For optimal performance, we strongly recommend that you configure the queue-limit to 272 or less.

Queue bandwidth and queue size (queue limit) are configured separately and are not interdependent. You should consider the type of traffic being sent when you configure bandwidth and queue-limit:

- A large buffer (queue limit) can better accommodate bursty traffic without packet loss, but at the cost of increased latency.
- A small buffer reduces latency but is more appropriate for steady traffic flows than for bursty traffic.
- Very small buffers are typically used to optimize priority queuing. For traffic that is priority queued, the buffer size usually needs to accommodate only a few packets; large buffer sizes that increase latency are not usually necessary. For high-priority latency-sensitive packets, configure a relatively large bandwidth and relatively small queue size.

These restrictions apply to WTD qualifiers:

- You cannot configure more than two threshold values for WTD qualifiers (cos, dscp, precedence, qos-group) by using the queue-limit command. However, there is no limit to the number of qualifiers that you can map to these thresholds. You can configure a third threshold value to set the maximum queue by using the queue-limit command with no qualifiers.
- A WTD qualifier in the queue-limit command must be the same as at least one match qualifier in the associated class map.
This example shows how to configure bandwidth and queue limit so that out-class1, out-class2, out-class3, and class-default get a minimum of 40, 20, 10 and 10 percent of the traffic bandwidth, respectively. The corresponding queue-sizes are set to 48, 32, 16 and 272 (256-byte) packets:

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# queue-limit 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 16
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 272
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-if)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

You can configure and attach as many output policy maps as there are switch ports, but only two unique queue-limit configurations are allowed. When another output policy map uses the same queue-limit and class configurations, even if the bandwidth percentages are different, it is considered to be the same queue-limit configuration.

## Configuring QoS

Before configuring QoS, you must have a thorough understanding of these factors:

- The types of applications used and the traffic patterns on your network.
- Traffic characteristics and needs of your network. Is the traffic bursty? Do you need to reserve bandwidth for voice and video streams?
- Bandwidth requirements and speed of the network.
- Location of congestion points in the network.

These sections describe how to classify, police, and mark incoming traffic, and schedule and queue outgoing traffic.

Depending on your network configuration, you must perform one or more of these tasks:

- Default QoS Configuration, on page 164
- QoS Configuration Guidelines, on page 164
- Using ACLs to Classify Traffic, on page 164
- Creating IP Extended ACLs, on page 166
- Creating Layer 2 MAC ACLs, on page 168
Default QoS Configuration

There are no policy maps, class maps, or policers configured. At the egress port, all traffic goes through a single default queue that is given the full operational port bandwidth. The default size of the default queue is 1000 packets (256 bytes).

The packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode without any rewrites and classified as best effort without any policing.

QoS Configuration Guidelines

- You can configure QoS only on physical ports.
- On a port configured for QoS, all traffic received through the port is classified, policed, and marked according to the input policy map attached to the port. On a trunk port configured for QoS, traffic in all VLANs received through the port is classified, policed, and marked according to the policy map attached to the port.
- QoS is not supported on logical ports (EtherChannel)
- Control traffic (such as spanning-tree bridge protocol data units [BPDUs] and routing update packets) received by the switch are subject to all ingress QoS processing.
- You are likely to lose data when you change queue settings; therefore, try to make changes when traffic is at a minimum.
- When you try to attach a new policy to an interface this brings the number of policer instances to more than 1024 minus 1 more than the number of interfaces on the switch 255, you receive an error message, and the configuration fails.

Using ACLs to Classify Traffic

You can classify IP traffic by using IP standard or IP extended ACLs. You can classify IP and non-IP traffic by using Layer 2 MAC ACLs.
Follow these guidelines when configuring QoS ACLs:

- You cannot match IP fragments against configured IP extended ACLs to enforce QoS. IP fragments are sent as best-effort. IP fragments are denoted by fields in the IP header.
- The switch supports only one access group per class in an input policy map.
- You cannot configure match-access group in an output policy map.

Creating IP Standard ACLs

Beginning in privileged EXEC mode, follow these steps to create an IP standard ACL for IP traffic:

**Note**
Choose from Step 2 OR Step 3 below.

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
</tr>
</tbody>
</table>
### What to do next

To delete an access list, use the no access-list access-list-number global configuration command.

This example shows how to allow access for only those hosts on the three specified networks. The wild card bits apply to the host portions of the network addresses.

```bash
Switch(config)# access-list 1 permit 192.5.255.0 0.0.0.255
Switch(config)# access-list 1 permit 128.88.0.0 0.0.255.255
Switch(config)# access-list 1 permit 36.0.0.0 0.0.0.255
```

### Creating IP Extended ACLs

Beginning in privileged EXEC mode, follow these steps to create an IP extended ACL for IP traffic:

<table>
<thead>
<tr>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong> access-list access-list-number permit protocol [source source-wildcard destination destination-wildcard] precedence precedence tos tos dscp dscp</td>
</tr>
</tbody>
</table>

Create an IP extended ACL. Repeat the step as many times as necessary.

#### Note

- For `access-list-number`, enter the access list number. The range is 100 to 199 and 2000 to 2699.
- Always use the `permit` keyword for ACLs used as match criteria in QoS policies. QoS policies do not match `deny` ACLs.
- For `source`, enter the network or host from which the packet is being sent. You can use the any keyword as an abbreviation for 0.0.0.0-255.255.255.255.
- For `protocol`, enter the name or number of an IP protocol. Use the value with no dscp. question mark (?) to see a list of available protocols. To match any Internet protocol (including ICMP, TCP, and UDP), enter `ip`.
- The `source` is the number of the network or host sending the packet.
- The `source-wildcard` applies wildcard bits to the source.
- The `destination` is the network or host number receiving the packet.
- The `destination-wildcard` applies wildcard bits to the destination.
You can specify source, destination, and wildcards as:

- The 32-bit quantity in dotted-decimal format.
- The keyword any for 0.0.0.0 255.255.255.255 (any host).
- The keyword host for a single host 0.0.0.0.

Other keywords are optional and have these meanings:

- precedence—Enter to match packets with a precedence level specified as a number from 0 to 7 or by name: routine (0), priority (1), immediate (2), flash (3), flash-override (4), critical (5), internet (6), network (7).
- tos—Enter to match by type of service level, specified by a number from 0 to 15 or a name: normal (0), max-reliability (2), max-throughput (4), min-delay (8).
- dscp—Enter to match packets with the DSCP value specified by a number from 0 to 63, or use the question mark (?) to see a list of available values.

### Step 3

**ip access-list extended name**

Define an extended IPv4 access list using a name, and enter access-list configuration mode. The name can be a number from 100 to 199.

In access-list configuration mode, enter permit protocol [source-wildcard destination destination-wildcard] precedence precedence tos tos dscp dscp as defined in the previous step.

### Step 4

**end**

Return to privileged EXEC mode.

### Step 5

**show access-lists**

Verify your entries.

### Step 6

**copy running-config startup-config**

(Optional) Save your entries in the configuration file.

### What to do next

To delete an access list, use the no access-list access-list-number global configuration command.

This example shows how to create an ACL that permits IP traffic from any source to any destination that has the DSCP value set to 32:

Switch(config)# access-list 100 permit ip any any dscp 32

This example shows how to create an ACL that permits IP traffic from a source host at 10.1.1.1 to a destination host at 10.1.1.2 with a precedence value of 5:

Switch(config)# access-list 100 permit ip host 10.1.1.1 host 10.1.1.2 precedence 5
## Creating Layer 2 MAC ACLs

Beginning in privileged EXEC mode, follow these steps to create a Layer 2 MAC ACL for non-IP traffic:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>mac access-list extended name</td>
<td>Create a Layer 2 MAC ACL by specifying the name of the list and enter extended MAC ACL configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>permit /host src-MAC-addr mask</td>
<td>Always use the permit keyword for ACLs used as match criteria in QoS policies. &lt;br&gt; - For src-MAC-addr, enter the MAC address of the host from which the packet is being sent. You can specify in hexadecimal format (H.H.H), use the any keyword for source 0.0.0, source-wildcard ffff.fff.fff, or use the host keyword for source 0.0.0. &lt;br&gt; - For mask, enter the wildcard bits by placing ones in the bit positions that you want to ignore. &lt;br&gt; - For dst-MAC-addr, enter the MAC address of the host to which the packet is being sent. You can specify in hexadecimal format (H.H.H), use the any keyword for source 0.0.0, source-wildcard ffff.fff.fff, or use the host keyword for source 0.0.0. &lt;br&gt; - (Optional) For type mask, specify the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. For type, the range is from 0 to 65535, typically specified in hexadecimal. For mask, enter the don’t care bits applied to the Ethertype before testing for a match.</td>
</tr>
<tr>
<td>4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>5</td>
<td>show access-lists [access-list-number</td>
<td>access-list-name]</td>
</tr>
<tr>
<td>6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

### What to do next

To delete an access list, use the no mac access-list extended access-list-name global configuration command.

This example shows how to create a Layer 2 MAC ACL with two permit statements. The first statement allows traffic from the host with MAC address 0001.0000.0001 to the host with MAC address 0002.0000.0001. The second statement allows only Ethertype XNS-IDP traffic from the host with MAC address 0001.0000.0002 to the host with MAC address 0002.0000.0002.

```
Switch(config)# mac access-list extended maclist1
```
Switch(config-ext-macl)# permit 0001.0000.0001 0.0.0 0002.0000.0001 0.0.0
Switch(config-ext-macl)# permit 0001.0000.0002 0.0.0 0002.0000.0002 0.0.0
Switch(config-ext-macl)# exit

Using Class Maps to Define a Traffic Class

You use the class-map global configuration command to name and to isolate a specific traffic flow (or class) from all other traffic. A class map defines the criteria to use to match against a specific traffic flow to further classify it. Match statements can include criteria such as an ACL, CoS value, DSCP value, IP precedence values. You define match criterion with one or more match statements entered in the class-map configuration mode.

Follow these guidelines when configuring class maps:

- A match-all class map cannot have more than one classification criterion (one match statement), but a match-any class map can contain multiple match statements.

- The match cos command is supported only on Layer 2 802.1Q trunk ports.

- For an input policy map, you cannot configure an IP classification (match ip dscp, match ip precedence, match access-group for an IP ACL) and a non-IP classification (match cos or match access-group for a MAC ACL) in the same policy map or class map. For a per-port, per-VLAN hierarchical policy map, this applies to the child policy map.

- You cannot configure match qos-group for an input policy map.

- In an output policy map, no two class maps can have the same classification criteria; that is, the same match qualifiers and values.

- The maximum number of class maps on the switch is 1024.

Beginning in privileged EXEC mode, follow these steps to create a Layer 2 MAC ACL for non-IP traffic:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> class-map [match-all</td>
<td>match-any] class-map-name</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Use the match-all keyword to perform a logical-AND of all matching statements under this class map. All match criteria in the class map must be matched.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Use the match-any keyword to perform a logical-OR of all matching statements under this class map. One or more match criteria must be matched.</td>
</tr>
<tr>
<td></td>
<td>• For class-map-name, specify the name of the class map.</td>
</tr>
<tr>
<td></td>
<td>If no matching statements are specified, the default is match-all.</td>
</tr>
</tbody>
</table>
### Command or Action

| Step 3 | match \{access-group acl-index-or-name | cos cos-list | ip dscp dscp-list | ip precedence ip-precedence-list | qos-group value | vlan vlan-list\} |

### Purpose

**Note**

A match-all class map cannot have more than one classification criterion (match statement).

Define the match criterion to classify traffic. By default, no match criterion is defined.

Only one match type per class map is supported, and only one ACL per class map is supported.

- For **access-group acl-index-or-name**, specify the number or name of an ACL. Matching access groups is supported only in input policy maps.
- For **cos cos-list**, enter a list of up to four CoS values in a single line to match against incoming packets. Separate each value with a space. You can enter multiple cos-list lines to match more than four CoS values. The range is 0 to 7.
- For **ip dscp dscp-list**, enter a list of up to eight IPv4 DSCP values to match against incoming packets. Separate each value with a space. You can enter multiple dscp-list lines to match more than eight DSCP values. The numerical range is 0 to 63. You can also configure DSCP values in other forms.
- For **ip precedence ip-precedence-list**, enter a list of up to four IPv4 precedence values to match against incoming packets. Separate each value with a space. You can enter multiple ip-precedence-list lines to match more than four precedence values. The range is 0 to 7.
- For **qos-group value**, specify the QoS group number. The range is 0 to 99. Matching of QoS groups is supported only in output policy maps.

### What to do next

Use the **no** form of the appropriate command to delete an existing class map or remove a match criterion.

This example shows how to create access list 103 and configure the class map called class1. The class1 has one match criterion, which is access list 103. It permits traffic from any host to any destination that matches a DSCP value of 10.

```bash
Switch(config)# access-list 103 permit any any dscp 10
```
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit

This example shows how to create a class map called class2, which matches incoming traffic with DSCP values of 10, 11, and 12.

Switch(config)# class-map match-any class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit

This example shows how to create a class map called class3, which matches incoming traffic with IP-precedence values of 5, 6, and 7:

Switch(config)# class-map match-any class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit

Attaching a Traffic Policy to an Interface

You use the service-policy interface configuration command to attach a traffic policy to an interface and to specify the direction in which the policy should be applied: either an input policy map for incoming traffic or an output policy map for outgoing traffic. Input and output policy maps support different QoS features.

You can attach a service policy only to a physical port. You can attach only one input policy map and one output policy map per port.

Note
If you enter the no policy-map configuration command or the no policy-map policy-map-name global configuration command to delete a policy map that is attached to an interface, a warning message appears that lists any interfaces from which the policy map is being detached. The policy map is then detached and deleted.

For example:

Warning: Detaching Policy test1 from Interface GigabitEthernet1/17

Beginning in privileged EXEC mode, follow these steps to attach a policy map to a port:

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface interface-id</td>
<td>Specify the port to attach to the policy map, and enter interface configuration mode. Valid interfaces are physical ports.</td>
</tr>
<tr>
<td>Step 3 service-policy [input</td>
<td>output] policy-map-name</td>
</tr>
<tr>
<td>Step 4 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5 show policy-map interface [interface-id]</td>
<td>Verify your entries.</td>
</tr>
</tbody>
</table>
Configuring Input Policy Maps

Policy maps specify which traffic class to act on and what actions to take. All traffic that fails to meet matching criteria of a traffic class belongs to the default class. Input policy maps regulate traffic entering the switch. In an input policy, you can match CoS, DSCP, or ACLs, and configure individual policing, aggregate policing, or marking to a CoS, DSCP, IP precedence, or QoS group value.

Follow these guidelines when configuring input policy maps:

- You can attach only one input policy map per port.
- The maximum number of policy maps configured on the switch is 193.
- The total number of configurable policer profiles on the switch is 193
- The maximum number of classes in each input policy map is 7 plus class-default.
- The number of input policy maps that can be attached in a switch is limited by the availability of hardware resources. If you attempt to attach an input policy map that causes any hardware resource limitation to be exceeded, the configuration fails.
- After you have attached a single-level policy map to an interface by using the service-policy input interface configuration command, you can modify the policy without detaching it from the interface. You can add or delete classification criteria, add or delete classes, add or delete actions, or change the parameters of the configured actions (policers, rates, mapping, marking, and so on).
- When an input policy map with only Layer 2 classification is attached to a routed port or a switch port containing a routed SVI, the service policy acts only on switching eligible traffic and not on routing eligible traffic.
- On an 802.1Q tunnel port, you can use only an input policy map with Layer 2 classification based on MAC ACLs to classify traffic. Input policy maps with Layer 3 classification or with Layer 2 classification based on CoS or VLAN ID are not supported on tunnel ports.
- Input policy maps support policing and marking, not scheduling or queuing. You cannot configure bandwidth, priority, queue-limit, or shape average in input policy maps.

These sections describe how to configure different types of input policy maps:

Configuring Input Policy Maps with Individual Policing

You use the police policy-map class configuration command to configure individual policers to define the committed rate limitations, committed burst size limitations of the traffic, and the action to take for a class of traffic.

Follow these guidelines when configuring individual policers:
Policing is supported only on input policy maps.

The switch supports a maximum of 200 policers.

2-rate, 3-color policing is supported only on input policy maps; 1-rate, 3-color policing is supported on both input and output policy maps.

The number of policer instances on the switch can be 1024 minus 1 more than the number interfaces. The switch supports a maximum of 200 policer profiles.

If you do not configure a violate-action, by default the violate class is assigned the same action as the exceed-action.

Follow these guidelines when configuring class maps:

- A match-all class map cannot have more than one classification criterion (one match statement), but a match-any class map can contain multiple match statements.

- The match cos command is supported only on Layer 2 802.1Q trunk ports.

- For an input policy map, you cannot configure an IP classification (match ip dscp, match ip precedence, match access-group for an IP ACL) and a non-IP classification (match cos or match access-group for a MAC ACL) in the same policy map or class map. For a per-port, per-VLAN hierarchical policy map, this applies to the child policy map.

- You cannot configure match qos-group for an input policy map.

- In an output policy map, no two class maps can have the same classification criteria; that is, the same match qualifiers and values.

- The maximum number of class maps on the switch is 1024.

In the procedure below, perform Step 5, 6, OR 7. Also, perform Step 8, OR Step 9.

Beginning in privileged EXEC mode, follow these steps to create an input policy map with individual policing:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> policy-map policy-map-name</td>
<td>Create a policy map by entering the policy map name, and enter policy-map configuration mode. By default, no class maps are defined.</td>
</tr>
<tr>
<td><strong>Step 3</strong> class {class-map-name</td>
<td>class-default}</td>
</tr>
</tbody>
</table>

**Note**
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 4    | `police {rate-bps | cir cir-bps} [burst-bytes | bc burst-bytes]` | Define a policer for the class of traffic.  
  - For `rate-bps`, specify average traffic rate in bits per second (bps). The range is 64000 to 1000000000.  
  - For `cir cir-bps`, specify a committed information rate (CIR) in bits per second (bps). The range is 64000 to 1000000000.  
  - For `burst-bytes` (optional), specify the normal burst size in bytes. The range is 64000 to 1000000000.  
  - For `bc burst-bytes` (optional), specify the conformed burst (bc) or the number of acceptable burst bytes. The range is 64000 to 1000000000. |
| 5    | `conform-action cos {cos_value | cos [table ] | dscp [table ] | precedence [table ]}` | (Optional) Enter the action to be taken on packets that conform to the CIR.  
  - For `cos cos_value`, enter a new CoS value to be assigned to the classified traffic. The range is 0 to 7. |
| 6    | `conform-action [ip] dscp {dscp_value | cos [table ] | dscp [table ] | precedence [table ]}` | (Optional) Enter the action to be taken on packets that conform to the CIR.  
  - For `[ip] dscp dscp_value`, enter a new DSACP value to be assigned to the classified traffic. The range is 0 to 63. |
| 7    | `conform-action [ip] precedence {precedence_value | cos [dscp table]}` | (Optional) Enter the action to be taken on packets that conform to the CIR.  
  - For `[ip] precedence precedence_value`, enter a new IP-precedence value to be assigned to the classified traffic. The range is 0 to 7.  
  **Note** You can enter a single conform-action as part of the command string following the police command. You can also press Enter after the police command to enter policy-map class police configuration mode, where you can enter multiple actions. In policy-map class police configuration mode, you must enter an action to take. |
| 8    | `exceed-action cos {cos_value | cos [table ] | dscp [table ] | precedence [table ]}` | (Optional) Enter the action to be taken on packets that conform to the CIR.  
  - For `cos cos_value`, enter a new CoS value to be assigned to the classified traffic. The range is 0 to 7. |
### Command or Action

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>(Optional) Enter the action to be taken on packets that conform to the CIR.</td>
</tr>
<tr>
<td></td>
<td>• For [ip] dscp dscp_value, enter a new DSACP value to be assigned to the classified traffic. The range is 0 to 63.</td>
</tr>
<tr>
<td>Note</td>
<td>You can enter a single exceed-action as part of the command string following the police command. Or you can press Enter after the police command to enter policy-map class police configuration mode, where you can enter multiple actions. In policy-map class police configuration mode, you must enter an action to take.</td>
</tr>
<tr>
<td>Note</td>
<td>If you explicitly configure exceed-action drop as keywords in the command, you must enter policy-map class police configuration mode and enter the no exceed-action drop command to remove the previously configured exceed action before you can enter the new exceed-action.</td>
</tr>
</tbody>
</table>

| Step 10 | exit | Return to policy-map configuration mode. |
| Step 11 | exit | Return to global configuration mode. |
| Step 12 | interface interface-id | Enter interface configuration mode for the interface to which you want to attach the policy. |
| Step 13 | service-policy input policy-map-name | Attach the policy map (created in Step 2) to the ingress interface. |
| Step 14 | end | Exit privileged EXEC mode. |
| Step 15 | show policy-map [policy-map-name [class class-map-name]] | Verify your entries. |
| Step 16 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

### What to do next

If you enter the no policy-map configuration command or the no policy-map policy-map-name global configuration command to delete a policy map that is attached to an interface, a warning message appears that lists any interfaces from which the policy map is being detached. The policy map is then detached and deleted. For example:

```
Warning: Detaching Policy test1 from Interface GigabitEthernet1/17
```
### Configuring Input Policy Maps with Individual 2-rate, 3-color Policing

Beginning in privileged EXEC mode, follow these steps to create an input policy map with individual 2-rate, 3-color policing:

**Note** In the procedure below, perform Step 5, 6, OR 7.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>policy-map policy-map-name</code></td>
<td>Create a policy map by entering the policy map name, and enter policy-map configuration mode. By default, no class maps are defined.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>`class {class-map-name</td>
<td>class-default}`</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>`policer {rate-bps</td>
<td>cir {cir-bps} [burst-bytes] [bc [conform-burst]] [pir pir-bps [be peak-burst]]`</td>
</tr>
</tbody>
</table>

- For `rate-bps`, specify average traffic rate in bits per second (bps). The range is 8000 to 1000000000.
- For `cir cir-bps`, specify a committed information rate at which the bc token bucket is updated in bits per second (b/s). The range is 8000 to 1000000000.
- For `burst-bytes` (optional), specify the normal burst size in bytes. The range is 8000 to 1000000000.
- For `bc burst-bytes` (optional), specify the conformed burst (bc) or the number of acceptable burst bytes. The range is 64000 to 1000000000.
- (Optional) For bc `conform-burst`, specify the conformed burst used by the bc token bucket for policing. The range is 8000 to 100000000 bytes.
- (Optional) For pir `pir-bps`, specify the peak information rate at which the be token bucket for policing is updated. The range is 8000 to 100000000 b/s. If you do not enter a pir `pir-bps`, the policer is configured as a 1-rate, 2-color policer.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• For be <strong>peak-burst</strong>, specify the peak burst size used by the be token bucket. The range is 8000 to 1000000 bytes. The default is internally calculated based on the user configuration.</td>
<td></td>
</tr>
</tbody>
</table>

### Step 5

conf-form-action \[drop | set-cos-transmit \{cos_value | cos | dscp | precedence\} \{table \}] | set-dscp-transmit \{dscp_value | cos | dscp | precedence\} \{table \}] | set-prec-transmit \{precedence_value | cos | dscp | precedence\} \{table \}] | set-qos-transmit qos-group_value | transmit\]

(Optional) Enter the action to be taken on packets, depending on whether or not they conform to the CIR and PIR.

(Optional) For conform-action, specify the action to perform on packets that conform to the CIR and PIR. The default is transmit.

### Step 6

exceed-action \[drop | set-cos-transmit \{cos_value | cos | dscp | precedence\} \{table \}] | set-dscp-transmit \{dscp_value | cos | dscp | precedence\} \{table \}] | set-prec-transmit \{precedence_value | cos | dscp | precedence\} \{table \}] | set-qos-transmit qos-group_value | transmit\]

(Optional) Enter the action to be taken on packets, depending on whether or not they conform to the CIR and PIR.

(Optional) For exceed-action, specify the action to perform on packets that conform to the PIR, but not the CIR. The default is drop.

### Step 7

violate-action \[drop | set-cos-transmit \{cos_value | cos | dscp | precedence\} \{table \}] | set-dscp-transmit \{dscp_value | cos | dscp | precedence\} \{table \}] | set-prec-transmit \{precedence_value | cos | dscp | precedence\} \{table \}] | set-qos-transmit qos-group_value | transmit\]

(Optional) Enter the action to be taken on packets, depending on whether or not they conform to the CIR and PIR.

(Optional) For violate-action, specify the action to perform on packets that exceed the PIR. The default is drop.

**Note**

If the conform action is set to drop, the exceed and violate actions are automatically set to drop.

If the exceed action is set to drop, the violate action is automatically set to drop.

- **set-cos-transmit cos-value**—Enter a new CoS value to be assigned to the packet, and send the packet. The range is from 0 to 7.

- **set-dscp-transmit dscp-value**—Enter a new IP DSCP value to be assigned to the packet, and send the packet. The range is from 0 to 63. You can also enter a mnemonic name for a commonly used value.

- **set-prec-transmit cos-value**—Enter a new IP precedence value to be assigned to the packet, and send the packet. The range is from 0 to 7.

- **set-qos-transmit qos-group-value**—Identify a qos-group to be used at egress to specify packets. The range is from 0 to 99.

- **transmit**—Send the packet without altering it.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong> You can enter a single conform-action as part of the command string following the police command. You can also press Enter after the police command to enter policy-map class police configuration mode, where you can enter multiple actions. In policy-map class police configuration mode, you must enter an action to take.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 8** exit  
Return to policy-map configuration mode.

**Step 9** exit  
Return to global configuration mode.

**Step 10** interface interface-id  
Enter interface configuration mode for the interface to which you want to attach the policy.

**Step 11** service-policy input policy-map-name  
Attach the policy map (created in Step 2) to the ingress interface.

**Step 12** end  
Exit privileged EXEC mode.

**Step 13** show policy-map [policy-map-name | interface]  
Verify your entries.

**Step 14** copy running-config startup-config  
(Optional) Save your entries in the configuration file.

### What to do next

Use the no form of the appropriate command to delete an existing policy map, class map, or policer.

This example shows how to configure 2-rate, 3-color policing using policy-map configuration mode.

```text
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000 conform-action transmit exceed-action set-dscp-transmit 24 violate-action drop
Switch(config-pmap-c)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input in-policy
Switch(config-if)# exit
```

This example shows how to create the same configuration using policy-map class police configuration mode.

```text
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000
Switch(config-pmap-c-policy)# conform-action transmit
```
This example shows how to create a traffic classification with a CoS value of 4, create a policy map, and attach it to an ingress port. The average traffic rate is limited to 10000000 b/s with a burst size of 10000 bytes:

Switch(config)# class-map video-class
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map video-policy
Switch(config-pmap)# class video-class
Switch(config-pmap-c)# police 10000000 10000
Switch(config-pmap-c)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input video-policy
Switch(config-if)# exit

This example shows how to create policy map with a conform action of set dscp and a default exceed action.

Switch(config)# class-map in-class-1
Switch(config-cmap)# match dscp 14
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class in-class-1
Switch(config-pmap-c)# police 230000 8000 conform-action set-dscp-transmit 33 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input in-policy
Switch(config-if)# exit

This example shows how to use policy-map class police configuration mode to set multiple conform actions and an exceed action. The policy map sets a committed information rate of 23000 bits per second (bps) and a conform burst size of 10000 bytes. The policy map includes multiple conform actions (for DSCP and for Layer 2 CoS) and an exceed action.

Switch(config)# class-map cos-set-1
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit
Switch(config)# policy-map map1
Switch(config-pmap)# class cos-set-1
Switch(config-pmap-c)# police cir 23000 bc 10000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 48
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input map1
Switch(config-if)# exit

Configuring Input Policy Maps with Marking

You use the set policy-map class configuration command to set or modify the attributes for traffic belonging to a specific class.
Beginning in privileged EXEC mode, follow these steps to create an input policy map that marks traffic:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>policy-map policy-map-name</td>
<td>Create a policy map by entering the policy map name, and enter policy-map configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>class {class-map-name</td>
<td>class-default}</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Choose from one of the following:</td>
<td>Mark traffic by setting a new value in the packet, specifying a table map, or specifying a QoS group.</td>
</tr>
<tr>
<td></td>
<td>• set qos-group value</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• set [ip] dscp {dscp_value</td>
<td>cos [table table-map-name]</td>
</tr>
<tr>
<td></td>
<td>• set [ip] precedence {precedence_value</td>
<td>cos [table table-map-name]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• You can also configure a CoS, DSCP, or IP precedence table and optionally enter the table name. If you do not enter table table-map-name, the table map default behavior is copy.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>exit</td>
<td>Return to policy-map configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>interface interface-id</td>
<td>Enter interface configuration mode for the interface to which you want to attach the policy.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>service-policy input policy-map-name</td>
<td>Attach the policy map (created in Step 2) to the ingress interface.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>show policy-map [policy-map-name class class-map-name]</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
What to do next

Use the no form of the appropriate command to delete a policy map or table map or remove an assigned CoS, DSCP, precedence, or QoS-group value.

This example uses a policy map to remark a packet. The first marking (the set command) applies to the QoS default class map that matches all traffic not matched by class AF31-AF33 and sets all traffic to an IP DSCP value of 1. The second marking sets the traffic in classes AF31 to AF33 to an IP DSCP of 3.

```bash
Switch(config)# policy-map Example
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class AF31-AF33
Switch(config-pmap-c)# set ip dscp 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input Example
Switch(config-if)# exit
```

Configuring Output Policy Maps

You use output policy maps to manage congestion avoidance, queuing, and scheduling of packets leaving the switch. The switch has four egress queues, and you use output policy maps to control the queue traffic. You configure shaping, queue-limit, and bandwidth on these queues. You can use high priority (class-based priority queuing). Policing is not supported on output policy maps, except when configuring priority with police for class-based priority queuing. Output policy map classification criteria are matching a CoS, or DSCP.

Follow these guidelines when configuring output policy maps on physical ports:

- You can configure and attach as many output policy maps as there are ports on the switch. Multiple output policy maps can use the same queue-limit configuration. However, these policy maps can have only two unique queue-limit configurations.
- Output policy maps can have a maximum of eight classes, including the class class-default.
- All output policy maps must use the same set of classes, although the actions for each class can differ for each output policy map.
- In a child policy map, the class-default supports all output policy map actions except priority and police. Action restrictions for class-default are the same as for other classes except that a queue limit configuration for class-default does not require a scheduling action.
- To classify based on criteria at the output, the criteria must be established at the input. You can establish criteria at the input through classification only when you configure only policing and not marking, or through explicit marking when you configure any marking (policing with conform or exceed marking or unconditional set marking).
- You cannot configure class-based priority queuing under the class class-default in an output policy map.
- In an output policy map, unless priority queuing is configured, the class default receives a minimum bandwidth guarantee equal to the unconfigured bandwidth on the port.
- After you have attached an output policy map to an interface by using the service-policy interface configuration command, you can change only the parameters of the configured actions (rates, percentages, and so on) or add or delete classification criteria of the class map while the policy map is attached to the
interface. To add or delete a class or action, you must detach the policy map from all interfaces, modify it, and then reattach it to interfaces.

If you anticipate that you might need three classes in a policy map, you should define three classes when you create the policy map, even if you are not ready to use all three at that time. You cannot add a class to a policy map after it has been attached to an interface.

- When at least one output policy map is attached to an active port, other active ports without output policy maps attached might incorrectly schedule and incorrectly order traffic that uses the same classes as the attached output policy maps. We recommend attaching output policy maps to all ports that are in use. We also recommend putting any unused ports in the shutdown state by entering the shutdown interface configuration command. For example, if you attach an output policy map that shapes DSCP 23 traffic to a port, DSCP traffic that is sent out of any other port without a policy map attached could be incorrectly scheduled or ordered incorrectly with respect to other traffic sent out of the same port.

- When configuring the interface to operate a fixed port speed if there's an output policy-map applied that has dependencies on port bandwidth. Use the interface level command to fix the port speed and remove the auto negotiation of speed. You can leave the negotiation of duplex. If an output policy-map is configured on a port that is set to auto negotiate speed, and the speed negotiates to a value that invalidates the output policy-map, the port is put into error-disabled state.

- You can attach only one output policy map per port.

- The maximum number of policy maps configured on the switch is 256.

These sections describe how to configure different types of output policy maps:

**Configuring Output Policy Maps with Class-Based-Weighted-Queuing**

You use the bandwidth policy-map class configuration command to configure class-based weighted fair queuing (CBWFQ). CBWFQ sets the relative precedence of a queue by allocating a portion of the total bandwidth that is available for the port.

Follow these guidelines when configuring CBWFQ:

- When configuring bandwidth in a policy map, all rate configurations must be in the same format, either a configured rate or a percentage.

- The total rate of the minimum bandwidth guarantees for each queue of the policy cannot exceed the total speed for the interface.

- You cannot configure CBWFQ (bandwidth) and traffic (shape average) or priority queuing (priority) for the same class in an output policy map.

- You cannot configure bandwidth as an absolute rate or a percentage of total bandwidth when strict priority (priority without police) is configured for another class map.

- You can configure bandwidth as a percentage of remaining bandwidth only when strict priority (priority without police) is configured for another class in the output policy map.

- When you configure CIR bandwidth for a class as an absolute rate or a percentage of total bandwidth, any excess bandwidth that remains after servicing the CIR of all classes in the policy map is divided among the classes the same proportion as the CIR rates. If you configure the CIR rate of a class to be 0, that class is not eligible for any excess bandwidth and will receive no bandwidth.
Beginning in privileged EXEC mode, follow these steps to use CBWFQ to control bandwidth allocated to a traffic class by specifying a minimum bandwidth as a bit rate or a percentage:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>policy-map policy-map-name</td>
<td>Create a policy map by entering the policy map name, and enter policy-map configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>class {class-map-name</td>
<td>class-default}</td>
</tr>
</tbody>
</table>
| 4     | bandwidth {rate | percent value | remaining value} | Set output bandwidth limits for the policy-map class.  
  • Enter a rate to set bandwidth in kilobits per second. The range is from 64000 to 1000000000.  
  • Enter percent value to set bandwidth as a percentage of the total bandwidth. The range is 1 to 100 percent.  
  • Enter remaining percent value to set bandwidth as a percentage of the remaining bandwidth. The range is 1 to 100 percent. This keyword is valid only when strict priority (priority without police) is configured for another class in the output policy map. You must specify the same units in each bandwidth configuration in an output policy (absolute rates or percentages). The total guaranteed bandwidth cannot exceed the total available rate. |
| 5     | exit                              | Return to policy-map configuration mode.                                |
| 6     | exit                              | Return to global configuration mode.                                    |
| 7     | interface interface-id            | Enter interface configuration mode for the interface to which you want to attach the policy. |
| 8     | service-policy output policy-map-name | Attach the policy map (created in Step 2) to the egress interface. |
| 9     | end                               | Return to privileged EXEC mode.                                         |
| 10    | show policy-map [policy-map-name [class class-map-name]] | Verify your entries.                                 |
| 11    | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

### What to do next

After you have created an output policy map, you attach it to an egress port.
Use the no form of the appropriate command to delete an existing policy map, class map, or bandwidth configuration.

**Note:** If you enter the no policy-map configuration command or the no policy-map policy-map-name global configuration command to delete a policy map that is attached to an interface, a warning message appears that lists any interfaces from which the policy map is being detached. The policy map is then detached and deleted. For example:

```
Warning: Detaching Policy test1 from Interface GigabitEthernet1/17
```

This example shows how to set the precedence of a queue by allocating 25 percent of the total available bandwidth to the traffic class defined by the class map:

```
Switch(config)# policy-map gold_policy
Switch(config-pmap)# class out_class-1
Switch(config-pmap-c)# bandwidth percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# service-policy output gold_policy
Switch(config-if)# exit
```

### Configuring Output Policy Maps with Class-Based Shaping

You use the shape average policy-map class configuration command to configure traffic shaping. Class-based shaping is a control mechanism that is applied to classes of traffic leaving an interface and uses the shape average command to limit the rate of data transmission used for the committed information rate (CIR) for the class.

Follow these guidelines when configuring class-based shaping:

- Configuring a queue for traffic shaping sets the maximum bandwidth or peak information rate (PIR) of the queue. Configuring traffic shaping automatically also sets the minimum bandwidth guarantee or CIR of the queue to the same value as the PIR.
- You cannot configure CBWFQ (bandwidth) or priority queuing (priority) and traffic (shape average) for the same class in an output policy map.
- You cannot configure traffic shaping for a traffic class when strict priority (priority without police) is configured for another class within the output policy-map.

Beginning in privileged EXEC mode, follow these steps to use class-based shaping to configure the maximum permitted average rate for a class of traffic:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> policy-map policy-map-name</td>
<td>Create a policy map by entering the policy map name, and enter policy-map configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> class {class-map-name</td>
<td>class-default}</td>
</tr>
</tbody>
</table>
## Configuring Output Policy Maps with Port Shaping

Port shaping is applied to all traffic leaving an interface. It uses a policy map with only class default when the maximum bandwidth for the port is specified by using the `shape average` command.

Beginning in privileged EXEC mode, follow these steps to use port shaping to configure the maximum permitted average rate for a class of traffic:

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> policy-map <code>policy-map-name</code></td>
<td>Create a policy map by entering the policy map name, and enter policy-map configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> class class-default</td>
<td>Enter a policy-map class configuration mode for the default class.</td>
</tr>
<tr>
<td><strong>Step 4</strong> shape average <code>target bps</code></td>
<td>Specify the average class-based shaping rate. For target bps, specify the average bit rate in bits per second. The range is from 64000 to 1000000000.</td>
</tr>
</tbody>
</table>
Configuring Output Policy Maps with Class-Based Priority Queuing

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong> interface interface-id</td>
<td>Enter interface configuration mode for the interface to which you want to attach the policy.</td>
</tr>
<tr>
<td><strong>Step 6</strong> service-policy output policy-map-name</td>
<td>Attach the policy map (created in Step 2) to the egress interface..</td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 9</strong> show policy-map [policy-map-name [class class-map-name]]</td>
<td>Verify your entries.</td>
</tr>
<tr>
<td><strong>Step 10</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**What to do next**

Use the no form of the appropriate command to delete an existing hierarchical policy map, to delete a port shaping configuration, or to remove the policy map from the hierarchical policy map.

This example shows how to configure port shaping by configuring a hierarchical policy map that shapes a port to 90 Mbps, allocated according to the out-policy policy map configured in the previous example.

```plaintext
Switch(config)# policy-map out-policy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

**Configuring Output Policy Maps with Class-Based Priority Queuing**

You can use the priority policy-map class configuration command to ensure that a particular class of traffic is given preferential treatment. With strict priority queuing, the priority queue is constantly serviced; all packets in the queue are scheduled and sent until the queue is empty. Excessive use of the priority queues can possibly delay packets in other queues and create unnecessary congestion.

You can configure strict priority queuing (priority without police), or you can configure an unconditional priority policer (priority with police). Follow these guidelines when configuring priority queuing:

- You can associate the priority command with a single unique class for all attached output policies on the switch.
- When you configure a traffic class as a priority queue, you can configure only police and queue-limit as other queuing actions for the same class. You cannot configure bandwidth or shape average with priority queues in the same class.
- You cannot associate the priority command with the class-default of the output policy map.

**Configuring Priority Without Police**

Follow these guidelines when configuring strict priority queuing (priority without police):
• You cannot configure priority queuing without policing for a traffic class when class-based shaping (shape average) or CBWFQ (bandwidth) is configured for another class within the output policy-map.

• When you configure priority queuing without policing for a traffic class, you can only configure the other queues for sharing by using the bandwidth remaining percent policy-map class configuration command to allocate excess bandwidth. This command does not guarantee the allocated bandwidth, but does ensure the rate of distribution.

Beginning in privileged EXEC mode, follow these steps to configure a strict priority queue:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>class-map class-map-name</td>
<td>Create classes for three egress queues. Enter match conditions classification for each class.</td>
</tr>
<tr>
<td>3</td>
<td>policy-map policy-map-name</td>
<td>Create a policy map by entering the policy map name, and enter policy-map configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>class class-map-name</td>
<td>Enter the name of the priority class (created by using the class-map global configuration command), and enter policy-map class configuration mode for the priority class.</td>
</tr>
<tr>
<td>5</td>
<td>priority</td>
<td>Set the strict scheduling priority for this class. <strong>Note</strong> Only one unique class map on the switch can be associated with a priority command. You cannot configure priority along with any other queuing action (bandwidth or shape average).</td>
</tr>
<tr>
<td>6</td>
<td>exit</td>
<td>Exit policy-map class configuration mode for the priority class.</td>
</tr>
<tr>
<td>7</td>
<td>class class-map-name</td>
<td>Enter the name of a nonpriority class, and enter policy-map class configuration mode for that class.</td>
</tr>
<tr>
<td>8</td>
<td>bandwidth remaining percent value</td>
<td>Set output bandwidth limits for the policy-map class as a percentage of the remaining bandwidth. The range is 1 to 100 percent.</td>
</tr>
<tr>
<td>9</td>
<td>exit</td>
<td>Exit policy-map class configuration mode for the class.</td>
</tr>
<tr>
<td>10</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>11</td>
<td>interface interface-id</td>
<td>Enter interface configuration mode for the interface to which you want to attach the policy.</td>
</tr>
<tr>
<td>12</td>
<td>service-policy output policy-map-name</td>
<td>Attach the policy map (created in Step 3) to the egress interface.</td>
</tr>
<tr>
<td>13</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action** | **Purpose**
--- | ---
Step 14 | show policy-map
Step 15 | copy running-config startup-config

---

### What to do next

After you have created an output policy map, you attach it to an egress port.

Use the no form of the appropriate command to delete an existing policy map or class map or to cancel strict priority queuing for the priority class or the bandwidth setting for the other classes.

This example shows how to configure the class out-class1 as a strict priority queue so that all packets in that class are sent before any other class of traffic. Other traffic queues are configured so that out-class-2 gets 50 percent of the remaining bandwidth and out-class3 gets 20 percent of the remaining bandwidth. The class class-default receives the remaining 30 percent with no guarantees.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

### Configuring Output Policy Maps with Weighted Tail Drop

Weighted tail drop (WTD) adjusts the queue size (buffer size) associated with a traffic class. You configure WTD by using the queue-limit policy-map class configuration command.

Follow these guidelines when configuring WTD:

- Configuring WTD with the queue-limit command is supported only when you first configure a scheduling action, such as bandwidth, shape average, or priority. The exception to this is when you are configuring queue-limit in the class-default.

- You can configure and attach as many output policy maps as there are ports. Multiple output policy maps can use the same queue-limit configuration. However, these policy maps can have only three unique queue-limit configurations.

- You can use the queue-limit command to configure the queue-limit for CPU-generated traffic.

- When you use the queue-limit command to configure queue thresholds for a class, the WTD thresholds must be less than or equal to the queue maximum threshold. A queue size configured with no qualifier must be larger than any queue sizes configured with qualifiers.

- You cannot configure more than two unique threshold values for the WTD qualifiers (cos, dscp, precedence, or qos-group) in the queue-limit command. However, there is no limit to the number of
qualifiers that you can map to those thresholds. You can configure a third unique threshold value to set the maximum queue, using the queue-limit command with no qualifiers.

- A WTD qualifier in the queue-limit command must be the same as at least one match qualifier in the associated class map.

- In an output policy map, when you configure a queue-limit for a unique class, all other output policy maps must use the same format of qualifier type and qualifier value. Only queue-limit threshold values can be different. For example, when you configure class A queue-limit thresholds for dscp 30 and dscp 50 in policy-map 1, and you configure class A queue-limits in policy-map 2, you must use dscp 30 and dscp 50 as qualifiers. You cannot use dscp 20 and dscp 40. The threshold values can be different, but different threshold values would create a new unique queue-limit configuration.

Beginning in privileged EXEC mode, follow these steps to use WTD to adjust the queue size for a traffic class:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> policy-map <em>policy-map-name</em></td>
<td>Create a policy map by entering the policy map name, and enter policy-map configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> class *{class-map-name</td>
<td>class-default}*</td>
</tr>
<tr>
<td><strong>Step 4</strong> bandwidth *{rate</td>
<td>percent value</td>
</tr>
<tr>
<td><strong>Step 5</strong> queue-limit *{cos value</td>
<td>dscp value</td>
</tr>
</tbody>
</table>

- (Optional) For cos value, specify a CoS value. The range is from 0 to 7.
- (Optional) For dscp value, specify a DSCP value. The range is from 0 to 63.
- (Optional) For precedence value, specify an IP precedence value. The range is from 0 to 7.
- (Optional) For qos-group value, enter a QoS group value. The range is from 0 to 99.
- For number-of-packets, set the minimum threshold for WTD. The range is from 16 to 544, in multiples of 16, where each packet is a fixed unit of 256 bytes.

**Note** For optimal performance, we strongly recommend that you configure the queue-limit to 272 or less.

The value is specified in packets by default, but the packets keyword is optional.
### Configuring Output Policy Maps with Weighted Tail Drop

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>exit</strong></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>interface interface-id</strong></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>service-policy output policy-map-name</strong></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>show policy-map [policy-map-name [class class-map-name]]</strong></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td><strong>copy running-config startup-config</strong></td>
</tr>
</tbody>
</table>

### What to do next

After you have created an output policy map, you attach it to an egress port.

Use the no form of the appropriate command to delete an existing policy map or class map or to delete a WTD configuration.

This example shows a policy map with a specified bandwidth and queue size. Traffic that is not DSCP 30 or 10 is assigned a queue limit of 112 packets. Traffic with a DSCP value of 30 is assigned a queue-limit of 48 packets, and traffic with a DSCP value of 10 is assigned a queue limit of 32 packets. All traffic not belonging to the class traffic is classified into class-default, which is configured with 10 percent of the total available bandwidth and a large queue size of 256 packets.

```
Switch(config)# policy-map gold-policy
Switch(config-pmap)# class traffic
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 112
Switch(config-pmap-c)# queue-limit dscp 30 48
Switch(config-pmap-c)# queue-limit dscp 10 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 256
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface GigabitEthernet1/17
```
Switch(config-if)# service-policy output gold-policy
Switch(config-if)# exit

Displaying QoS Information

To display QoS information, use one or more of the privileged EXEC commands in Table.

This section contains the following topics:

• QoS Statistics, on page 191
• Restrictions and Limitations, on page 193

Commands for Displaying Standard QoS Information:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show class-map [class-map-name]</td>
<td>Display QoS class-map information for all class maps or the specified class map.</td>
</tr>
<tr>
<td>show policer aggregate [aggregate-policer-name]</td>
<td>Display information about all aggregate policers or the specified aggregate policer.</td>
</tr>
<tr>
<td>show policy-map [policy-map-name</td>
<td>interface [interface-id] [input</td>
</tr>
<tr>
<td>show cpu traffic qos</td>
<td>Display the QoS marking values for CPU-generated traffic.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Display the configured class maps, policy maps, table maps, and aggregate policers.</td>
</tr>
<tr>
<td>show table-map [table-map-name]</td>
<td>Display information for all configured table maps or the specified table map.</td>
</tr>
</tbody>
</table>

To test full-path QoS in both directions on an interface, you can configure Ethernet terminal loopback by entering the ethernet loopback facility interface configuration command. In terminal loopback mode, the port appears to be up but the link is actually down and no packets are sent out. Configuration changes on the port immediately affect the traffic being looped back.

QoS Statistics

There are several ways to display QoS input and output policy-map statistics.

For input policy maps, you can use the `show policy-map interface [interface-id]` privileged EXEC command to display per-class per-policer conform and exceed statistics. Policer conform statistics are the number of packets that conform to the configured policer profile; policer exceed statistics are the number of packets that exceed the configured policer profile. The switch does not support per-class classification statistics, but you can determine these statistics by configuring policing at line rate for the class. In this case, no packets exceed the configured policer profile, and the policer conform statistics would equal the class classification statistics.

This output also includes byte-level statistics for conform, exceed, and violate classes.

Another way to view input QoS statistics is in the output of the `show platform qos statistics interface [interface-id]` privileged EXEC command. The per-port frame statistics are sorted by the DSCP and CoS
values of the incoming frames on the port. These statistics do not provide any information about the MQC input policy map configured on the interface.

For output policy maps, you can use the `show policy-map interface [interface-id]` command to display per-class classification statistics that show the total number of packets that match the specified class. This count includes the total number of packets that are sent and dropped for that class. You can use the same command to view the per-class tail drop statistics.

For details on queue and packets processed details use the show platform hardware qos asic 0 port [port id]. Portid can be obtained from the CLI show platform pm port-map

Example:

```
Switch#show platform pm port-map
interface gid gpn asic slot unit gpn-idb
------------------------------------------------------------------------
Te1/1 1 1 0/25 1 1 Yes
Te1/2 2 2 0/27 1 2 Yes
Gi1/3 3 3 0/2 1 3 Yes
Gi1/4 4 4 0/3 1 4 Yes
Gi1/5 5 5 0/0 1 5 Yes
Gi1/6 6 6 0/1 1 6 Yes
Gi1/7 7 7 0/6 1 7 Yes
Gi1/8 8 8 0/7 1 8 Yes
Gi1/9 9 9 0/4 1 9 Yes
Gi1/10 10 10 0/5 1 10 Yes
Gi2/1 11 11 0/10 2 1 Yes
Gi2/2 12 12 0/11 2 2 Yes
Gi2/3 13 13 0/8 2 3 Yes
Gi2/4 14 14 0/9 2 4 Yes
Gi2/5 15 15 0/14 2 5 Yes
Gi2/6 16 16 0/15 2 6 Yes
Gi2/7 17 17 0/12 2 7 Yes
Gi2/8 18 18 0/13 2 8 Yes
Gi2/9 19 19 0/18 2 9 Yes
Gi2/10 20 20 0/19 2 10 Yes
Gi2/11 21 21 0/16 2 11 Yes
Gi2/12 22 22 0/17 2 12 Yes
Gi2/13 23 23 0/22 2 13 Yes
Gi2/14 24 24 0/23 2 14 Yes
Gi2/15 25 25 0/20 2 15 Yes
Gi2/16 26 26 0/21 2 16 Yes
Switch#
```

```
Switch#show platform hardware qos asic 0 port 1
Dropping QoS settings for port 1Port | Trust | Modify | Modify | Default | Default| Mode |
DSCP | UP | QosProfile | UP---- |------ | ------ | ------ | ---------- | -------1 | L2+L3
| No | No | 65 | 0Queue[0]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:22
| Drops[2]:0Queue[1]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:0
| Drops[2]:0Queue[2]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:0
| Drops[2]:0Queue[3]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:0
| Drops[2]:0Queue[4]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:0
| Drops[2]:0Queue[5]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:0
| Drops[2]:0Queue[6]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:196
| Drops[2]:0Queue[7]: Thresh[0]:0 Drops[0]:0 Thresh[1]:0 Drops[1]:0 Thresh[2]:104455
| Drops[2]:0Switch#
```
## Restrictions and Limitations

<table>
<thead>
<tr>
<th>Feature</th>
<th>Restriction / Limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.of Class-maps in a policy-map</td>
<td>8 (7 + Class default) for both ingress and egress.</td>
</tr>
<tr>
<td>No.of Filters in a policy-map</td>
<td>8 (Including ACL’s, Match-Criteria across all classes)</td>
</tr>
<tr>
<td>No.of ACE’s in a policy-map</td>
<td>256 (Across all classes in a policy)</td>
</tr>
<tr>
<td>Match-all with multiple match criteria</td>
<td>Not supported with current-release</td>
</tr>
<tr>
<td>Classmap matching on access-group of different types</td>
<td>Within a policymap, classmap's matching on access-group of different types is not supported. All classmap's should be matching on the same type of access-group, (mac or ipv4 or ipv6), not a combination of these.</td>
</tr>
<tr>
<td>No support for this interface level QOS command</td>
<td><strong>bandwidth qos-reference</strong> <em>(value)</em></td>
</tr>
</tbody>
</table>
Locate Switch

- Configuring Locate Switch, on page 195

**Configuring Locate Switch**

The Locate Switch feature allows you to easily locate the physical location of a specific switch on your network. This feature enables the flashing of LEDs on a specific switch, which is useful for locating a device within a room with many interconnected devices. When this feature is activated, the following LEDs on the device blink alternately green and red for the specified amount of time:

- Alarm IN (there are two alarm IN LEDs)
- Alarm OUT
- System
- Express Setup

To configure and activate Locate Switch:

Enter the following command and a value from 9 to 255 for the number of seconds to continue the blinking pattern:

```
locate-switch [seconds]
```

The default is 255. The LEDs continue the blinking pattern for the specified number of seconds. Enter 0 seconds to stop the blinking pattern before the number of seconds expires.

The `locate-switch` command is a volatile command and will not be saved or displayed in running or startup configuration.

**Example**

```
Switch# locate-switch
Switch# locate-switch 0
```